digital

Panoramas **Phishing** 2023

Panorama de Phishing 2023

TLP:RED

No divulgar, restringido solo a participantes.

TLP:AMBER

Divulgación limitada, restringida a la organización de los participantes y sus clientes.

TLP:GREEN

Divulgación limitada, restringida a la comunidad.

TLP:CLEAR

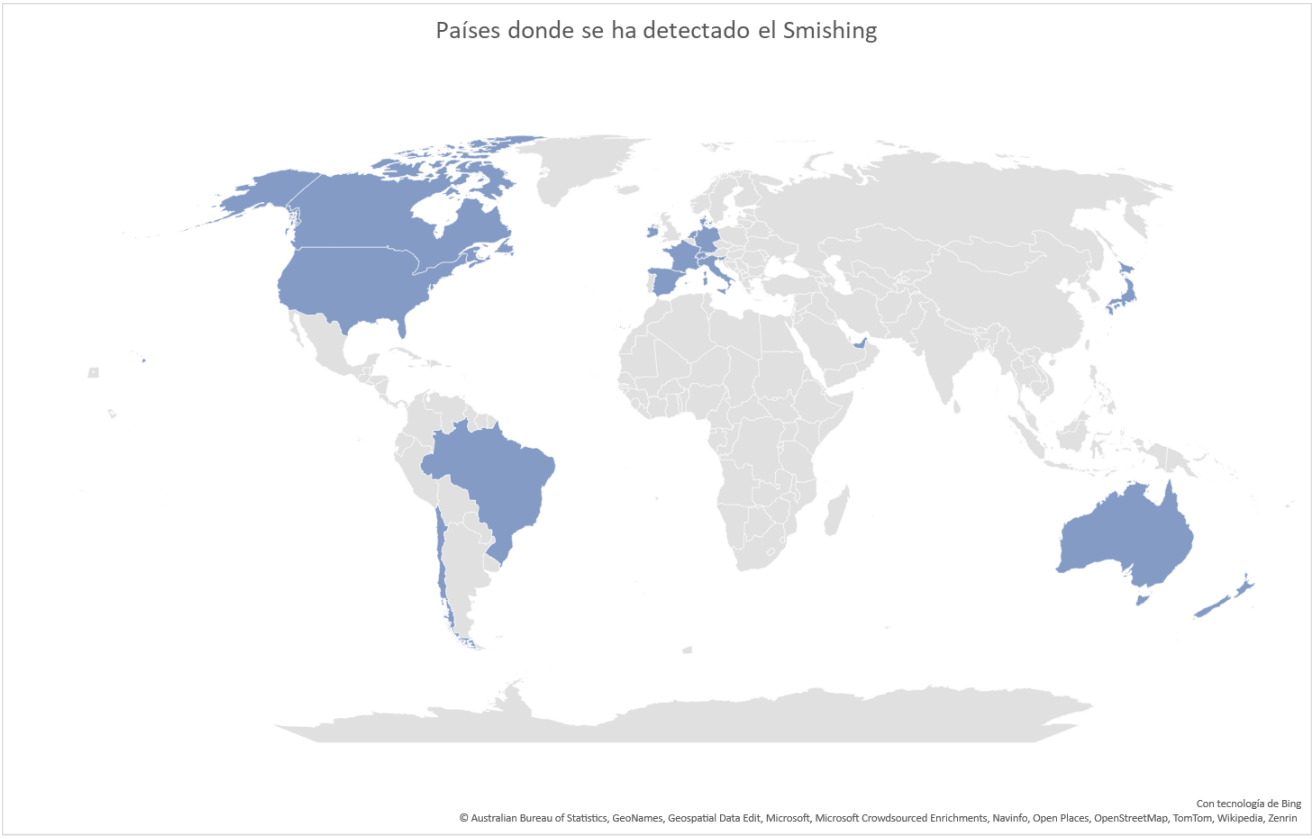
Divulgación sin restricciones.

A lo largo del 2023, hemos identificado numerosas campañas de Smishing dirigidas a usuarios chilenos, donde se suplantan diversas entidades locales usando técnicas de ingeniería social en esquemas de fraude altamente sofisticados.

En los siguientes apartados, desglosamos aspectos de este esquema, que sigue en análisis debido a su considerable impacto y rápida propagación. Lo observado hasta ahora pone de manifiesto la presencia de actores de amenaza altamente especializados, respaldados por una amplia infraestructura y un notable nivel de coordinación, factores esenciales para el éxito de sus campañas.

Smishing en Chile y el mundo

Si bien esta campaña en Chile ha tenido un peak de actividad que comenzó aproximadamente en julio de 2023 al igual que en Brasil, esta actividad no es nueva, ya que a nivel global se habían observado casos como este desde octubre de 2022 en Norteamérica suplantando a diferentes entidades según cada país, pero todas coincidiendo con la misma temática, compañías de correos o de transporte de encomiendas.



- Alemania
- Australia
- Brasil
- Canadá
- Chile
- Dinamarca
- Emiratos Arabes Unidos
- Eslovenia
- España
- Estados Unidos
- Francia
- Holanda
- Irlanda
- Italia
- Japón
- Nueva Zelanda
- Singapur
- Suiza

Detecciones

Mediante un análisis a diferentes sitios y portales web, fue posible generar un seguimiento de distintos reportes de sitios fraudulentos vinculados a esta campaña desde diferentes partes del mundo, pudiendo obtener 11.934 reportes y detecciones las cuales corresponden a 3.584 dominios únicos, vinculados tanto al sitio de fraude direccionado mediante el Smishing, como al panel de administración de sus campañas.

En esta misma línea, también se ha podido evidenciar un total de 99 TLD (Top Level Domain) desde donde se extrae Top 20 con los dominios más utilizados por los actores para registrar sus campañas, siendo estos tres considerablemente los más abundantes en las campañas.

- .top
- .com
- .xyz

De la misma investigación se pudo identificar los sitios web fraudulentos detectados para cada uno de los países, los cuales se ordenan de la siguiente forma:

- Canadá:
  - Canada Post (canadapost-postescanada.ca)
- Estados Unidos:
  - United States Postal Service (usps.com)
  - Amazon (amazon.com)

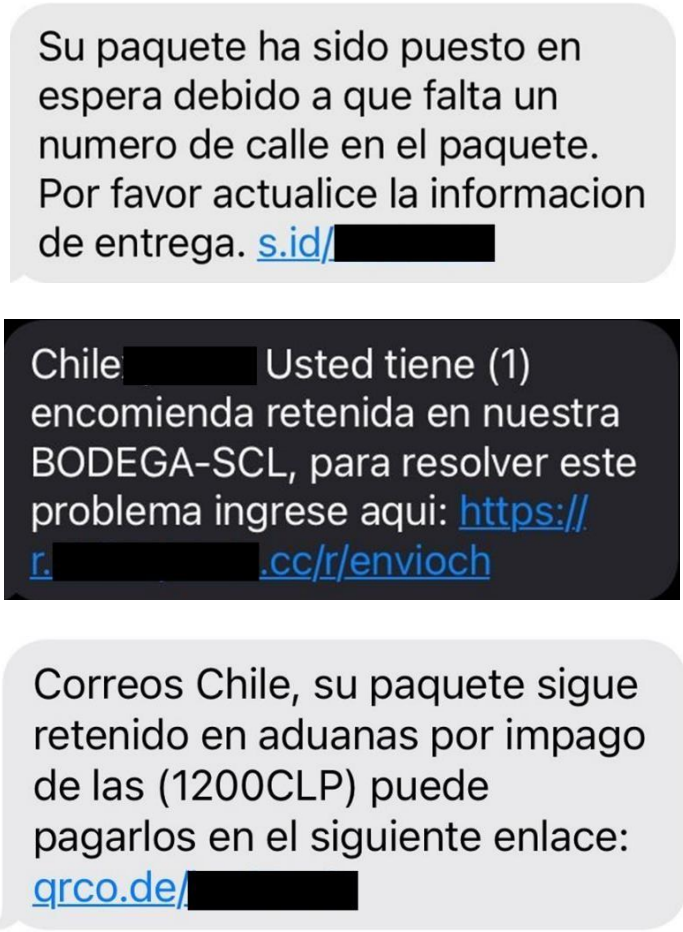
- Australia:
  - Australia Post (auspost.com.au)
  - LinkT (linkt.com.au)
  - Amazon Australia (amazon.com.au)
- Japón:
  - Amazon Japan (amazon.co.jp)
- Singapur:
  - DHL Singapur (dhl.com/sg-en)
  - OneMotoring (onemotoring.lta.gov.sg)
- Francia:
  - LaPoste (laposte.fr)
- Irlanda:
  - An Post (anpost.com)
- España:
  - Correos (correos.es)
  - Vodafone (vodafone.es)
- Nueva Zelanda:
  - New Zealand Transport Agency (nzta.govt.nz)
- Dinamarca:
  - Postnord (postnord.com)
- Italia:
  - Posteitaliane (poste.it)
- Holanda:
  - Post NL (postnl.post)
- Alemania:
  - Telekom Erleben (telekom.de)

- Emiratos Arabes Unidos:
  - Etisalat (etisalat.ae)
- Chile:
  - Correos Chile (correos.cl)
- Brasil:
  - Correios (correios.com.br)
- Suiza:
  - Die Post (post.ch)
- Eslovenia:
  - Pošta Slovenije (posta.si)

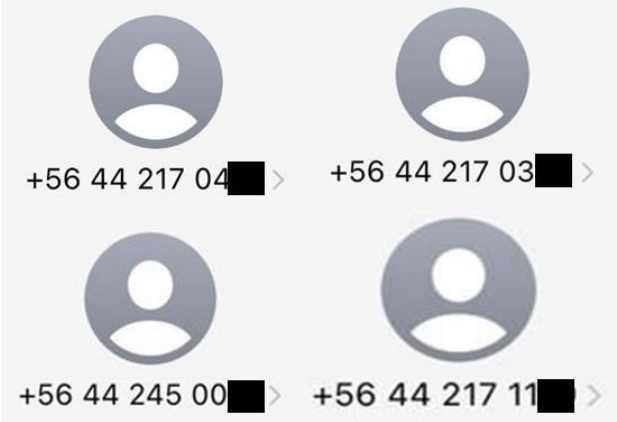
¿Cómo se desarrolla la campaña y cuáles son sus objetivos?

Distribución

Es muy probable que usted o algún conocido haya recibido un mensaje de texto de dudosa procedencia mencionando que "la entrega de su paquete ha sido suspendida debido a que falta un número de la calle en el paquete", alertando sobre "Encomienda retenida en nuestra BODEGA-SCL" o que "su paquete sigue retenido en aduanas por impago de las (1200CLP)", en donde todas ellas mediante un mensaje de urgencia lo incitan a acceder a un enlace malicioso, el cual en gran parte de las ocasiones viene acortado para que no se pueda identificar de manera rápida el destino final de dicho enlace. Esto es posible ocupando técnicas de ingeniería social como es el llamado a la urgencia y a la rápida acción, objeto la víctima ingrese al enlace y siga las instrucciones, sin cuestionarse la veracidad del mensaje.



Todos estos mensajes, al menos para el caso de Chile, se encuentran originados desde un número de teléfono iniciado con +56 44 y que inclusive muchas veces los usuarios han recibido mensajes previos del mismo número, pero con códigos MFA de plataformas válidas.



El código +56 44 resulta poco común debido a que no pertenece a un número de teléfono móvil, fijo, ni de regiones en chile. Este código se encuentra compuesto por el identificador de país (+56) y el identificador de línea telefónica VoIP (44), el cual es comúnmente utilizado por centrales de Call Center, por lo que resulta ser un número completamente válido. Sin embargo, pese que según la siguiente tabla se menciona que los códigos de ciudades son los usados (hasta el año 2014), el código 44 en la actualidad se mantiene para el mismo fin.

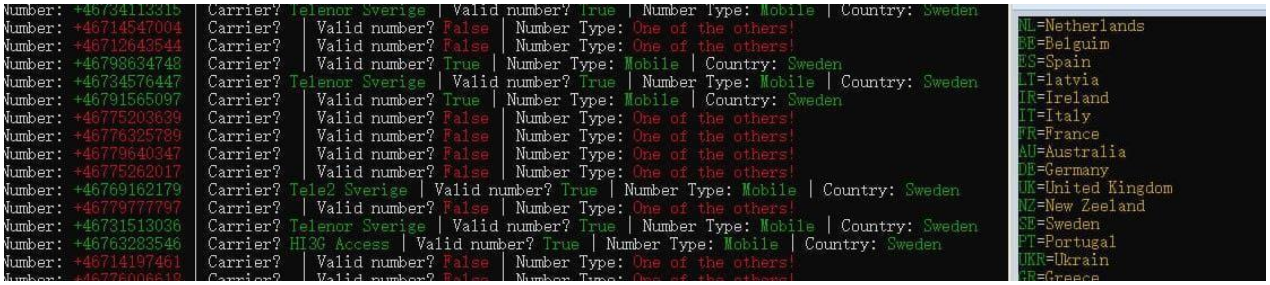
Antiguos prefijos telefónicos de Chile (usados hasta 2014)

Prefijo	Provincia	Región	Zona
2	Provincias de Santiago, Chacabuco, Cordillera, Maipo, Melipilla y Talagante	Región Metropolitana de Santiago	Centro
32	Provincias de Valparaíso y Marga Marga (comunas de Quilpué y Villa Alemana)	Región de Valparaíso	
33	Provincias de Petorca, Quillota y Marga Marga (comunas de Limache y Olmué)	Región de Valparaíso	
34	Provincias de Los Andes y San Felipe de Aconcagua	Región de Valparaíso	
35	Provincia de San Antonio	Región de Valparaíso	
39	Provincia de Isla de Pascua[2]	Región de Valparaíso	
41	Provincias de Arauco y Concepción	Región del Biobío	Sur
42	Provincias de Diguillín, Itata y Punilla	Región de Ñuble	
43	Provincia de Biobío	Región del Biobío	
44	Telefonía sobre IP	Nivel nacional	Especial
45	Provincias de Cautín y Malleco	Región de la Araucanía	Sur
51	Provincias de Huasco y Elqui	Región de Atacama y Región de Coquimbo	Norte
52	Provincias de Chañaral y Copiapó	Región de Atacama	
53	Provincias de Choapa y Limarí	Región de Coquimbo	
55	Provincias de Antofagasta, El Loa y Tocopilla	Región de Antofagasta	
57	Provincias de Iquique y Tamarugal	Región de Tarapacá	
58	Provincias de Arica y Parinacota	Región de Arica y Parinacota	
61	Provincias de Antártica Chilena, Magallanes, Tierra del Fuego y Última Esperanza	Región de Magallanes y de la Antártica Chilena	Sur
63	Provincias de Valdivia y del Ranco (excepto comunas de La Unión y Río Bueno)	Región de Los Ríos	
64	Provincias del Ranco (comunas de La Unión y Río Bueno) y de Osorno	Región de Los Ríos y Región de Los Lagos	
65	Provincias de Chiloé, Llanquihue y Palena	Región de Los Lagos	
67	Provincias de Aysén, Capitán Prat, Coyhaique y General Carrera	Región de Aysén del General Carlos Ibáñez del Campo	
68	Provincia de Aysén, (Puyuhuapi)	Región de Aysén del General Carlos Ibáñez del Campo	
71	Provincia de Talca	Región del Maule	Centro Sur
72	Provincias de Cachapoal, Cardenal Caro y Colchagua	Región del Libertador General Bernardo O'Higgins	
73	Provincias de Cauquenes y Linares	Región del Maule	
75	Provincia de Curicó	Región del Maule	

Entonces, la interrogante es la siguiente, ¿cómo los actores logran esto sin ser descubiertos?, pudiendo obtener de forma general dos principales respuestas:

- Abuso de canales y plataformas válidas de marketing telefónico o de call center.
- Spoofing de telefonía VoIP, lo cual requiere otras técnicas para lograr facilitar esta tarea.

Sin embargo, este antecedente aún se encuentra bajo materia de análisis, debido a que mediante los hallazgos de canales de comunicación se evidencian capturas de pantalla y video de un software que comprueba la validez, el carrier y el país de largas listas de números telefónicos de potenciales víctimas.



Phishing

Cuando el usuario accede al mensaje fraudulento y visita el sitio web proporcionado, se encuentra con una página que suele ser sorprendentemente similar, si no es que idéntica, al sitio legítimo. Existen diversas herramientas que facilitan la creación de estas réplicas con relativa sencillez.

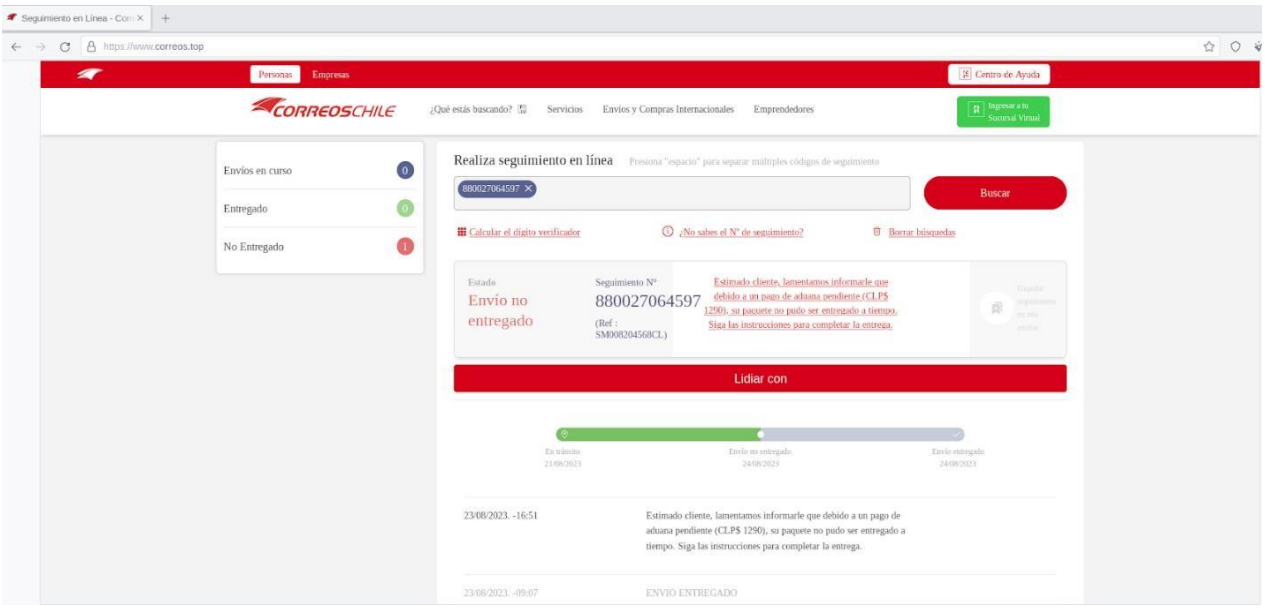
Es crucial subrayar que hay múltiples campañas de phishing que operan simultáneamente, conduciendo a diferentes sitios web fraudulentos. Estas campañas pueden variar en sus características o configuraciones. De hecho, las muestras recolectadas en diferentes fechas han mostrado cómo los ciberdelincuentes han ido refinando sus tácticas a través de un proceso de ensayo y error, haciendo cada vez más difícil el rastreo hacia sus servidores de comando y control.

En el presente reporte, se analizarán dos muestras recopiladas en distintos momentos: la primera en julio y la segunda en septiembre de 2023. Estas muestras ilustran claramente los cambios y evoluciones previamente mencionados.

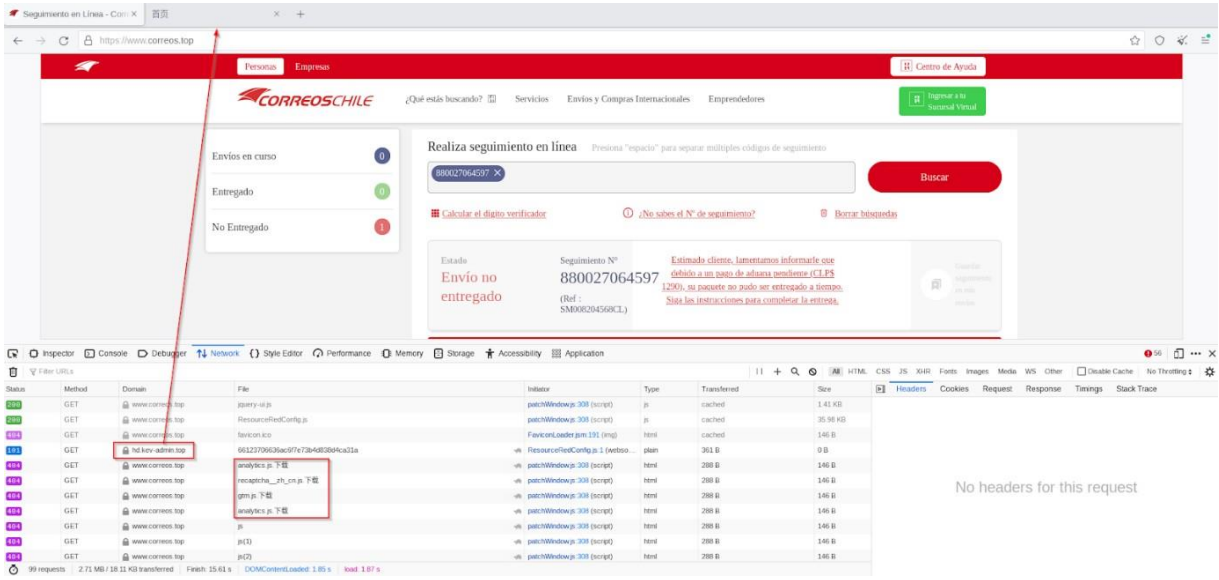
Muestra 1

Para el primer caso, se observa cómo el sitio web suplantado pese a coincidir en gran parte con el oficial, al insertar el código de seguimiento fraudulento este presenta fallas de diseño en la tipografía, que hacen sospechar de su legitimidad, pero que de igual forma presenta otros factores que llevan a la confusión.

En este sitio, se mantiene la premisa entregada en el mensaje de texto, donde se mencionan problemas con un paquete en específico y que necesitan ser resueltos para el correcto envío.

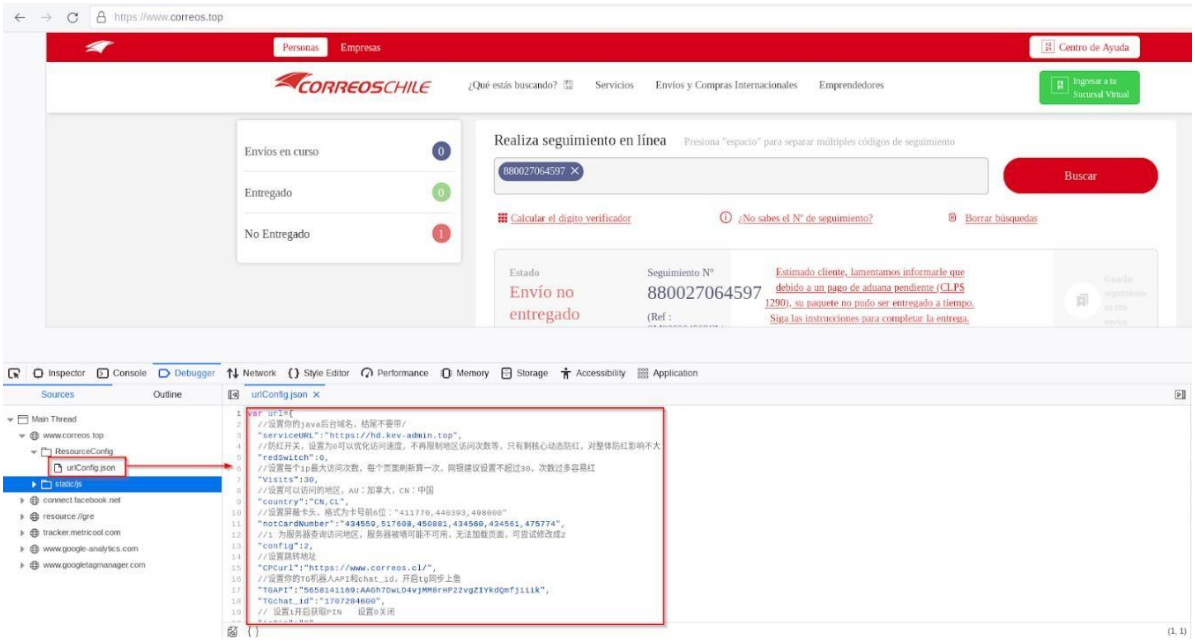


Una vez que se inspeccionan los elementos de red cargados en el sitio, es posible visualizar comunicación con un dominio que no corresponde al mismo en que se navega, mientras que en algunos de los javascript cargados, se identifican caracteres del alfabeto chino, pudiendo identificar rápidamente el origen de esta campaña.



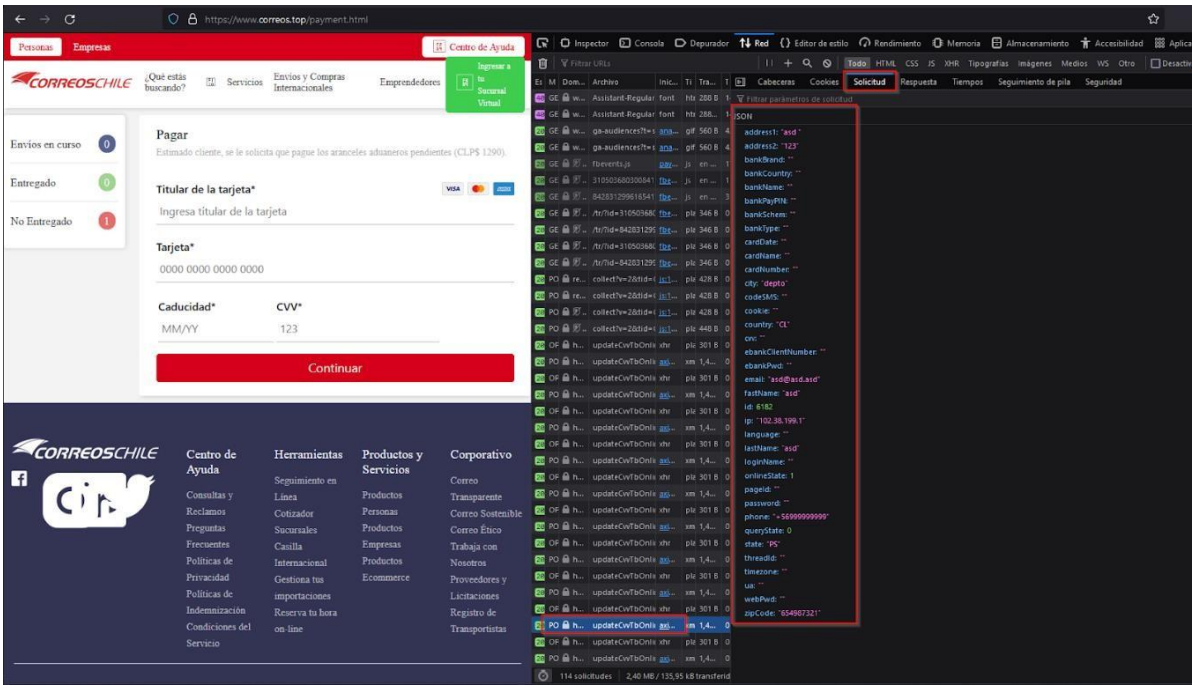
En este mismo análisis, también es posible detectar un archivo de configuración en donde se establecen diferentes parámetros para la ejecución del fraude. Pese a que se encuentra en idioma Chino, tras una rápida revisión se identifica que se establecen los siguientes parámetros:

- Servidor Command And Control.
- Cantidad máxima de visitas simultáneas.
- Acceso georreferenciado para China y Chile.
- Sitio web legítimo para redirección.
- BINS de tarjetas bancarias NO aceptadas
- Datos de Telegram para recopilación de información capturada.



Una vez que se han seguido todos los pasos solicitados para "recuperar el paquete en tránsito" el sitio web entrega un formulario para el ingreso de datos bancarios, lo que sumado a la información de contacto entregada en una fase previa se logran capturar los siguientes datos personales, ya sea de forma manual o de forma automatizada como el caso de la IP, lo que brinda a los actores de amenaza información más que suficiente para realizar suplantación de identidad y fraude bancario.

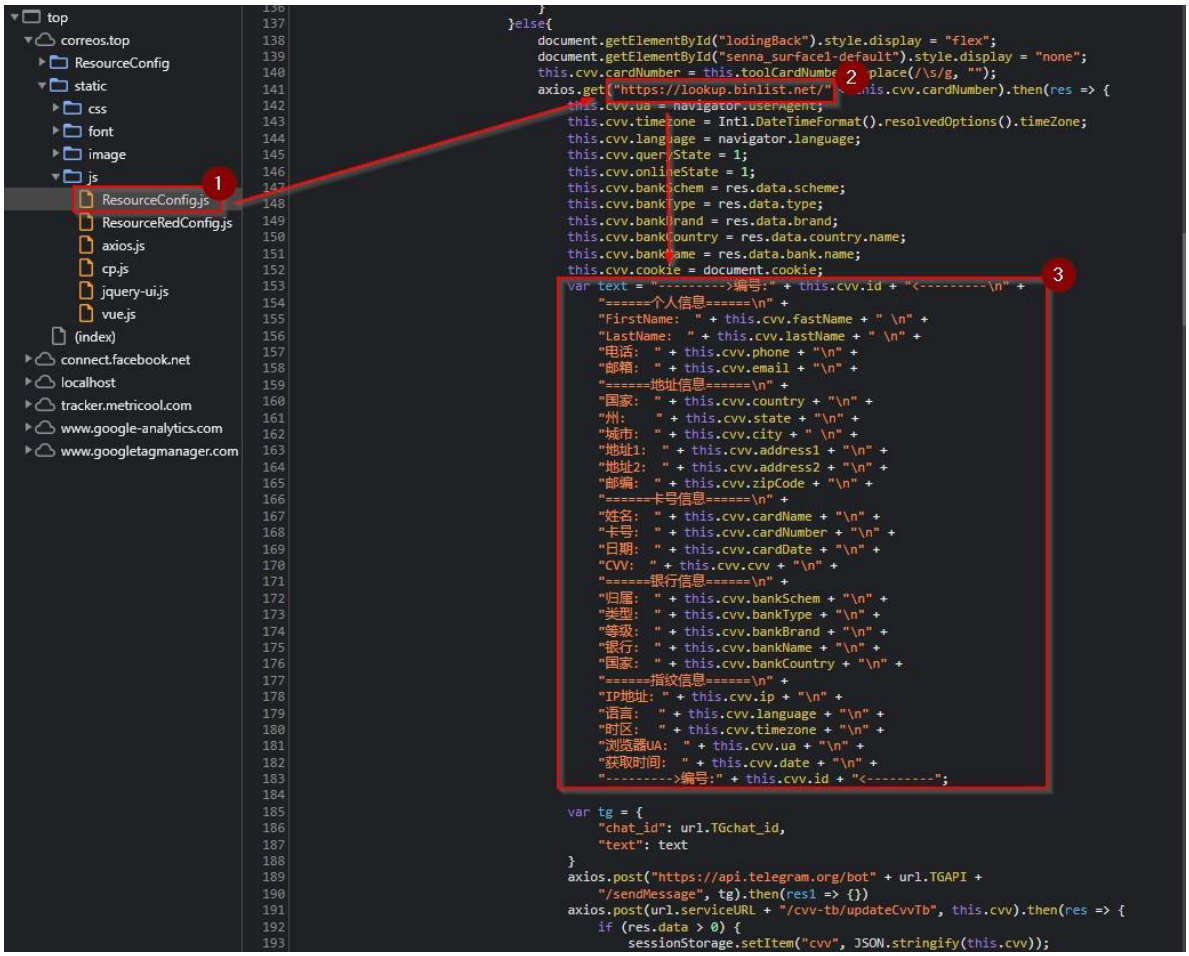
- Nombre completo
- Dirección
- País
- Correo electrónico
- IP
- Número de teléfono
- Código postal
- Nombre del banco
- Número de tarjeta
- Fecha de vencimiento de tarjeta
- Código de seguridad de tarjeta



Por otra parte, antes de proceder al canal de pago, el sitio web realiza una comprobación de que la tarjeta bancaria se encuentre dentro de sus parámetros aceptados para posteriormente hacer envío de datos al servidor de Command And Control y así generar el cobro respectivo por los canales de pago establecidos por los ciberactores.

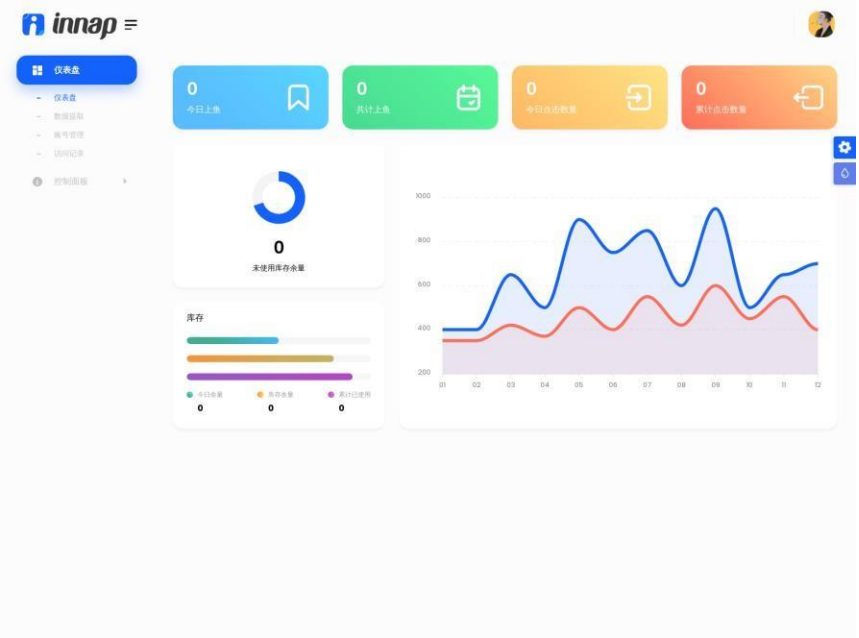
La validación de las tarjetas bancarias se realiza mediante la identificación de su BIN, obteniendo la siguiente información, mediante la API del sitio binlist.

- Tipo de tarjeta
- Banco
- Membresía
- País de emisión



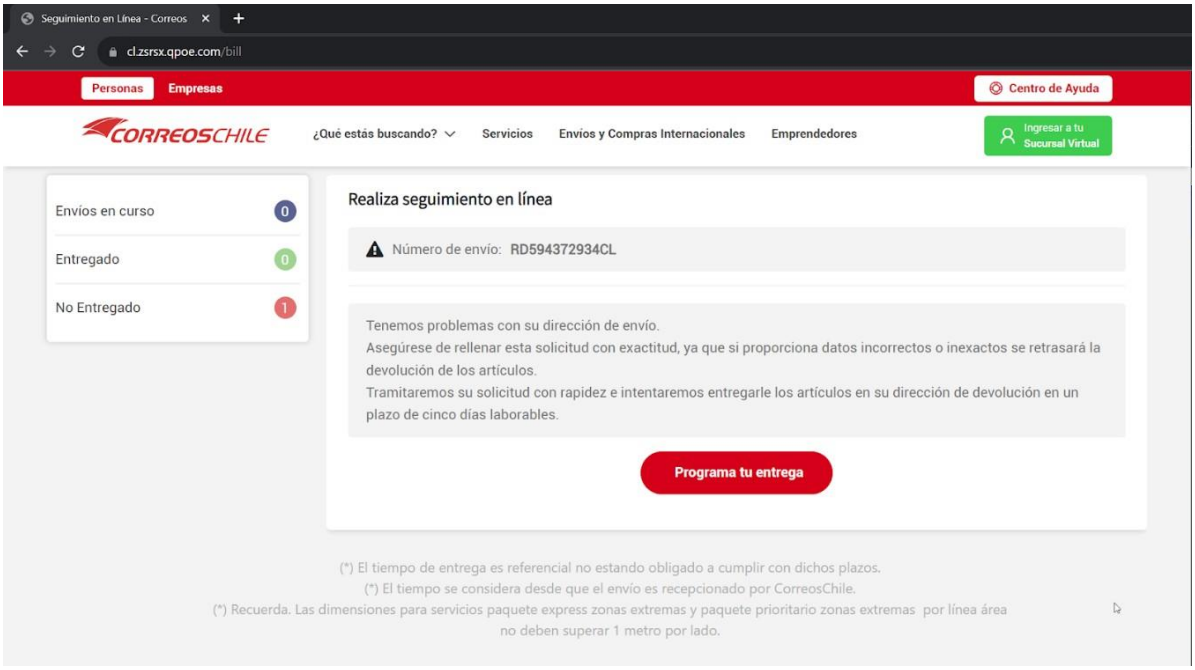
En paralelo, tras acceder a los dominios del panel de administración obtenidos, este presenta un dashboard que, si bien se encuentra todo en valor cero, en un correcto funcionamiento debiese permitir visualizar y administrar la información capturada mediante las campañas ejecutadas.

Si bien no se visualiza el panel en total funcionamiento, permite obtener una representación visual aproximada de cómo se encuentran organizados los actores detrás de este esquema de fraude.



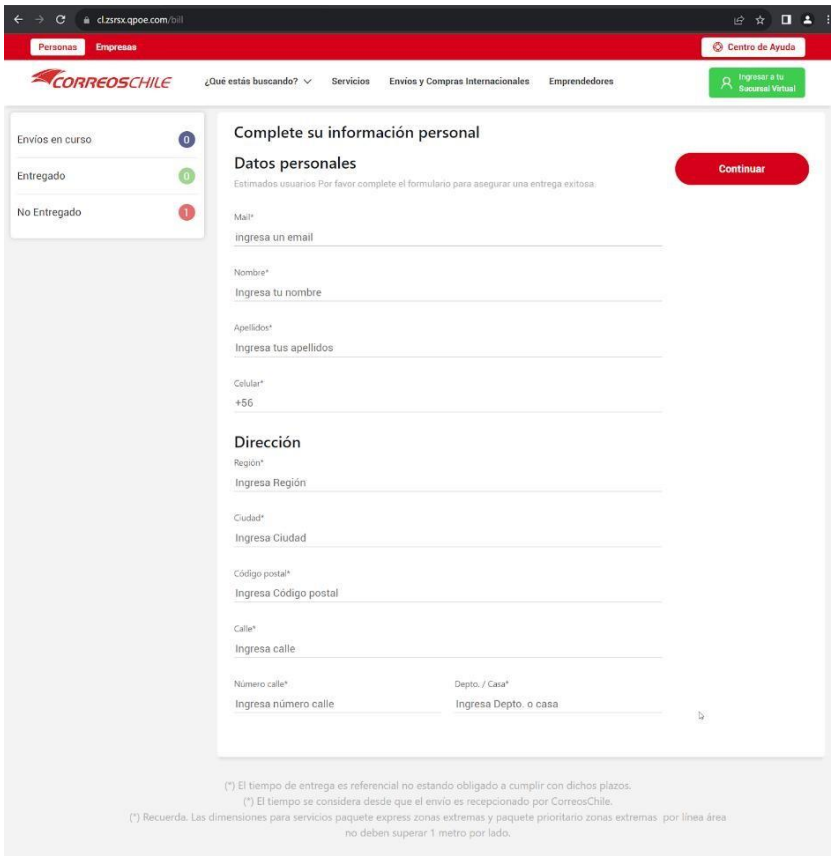
Muestra 2

Para el caso revisado durante el mes de septiembre de 2023, se observa gran similitud en el esquema anterior salvo diferencias visuales, donde se ha mejorado el aspecto, diseño y tipografía, haciéndolo cada vez más similar al sitio oficial mediante leves mejoras.

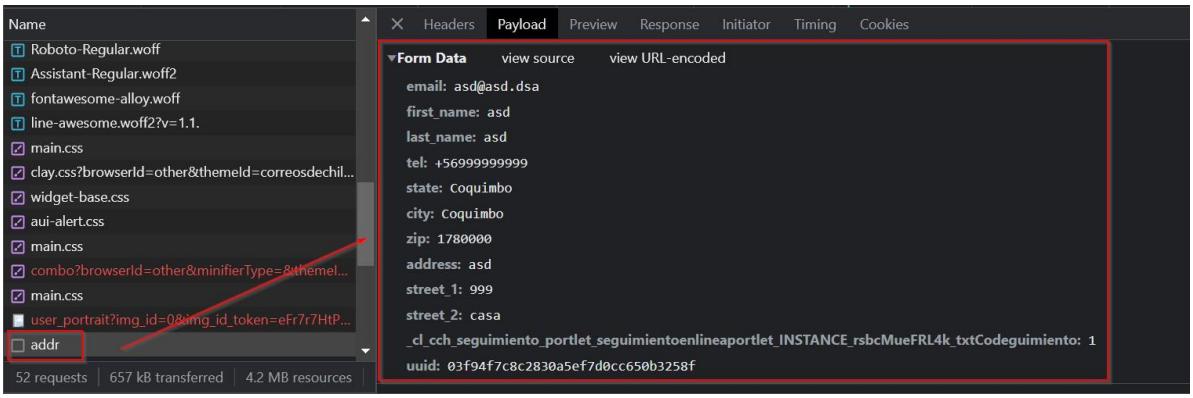


Una vez se continúa con el proceso, se solicita una gran cantidad de datos personales tal como en el análisis previo, lo que, si bien se ve con un formato legítimo, debiese saltar las alarmas y cuestionar el ¿para qué necesitan todos estos datos? Tales como:

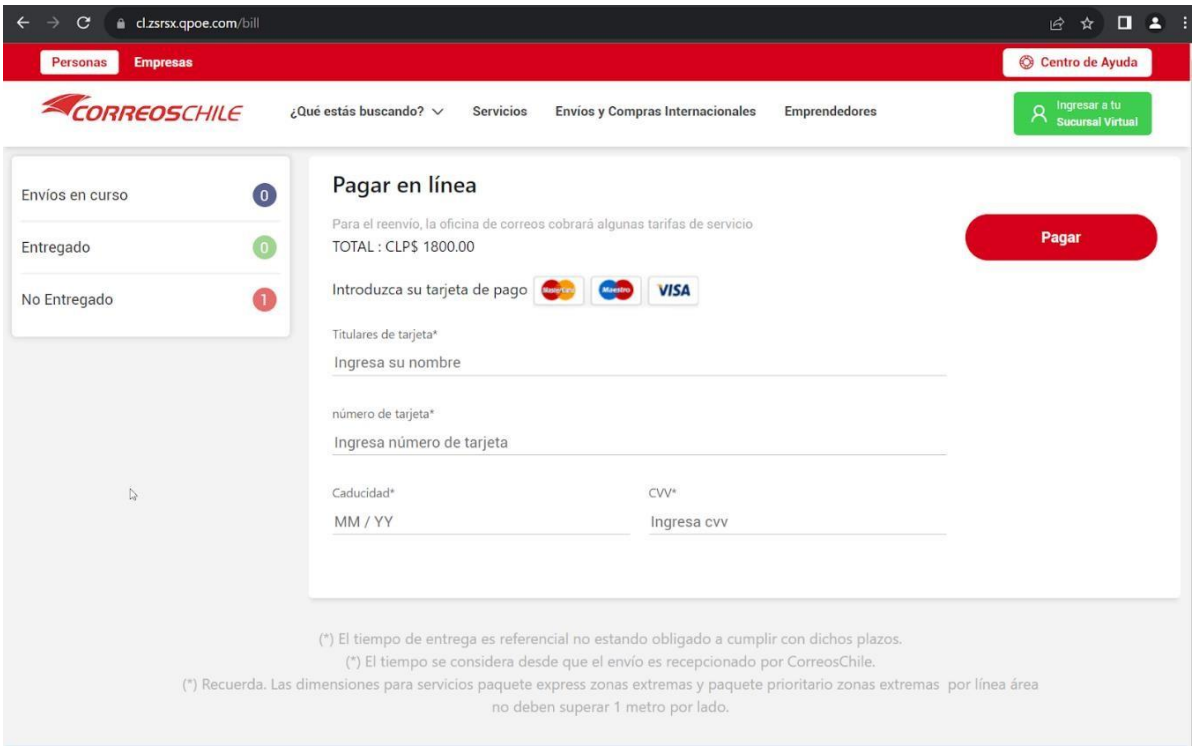
- Correo electrónico
- Nombre y apellido
- Numero de celular
- Dirección exacta



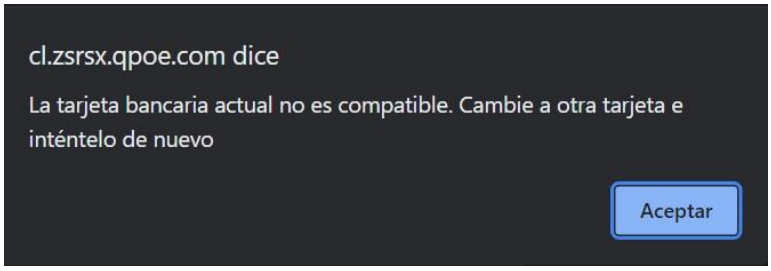
Todos estos datos se transmiten al servidor de comando y control de una manera específica. Sin embargo, a diferencia del caso anterior, en este sitio se han implementado diversas medidas de seguridad y prácticas de SecOps. Estas medidas salvaguardan la infraestructura de los actores, permitiendo una comunicación segura entre el backend y el frontend que no es detectable ni interceptable por la víctima. Esto añade un grado de realismo que incrementa las probabilidades de éxito del ataque y, simultáneamente, complica la labor de los analistas.



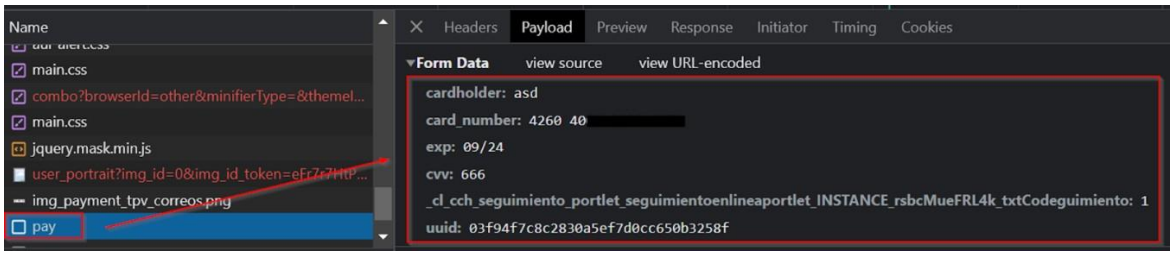
Una vez que el usuario completa los datos, el paso siguiente es la recolección de información bancaria a través de formularios. Estos no solo capturan la información, sino que también pueden verificar si los datos bancarios proporcionados son vigentes o auténticos. Si detecta alguna inconsistencia, el sistema muestra un mensaje sugiriendo cambiar la tarjeta ingresada.



Aunque podría parecer una simple validación, también es posible que sea una pseudo-validación diseñada para alentar a las víctimas a introducir múltiples tarjetas al intentar el pago. Esto incrementa significativamente el éxito del ataque y la cantidad de información obtenida, sin requerir mayores esfuerzos por parte del atacante.



Toda esta información se envía nuevamente al servidor de Command And Control, sin embargo, la única diferencia es que en el caso analizado durante junio, todos los datos capturados se enviaban en un único Payload hacia el servidor de los atacantes, mientras que en el caso actual, se envía mediante payloads segmentados bajo el nombre "addr" con datos de la dirección y bajo el nombre "pay" con los datos bancarios.



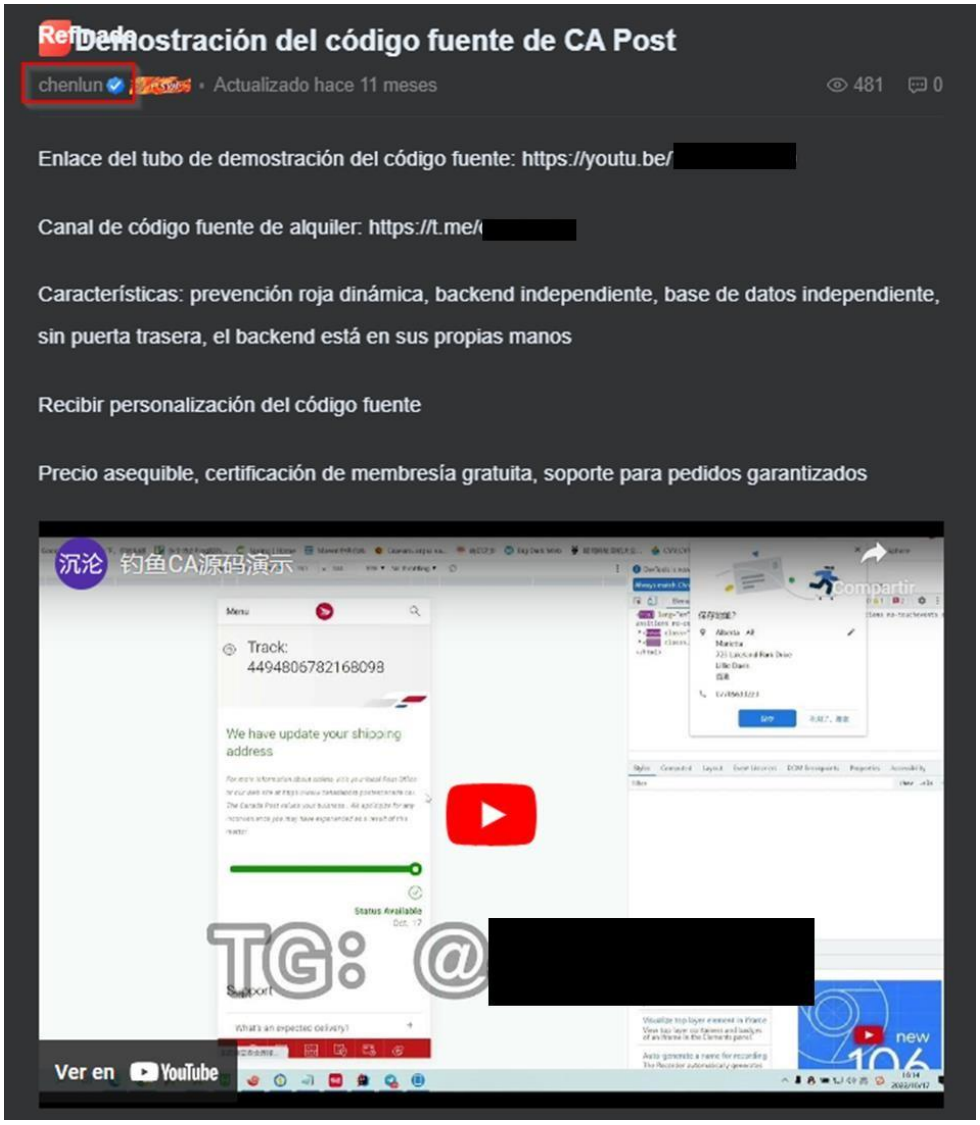
A diferencia del caso de junio, no se han logrado capturar imágenes o dominios de los paneles o sitios de login de la administración o de los servidores de command and control.

Actores de amenaza

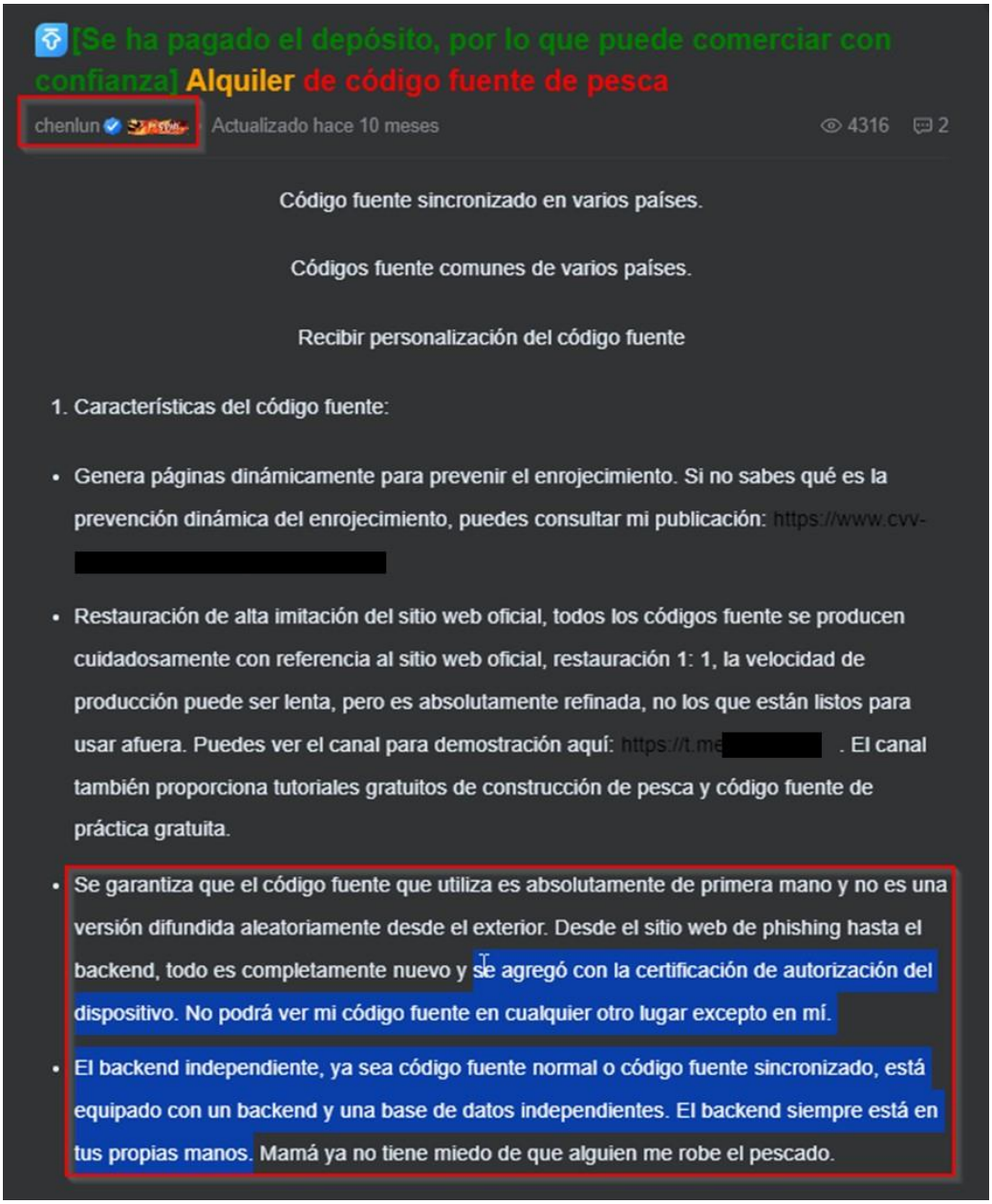
Mediante un monitoreo y seguimiento se ha logrado identificar que en uno de los sitios web fraudulentos, el sitio se encontraba firmado bajo el alias de "Chenlun" el cual tras una consulta a canales de Telegram se obtuvieron diversos resultados en idioma chino, coincidiendo con los hallazgos previos.

De esta forma, mediante la revisión de los canales del actor de amenaza, se logra identificar que son proveedores de Phishing As A Service (PaaS) y que ofrecen generar una clonación personalizada con gran detalle de los sitios web que sus clientes deseen según el sector geográfico donde busquen desplegarse.

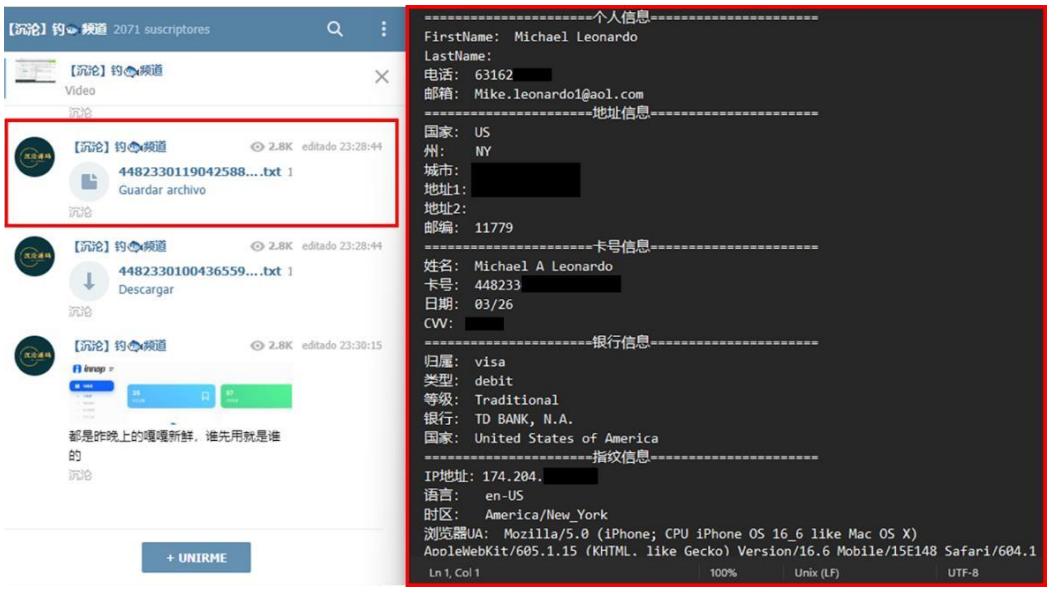
Debido a esto es que los actores cuentan con diferentes recursos audiovisuales para acompañar a sus clientes en el proceso de creación y despliegue de la campaña, ya que ellos sólo brindan el sitio web de fraude y el panel de administración enseñado anteriormente.



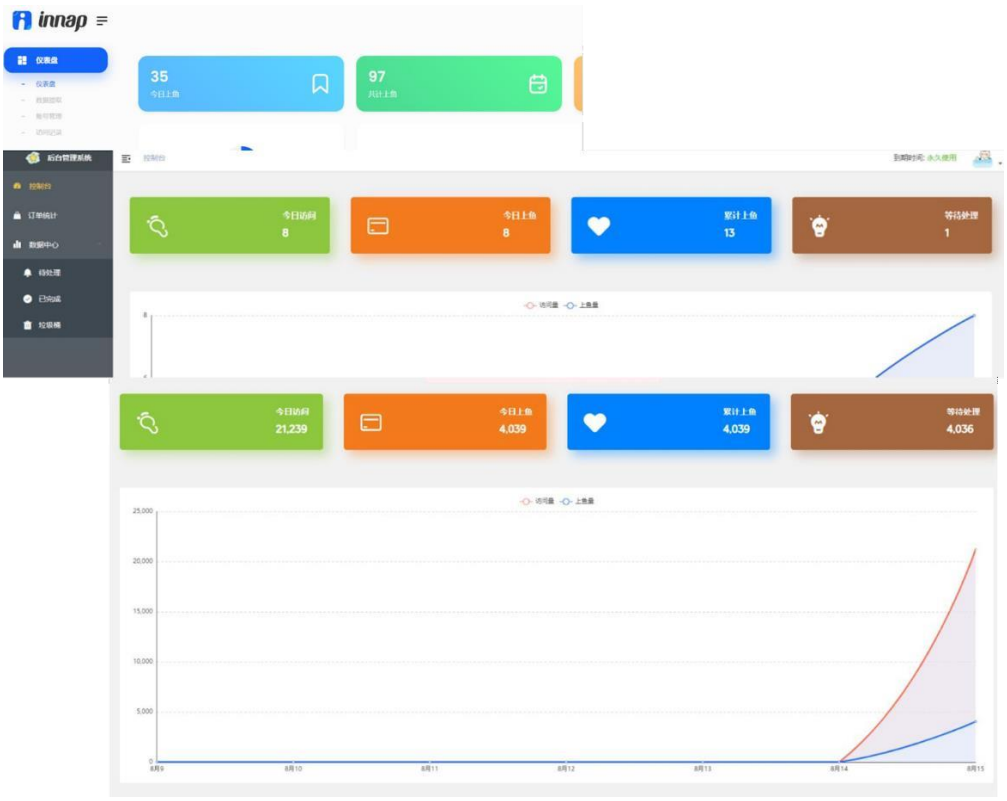
Asimismo, en sus canales se comunica sobre el continuo desarrollo de sus operaciones, mencionando las capacidades de ocultamiento y SecOps que se han identificado en la muestra 2.

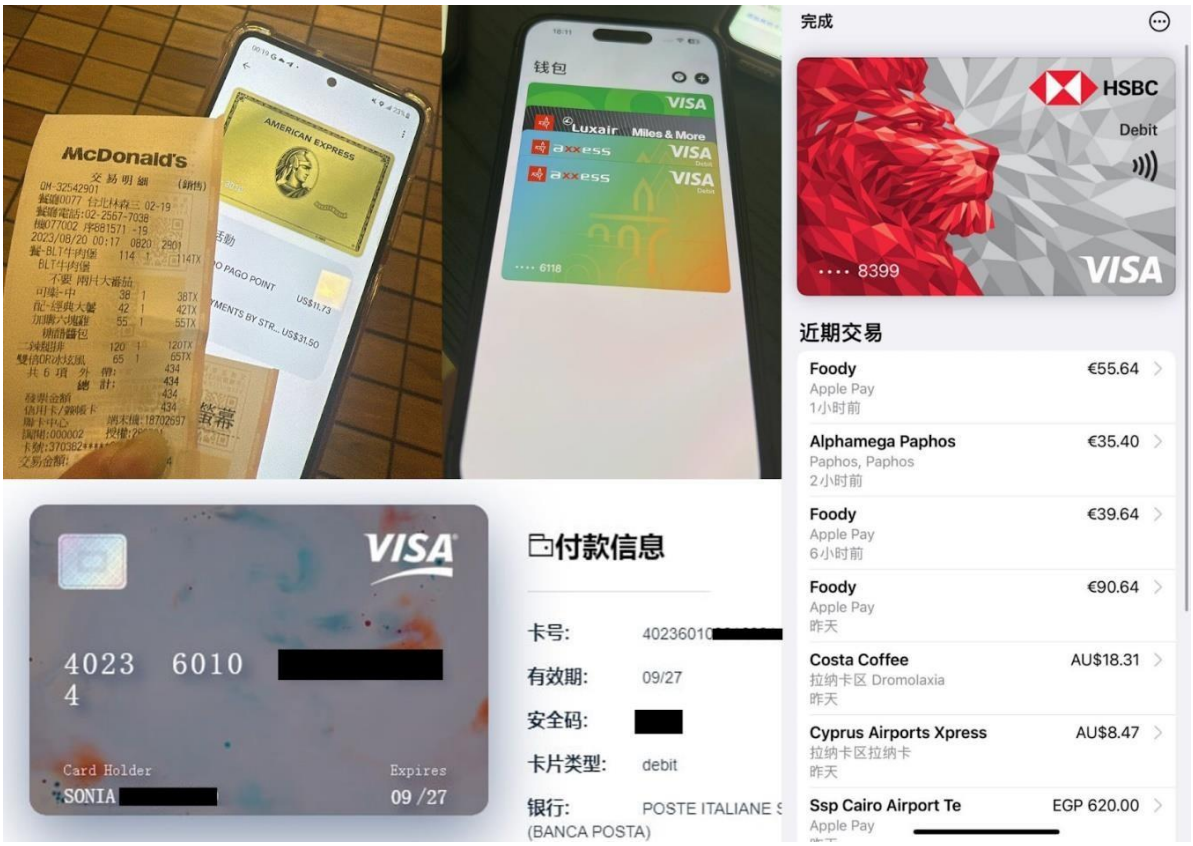


Adicionalmente, entre los canales de comunicación y de compartimentaje de información de sus clientes/afiliados, es posible obtener diferentes filtraciones capturadas a modo de muestra, para entregar confianza y seguridad a quienes deseen contratar los servicios de este grupo de actores, los que vienen con el mismo formato de los Payload de los sitios web hacia sus servidores de comando y control y canales de Telegram.



Por otra parte, mediante información compartida por los mismos clientes es posible obtener capturas de pantalla de paneles de administración con estadísticas de las capturas junto a usuarios que evidencian estar usando tarjetas bancarias de terceros, principalmente mediante billeteras digitales ofrecidas por teléfonos móviles.





Si bien no se ha logrado perfilar al creador o administrador de este servicio de phishing, si se han identificado diferentes canales oficiales de contacto tanto con los administradores como con otros usuarios, los que se detallan a continuación:

- hxxps://t.me/ChenlunConsultBot - Bot de consultas
- hxxps://t.me/chenlun - Chat administrador
- hxxps://t.me/chenlunjl - Chat de comunidad
- hxxps://t.me/chenlunjx - Muestras de tarjetas capturadas
- hxxps://t.me/chenlunvip - Canal de clientes
- hxxps://www.youtube.com/@user-ty4zn3fr3s – Tutoriales de Youtube
- hxxps://wentogov.xyz/WhLrVs - Foro Chino
- hxxps://www.cvv-goods.com/author/521 - Foro Chino

Apreciación

De acuerdo a lo observado durante el presente documento, es posible evidenciar una constante alza y sofisticación en campañas de phishing, que pese a ser disponibilizada por un actor principal, este ha generado que sus clientes hayan llevado a la creación de una infraestructura de grandes dimensiones exclusivamente dedicada al fraude, que otorga un fácil y rápido despliegue para aquellos que por falta de tiempo y/o conocimiento no pueden desarrollar por sí mismos, de esta forma se ha creado una ola de smishing alrededor del mundo y que cuenta con múltiples cabezas en donde detener una, no bastará para detener el esquema completo, si no que se deben dirigir los esfuerzos en detener al proveedor del servicio.

En esta misma línea, es importante concientizar a los usuarios o colaboradores para evitar caer en este tipo de campañas de fraude, donde el único motivo para mantenerse vigentes, es debido a que sus resultados son altamente lucrativos y se encuentran dados debido a la brecha digital, en donde si bien la gran parte de la población cuenta con un dispositivo móvil en sus manos, no comprenden el real significado de la seguridad digital y de la protección de la información personal, logrando que actores levemente más avanzados sean capaces de capturar información suficiente para realizar tanto suplantaciones de identidad como fraude.

En este punto es importante dimensionar cómo y a quién se le genera el daño por estos actos, ya que para los atacantes es más fácil engañar a la gente común y corriente que vulnerar un banco o un sitio web de compras para obtener la misma información, siendo el usuario el único afectado ya que según la legislación Chilena, el banco solo se hace responsable si se han vulnerado sus sistemas (plataformas digitales, cajeros automáticos u otros), mientras que si la víctima entrega sus datos voluntariamente sea o no bajo la premisa de un engaño, es el usuario el único responsable de la sustracción o uso de sus fondos.

Con estos antecedentes, entendiendo los esfuerzos y el nivel de sofisticación que hacen los ciberactores por llevar a cabo sus esquemas de fraude y la desventaja legislativa que acompaña a las víctimas, es importante revisar, comprobar y asegurarse adecuadamente de que el sitio desde donde se solicitan los datos personales sea la oficial, lo cual se puede llevar a cabo mediante la rápida respuesta de las siguientes preguntas y/o procedimientos.

- ¿He realizado alguna compra que involucre el envío de un paquete a mi domicilio?
- ¿El número de seguimiento corresponde al artículo que efectivamente estoy esperando?
- ¿El sitio web en el que estoy navegando es el oficial?, lo cual se puede comprobar con una simple búsqueda del servicio o sitio web a través de su motor de búsqueda preferido y así comparar este resultado con el enlace malicioso entregado desde cualquier vía de comunicación. (SMS, email, Whatsapp, otros).