FINSIN

Reporte de Phishing

Marzo 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 Marzo[1]:

¡Ahora Chile y Colombia están mucho más cerca en los porcentajes de detecciones!

Para FC-01 tenemos más de 130 detecciones que usan el mismo dominio de pasarela. ¡Y desde febrero del 2022!

El grupo FC-03, realizó un nuevo cambio de dominio pero esta vez fue a principios de abril.

El pack 0032 volvió ahora con más fuerza en marzo y al parecer lo continuaremos viendo en abril.

Después de 3 meses los controladores del canal 2 acumularon 5 millones de pesos colombianos.

Las comunicaciones internas del canal 3 de Telegram ocurren entre personas que están en tres ubicaciones diferentes.

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

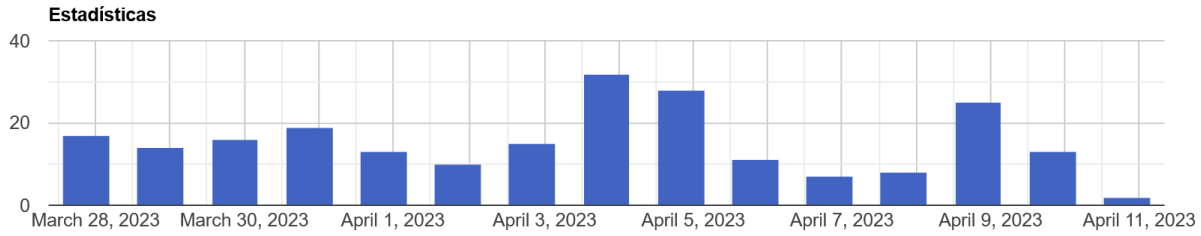
Phishing Checker

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.

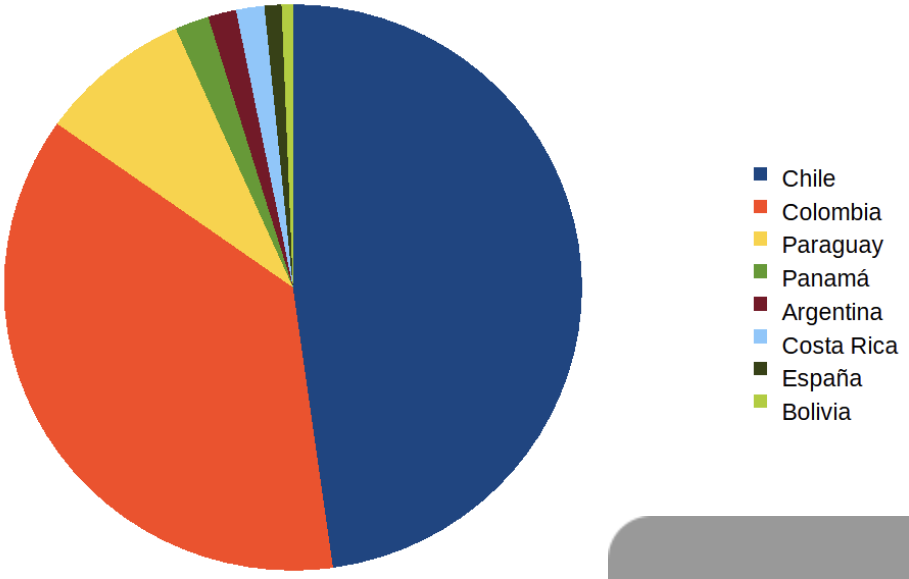
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Marzo 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 un gran cambio en las detecciones:



País	Porcentaje
Chile	47,78%
Colombia	37,03%
Paraguay	8,54%
Panamá	1,90%
Argentina	1,58%
Costa Rica	1,58%
España	0,95%
Bolivia	0,63%

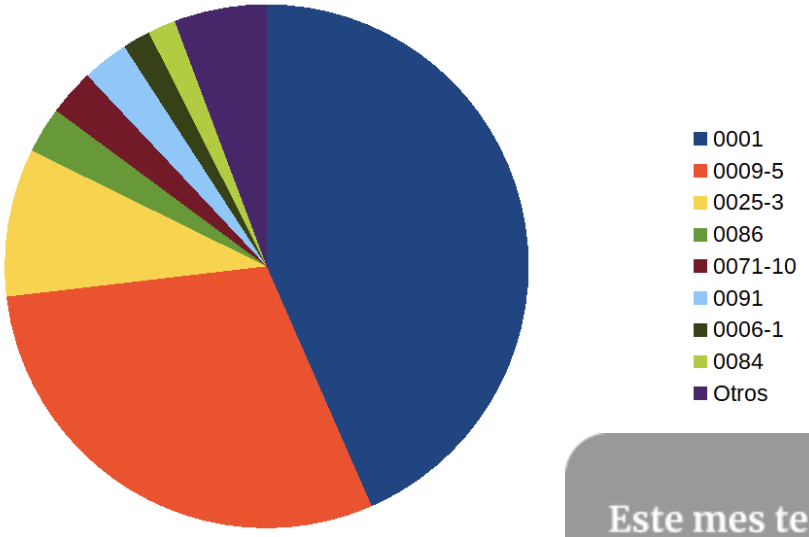
Ahora Chile y Colombia están mucho más cerca en los porcentajes de detecciones

Podemos ver que ahora Chile y Colombia están mucho más cerca en los porcentajes de detecciones, ¡nunca antes Chile había tenido menos del 65%!

Este mes aumentamos mucho las detecciones gracias a que comenzamos a realizar detecciones automáticas relacionadas con Colombia. Vamos a ampliar este punto más adelante.

Datos de kits

Si graficamos los datos del mes asociados a los kits de phishing, podemos ver que con los cambios de automatización, también cambian los pack más detectados:



Este mes tenemos una gran lista de otros con más del 20% de las detecciones.

Pack	Porcentaje
0001	39,15%
0010-2	30,07%
0025-3	17,48%
0053	9,09%
0009-5	7,69%
0071-3	5,59%
0071-9	4,20%
0086	3,50%
Otros	22,38%

Este mes podemos ver que la distribución de las detecciones está siendo mucho más homogénea que el mes anterior.

Seguimos con muchas detecciones del pack 0001, 0010-2, 0025-3 y 0009-5, pero, además, tenemos una gran lista de otros con más del 20% de las detecciones del mes.

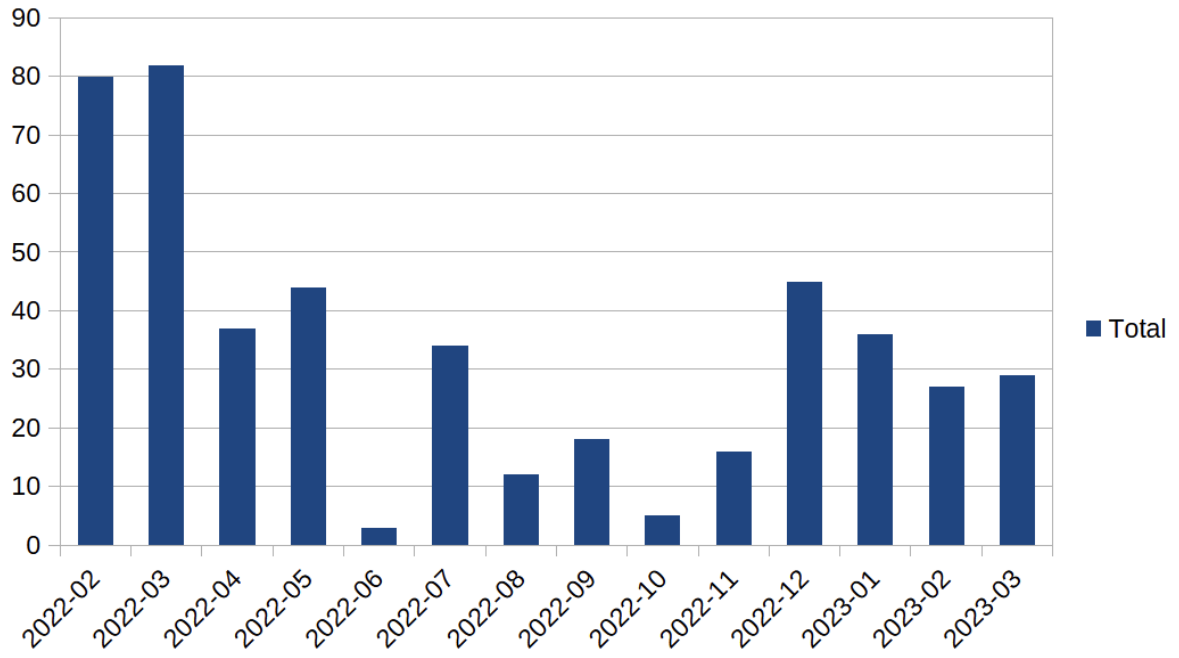
Actualización de Fishers Constantes (FC)

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[2], 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:



Como vemos, estos últimos meses han estado un poco estancados levantando alrededor de 30 sitios "solamente" por mes este 2023.

Lo interesante es que el comportamiento del grupo lo hemos monitoreado principalmente a través de los mismos links que se han mantenido en el tiempo.

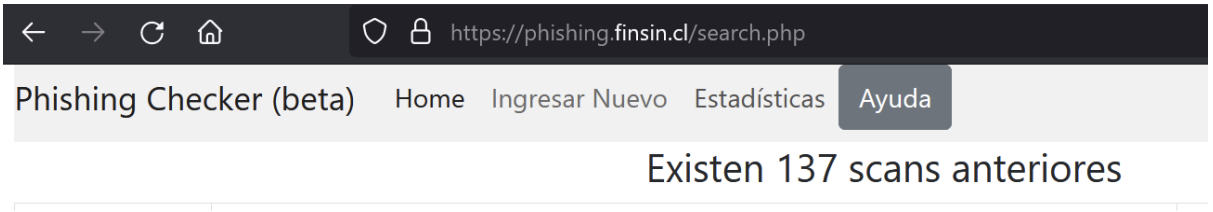
[2] Este grupo fue definido en el reporte de febrero del 2022: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/

Como lo habíamos visto anteriormente, tenemos que este grupo usa una estructura de varias capas para ocultar su funcionamiento, por ejemplo, usando una de las detecciones[3] tenemos que:

N° Redirección	URL Redirección
0	https://bit.ly/3DtqzqY?l=www.bancoripley.cl
1	https://sam-tech.jp/bancoripley/cuenta-cokr/
2	https://web.bancoripley.cl.hokonuipioneervillage.co.nz/
3	https://web.bancoripley.cl.hokonuipioneervillage.co.nz/1680278956/Login

Ahora simplificaron las capas usadas para solamente usar una intermedia, la del pack 0006-1 de redirección que pasa por el dominio: "sam-tech.jp". De hecho todas las detecciones del mes pasan por el mismo dominio, hasta usando distintas URL de acortadores de bit.ly usan el mismo dominio de redirección.

Pero este dominio nos es muy familiar, de hecho si ponemos en la búsqueda de nuestra plataforma[4], podemos encontrar el historial de detecciones que hayan pasado por ahí, y vemos que son muchísimas.



Al momento de escribir este reporte tenemos más de 130 detecciones que usan el mismo dominio, ¡y comenzando desde febrero del 2022!

Este es un dominio de pasarela que lo han usado hace mucho tiempo y lo siguen usando, de hecho, lo detectamos en febrero y marzo del 2022, luego no lo usaron más hasta diciembre del mismo año, donde retomaron su uso hasta ahora.

Tenemos más de 130 detecciones que usan el mismo dominio.
¡Y desde febrero del 2022!

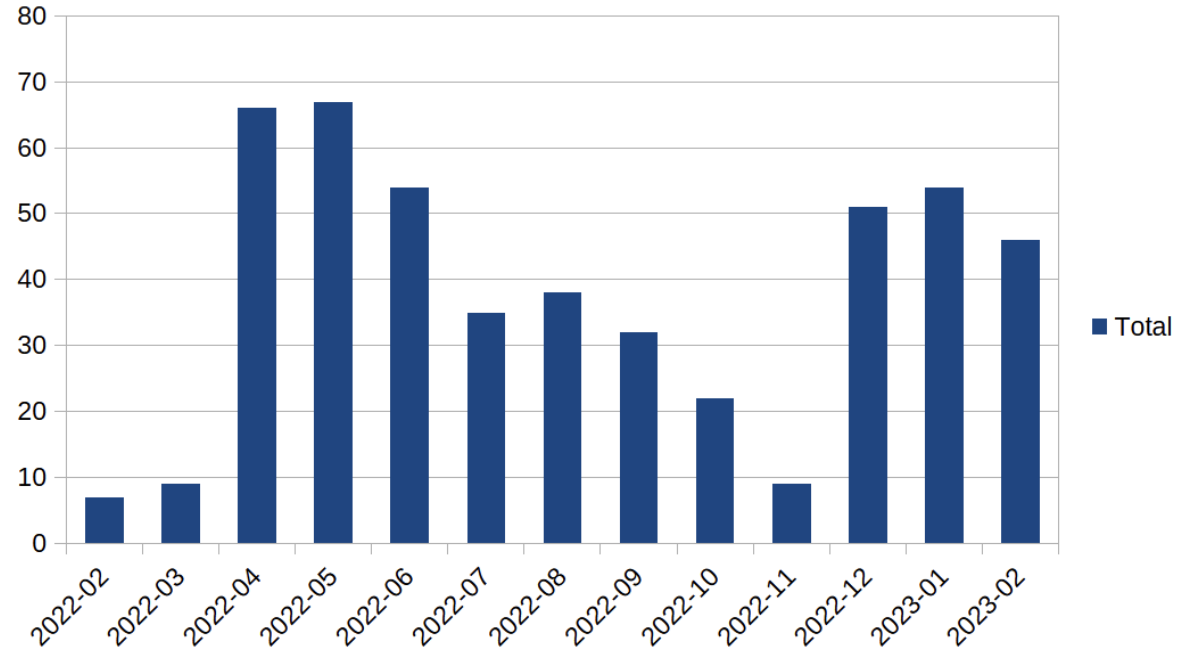
Les recomendamos a los afectados por este grupo que busquen el takedown de este dominio para por lo menos "incomodar un poco" al grupo y aumentar sus costos, al tener que usar algún otro como pasarela.

[3] https://phishing.finsin.cl/list.php?query=3a35190573354442 01d7e07ec9238b57ca37f3e8eeae689b9bbb73da53c3c30b

[4] https://finsin.cl/plataforma-phishing-checker/#1-1-busqueda

FC-03

Como ya vimos en un reporte anterior[5], 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 están siendo muy parejas.



En estos últimos meses se están estancando, y según lo que hemos podido detectar es por el comportamiento errático de las detecciones. Al igual que el mes pasado, el comportamiento extraño es porque no están siendo constantes, algunos días aparecen y otros no.

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:

2023-03-02	0009-5	https://edohello.info
2023-03-06	0009-5	https://edohello.info
2023-03-08	0009-5	https://edohello.info
2023-03-11	0009-5	https://edohello.info
2023-03-17	0009-5	https://edohello.info

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

2023-03-22	0009-5	https://edohello.info
2023-03-23	0009-5	https://edohello.info
2023-03-26	0009-5	https://edohello.info
2023-03-28	0009-5	https://edohello.info
2023-03-29	0009-5	https://edohello.info
2023-03-30	0009-5	https://edohello.info
2023-04-01	0009-5	https://edohello.info
2023-04-02	0009-5	https://edohello.info
2023-04-03	0009-5	https://edohello.info
2023-04-04	0009-5	https://r4gn4r0kr4.dinamics.info
2023-04-05	0009-5	https://r4gn4r0kr4.dinamics.info

Podemos ver que durante todo marzo mantuvieron el mismo dominio de febrero: edohello.info.

El grupo FC-03, realizó un nuevo cambio de dominio pero esta vez fue a principios de abril.

Agregamos las detecciones de los primeros días de abril porque nuevamente hicieron un cambio en el dominio del C2, pero esta vez fue a principios de abril, y volvieron a las "andanzas anteriores", porque ahora están usando el subdominio r4gn4r0kr4 del dominio dinamics.info.

Esto es muy similar a lo identificado en el mes de febrero (en donde era r4gn4r0kr4.edoblog.info) y en otros meses anteriores que tenían prefijos similares. Quedará para investigaciones posteriores si existe algo más ahí.

Ahora, si buscamos los dominios de C2, pero en las variantes del pack 0010 tenemos que reaparecieron este mes con fuerza, pero a finales de mes:

2023-03-23	0010-5	https://new-falav2.edoblog.info
2023-03-28	0010-5	https://new-falav2.edoblog.info
2023-03-29	0010-5	https://new-falav2.edoblog.info
2023-03-30	0010-5	https://new-falav2.edoblog.info
2023-03-31	0010-5	https://new-falav2.edoblog.info

2023-04-01	0010-5	https://new-falav2.edoblog.info
2023-04-02	0010-5	https://new-falav3.edoblog.info
2023-04-03	0010-5	https://new-falav2.edoblog.info
2023-04-03	0010-5	https://new-falav3.edoblog.info
2023-04-04	0010-5	https://falav2.dinamics.info

Acá tenemos una “variación”, el C2 del pack 0009-5 por buena parte de febrero y por todo marzo era el c2 edohello.info, pero en marzo (y principios de abril), el C2 para el pack 0010-5 era parte del dominio edoblog.info (un C2 antiguo de 0009-5). A veces usando el subdominio “new-falav2” y otras veces el “new-falav3”

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 2023-04	edohello.info y edoblog.info
2023-04 a la actualidad	dinamics.info

El dominio dinamics.info, sigue siendo un dominio registrado en namecheap, y usan las mismas IPs (66.29.146.71), aunque como están usando un hosting, no se puede marcar a esa IP como completamente maliciosa.

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.

Pack 0032

Este mes queremos presentar un pack, que afecta a personas de Chile y aunque no es tan nuevo, hemos visto un resurgimiento estas últimas semanas.

De hecho, lo habíamos visto en la primera mitad del 2022 y luego había desaparecido de nuestro radar. Ahora volvió con más fuerza en marzo y al parecer lo continuaremos viendo en abril.

Queremos mostrar este pack para que podamos hacer algo más, aun cuando no siempre tengamos toda la información.

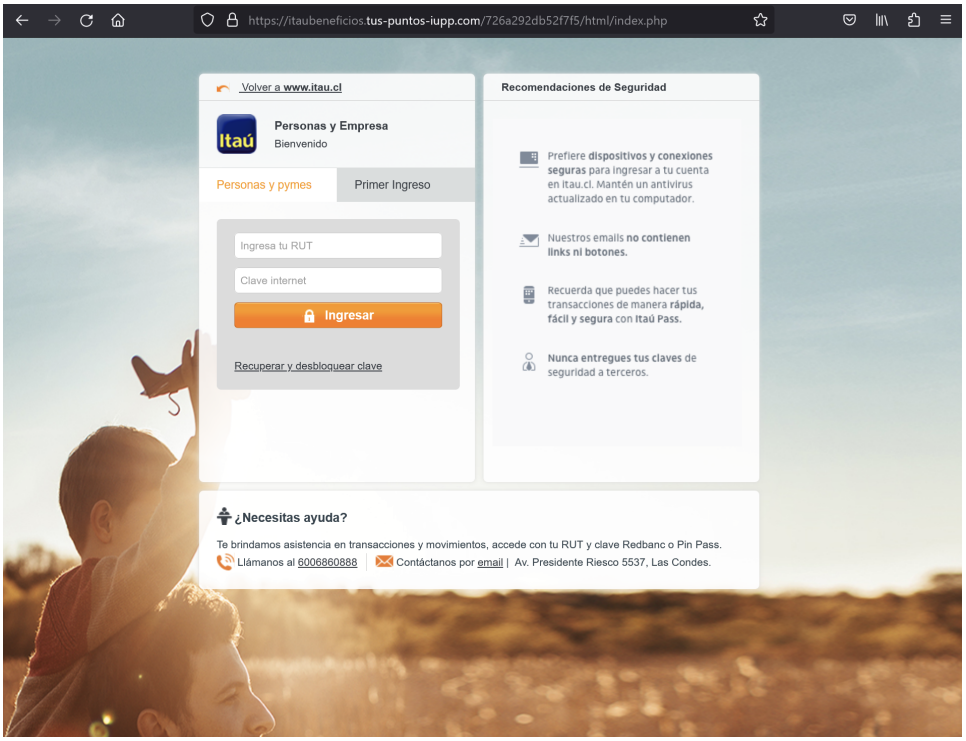
Tenemos la gran sospecha de que este pack fue desarrollado por brasileños para un banco de ese país, y lo adaptaron para atacar a las personas en Chile.

El pack 0032 volvió ahora con más fuerza en marzo y al parecer lo continuaremos viendo en abril

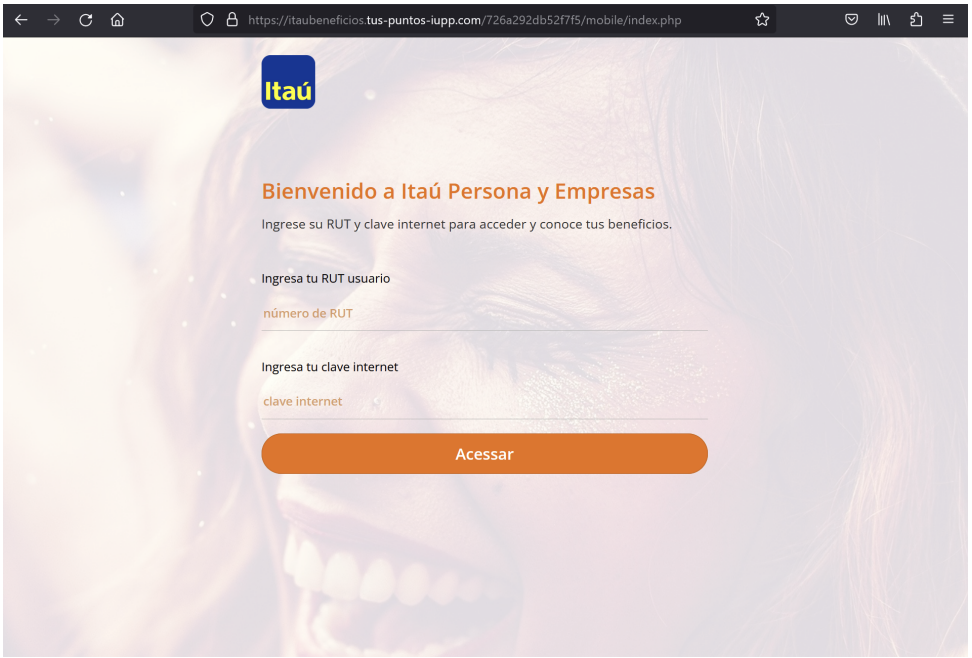
Inicio

Este pack comienza con una revisión del tipo de dispositivo que uno está usando para entrar al sitio y dependiendo de eso te redirige a lo siguiente:

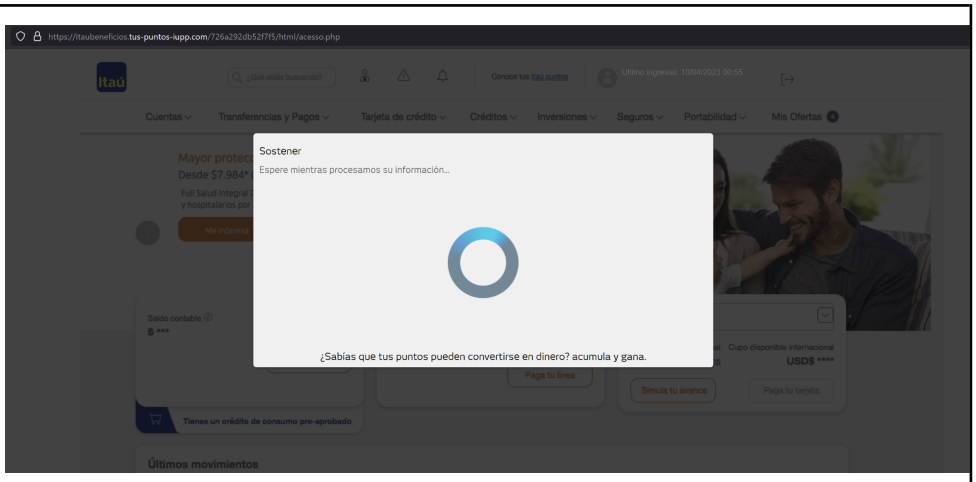
Escritorio: [dominio]/726a292db52f7f5/html/index.php



Smartphone: [dominio]/726a292db52f7f5/mobile/index.php



Y aunque los destinos sean distintos, tienen un mismo comportamiento, si es que uno sigue ingresando datos tenemos que se queda pegado en la ruta "726a292db52f7f5/[html o mobile]/api.php", similar a esto:

Escritorio	
Smartphone	

Un detallito interesante, es que el título de la barra es distinto para ambos formatos: para la página de escritorio es simplemente "~" y para la página de dispositivos móviles (que generalmente no se muestra en los celulares) dice "Tudo pra você" ("todo para tí" en portugués).

Para dejar a la persona "pegada" en el sitio mientras los controladores pueden validar la cuenta (RUT y clave) el kit fuerza recargar la página a través de un código html.

```
<div class="container all_content">
    <div class="content">
        <br>
        <br>

        <center>
            <div class="ms_content">
                <meta http-equiv="refresh" content=6;url="acesso.php"><div class="block_loading">
    <div class="block_title">

            <span class="headline">Sostener<b> </b></span>
        <p class="description">Espere mientras procesamos su información...
</p>
    </div>
```

Este código hace que la página se recargue cada 6 segundos e invoque el script en acesso.php. En nuestro caso, como nosotros colocamos datos no-válidos, la página se queda dando vueltas en ese loop.

Al hacer esto le da tiempo a los operadores (los que están trabajando por detrás recibiendo las claves de las víctimas) para que actúen y validen estas credenciales en el sitio real del banco.

Luego de ese paso, asumimos que ellos quieren validar el segundo factor o las demás herramientas de seguridad del banco, pero no pudimos revisarlo directamente.

Si revisamos los archivos expuestos en el servidor web para ambas "carpetas"[6] vemos que tenemos subcarpetas con listado de directorios:

- /726a292db52f7f5/html/2_files/
- /726a292db52f7f5/mobile/f/

Aquí solo logramos encontrar algunos flujos validados en javascript que podemos asumir que luego pide el valor del SMS enviado por el banco, por ejemplo, en el siguiente archivo "/726a292db52f7f5/mobile/f/javascript.js"

[6] El "directory scanning" es la prueba 1 a 1 (con herramientas) de los archivos más comunes

```
function val_sms(){
    var sms = $('#inp_sms').val();

    if(sms.length < 4){
        alert("El código SMS ingresado no es válido. ¡Inténtalo de nuevo!");
        $('#inp_sms').val('');
        $('#inp_sms').focus();
        return false;
    }else{
        $('.button_enter').removeClass('btn_all').addClass('btn_disabled').attr('disabled', 'true');
        $('.loader_small').css('display', 'block');
        return;
    }
}

function val_fone(){
    var fone = $('#inp_fone');

    if(fone.val().length < 12){
        alert("El número de teléfono ingresado no es correcto. ¡Inténtalo de nuevo!");
        fone.val('').focus();
        return false;
    }else{
        $('.button_enter').removeClass('btn_all').addClass('btn_disabled').attr('disabled', 'true');
        $('.loader_small').css('display', 'block');
        return;
    }
}
```

¿Cómo sabemos que hay un flujo de los operadores por detrás?

¿Cómo sabemos que están esperando a validar esas credenciales?

Lo veremos a continuación.

Panel de administración

Si hacemos una revisión de "rutas conocidas" en el servidor encontramos que tenemos algo interesante en la ruta: /operador/. En esta ruta podemos encontrar lo siguiente:

Efectivamente podemos ver que tenemos el portal de acceso al panel de control, pero lamentablemente no sabemos las contraseñas, si es que tienen alguna.

Entonces tenemos algunos caminos, como intentar forzar la contraseña o intentar algún tipo de inyección SQL, pero tenemos una forma más sencilla de obtener información, seguir identificando los archivos de esta nueva carpeta.

El primer archivo interesante es el ".DS_Store", que es un archivo que agrega los sistemas operativos MacOS para saber qué archivos están descritos en la carpeta[7]. Cuando uno comprime una carpeta en este sistema operativo se comprimen todos los archivos, y también comprime el .DS_Store.

Lo interesante del archivo es que justamente nos da información de que el atacante en algún momento comprimió la carpeta del kit de phishing en un sistema operativo MacOS, y además gracias al trabajo de otros investigadores[8] podemos "abrir" el archivo y que nos liste los archivos más importantes.

[7] https://en.wikipedia.org/wiki/.DS_Store
[8] https://0day.work/parsing-the-ds_store-file-format/

Usando entonces una herramienta como la siguiente[9] podemos analizar el archivo y ver que tenemos una carpeta llamada _sound (porque se repite y porque no tiene extensión) y varios archivos.

```
root@kali:~/Python-dsstore# python3 main.py samples/itau_0032_scam_dsstore
Count:  10
_sound
_sound
_sound
acesso.php
add-user.php
down.php
edite-user.php
index.php
lista-clientes.php
lista-infos.php
```

Ahora nos queda validar si es que de verdad tenemos esos archivos "interesantes":

Ruta	Código HTTP	Tamaño	Redirección
/operador/acesso.php	302	28KB	index.php
/operador/add-user.php	500	1KB	
/operador/down.php	200	0B	
/operador/edite-user.php	200	722B	
/operador/index.php	200	2KB	
/operador/lista-clientes.php	500	395B	
/operador/lista-infos.php	500	355B	

Lo interesante es que sí, son visibles dentro de la estructura real de la carpeta, pero además que los archivos sí tienen contenido, y los más interesantes son justamente los que NO retornan el código HTTP 200.

Los archivos interesantes son justamente los que NO retornan el código HTTP 200

Si vemos con detención los archivos que tiran error 500, tenemos que los archivos traen información interesante, pero sin contexto, solamente traen el formato de una tabla, pero nada más.

[9] https://github.com/gehaxelt/Python-dsstore

Por ejemplo, en el archivo lista_clientes.php:

```
<table width="100%" border="0" cellspacing="5" cellpadding="5" class="table_lista_clientes">
    <thead>
        <tr>
            <td>IP:</td>
            <td>Data:</td>
            <td>Tipo:</td>
            <td>RUT:</td>
            <td>SENHA:</td>
            <td>Nome:</td>
            <td>TELEFONE:</td>
            <td>CORDENADAS</td>
            <td>ITOKEN:</td>
            <td>SMS:</td>
            <td>E-MAIL:</td>
            <td>C-C:</td>
            <td>Comando:</td>
            <td>Gerenciar</td>
        </tr>
    </thead>
```

Lo más interesante es cuando observamos el archivo que supuestamente fuerza la redirección: acesso.php

```
<meta http-equiv="refresh" content=5;url="acesso.php"><!DOCTYPE html>
<html>
<head>
```

Vemos que inicialmente tiene contenido, y no solo eso, sino que usa el mismo truco de la "redirección a sí mismo" para actualizar el sitio con las nuevas víctimas. Pero tenemos muchos datos más en el mismo archivo como:

```
    <thead>
        <tr>
            <td>IP:</td>
            <td>Data:</td>
            <td>Tipo:</td>
            <td>RUT:</td>
            <td>SENHA:</td>
            <td>Nome:</td>
            <td>TELEFONE:</td>
            <td>CORDENADAS</td>
            <td>ITOKEN:</td>
            <td>SMS:</td>
            <td>E-MAIL:</td>
            <td>C-C:</td>
            <td>Comando:</td>
            <td>Gerenciar</td>
        </tr>
    </thead>
```

Esta es la definición de las celdas de la tabla de las víctimas, las cuales por nuestra conveniencia las podemos ver un poco más adelante:

```
<tr>
    <td>190.22.30.33</td>
    <td>2023-04-10 00:50:11</td>
    <td>D. Fisico</td>
    <td>123456785</td>
    <td>1234</td>
    <td></td>
    <td></td>
        <td></td>
    <td></td>
    <td></td>
    <td></td>
    <td> <br>  <br><br></td>

    <td style="color:red;font-weight:bolder;">OFFLINE</td>
    <td><a href="acesso.php?gerenciar_fisi=643382ab51ea5" class="manage_user_link"><i class="fa fa-cog"></i></a></td>
</tr>
```

¡Es real! Aunque nos fuercen la redirección, igual nos muestran todas las víctimas que están manejando en ese momento.

Aunque nos fuercen la redirección, igual nos muestran todas las víctimas que están manejando en ese momento.

Tenemos la definición de: la IP origen del cual se conectó la víctima, la fecha, el RUT, la clave, y todos los demás datos que se hayan podido obtener.

Y otro dato interesante es que nos muestran las funcionalidades que internamente pueden realizar los operadores. Como sabemos que cada usuario se queda en un loop esperando el siguiente paso, en el menú de operador pueden enviar el paso siguiente que necesiten . Por ejemplo:

- Mostrar la página que pide la tarjeta de coordenadas
- Mostrar la página que pide el número de teléfono para enviar el SMS
- Mostrar la página que pide el código enviado por SMS

Aunque no hemos interactuado directamente con el kit (con el código PHP) para poder saber exactamente si estamos en lo correcto, es una buena aproximación de cómo controlan a las víctimas.

Entonces... ¿Qué podemos hacer?

Si sabemos que tenemos un listado de víctimas actuales (las que no han parseado todavía) en la ruta acesso.php, podemos estar monitoreando esta ruta para tener las víctimas que están cayendo en este kit.

Esto no lo estamos haciendo automáticamente hoy en día, y se lo dejamos a los potenciales afectados, o a las policías para que las puedan monitorear. Pero es una buena vía para saber a quienes van a tener que contactar para los planes preventivos de mitigación.

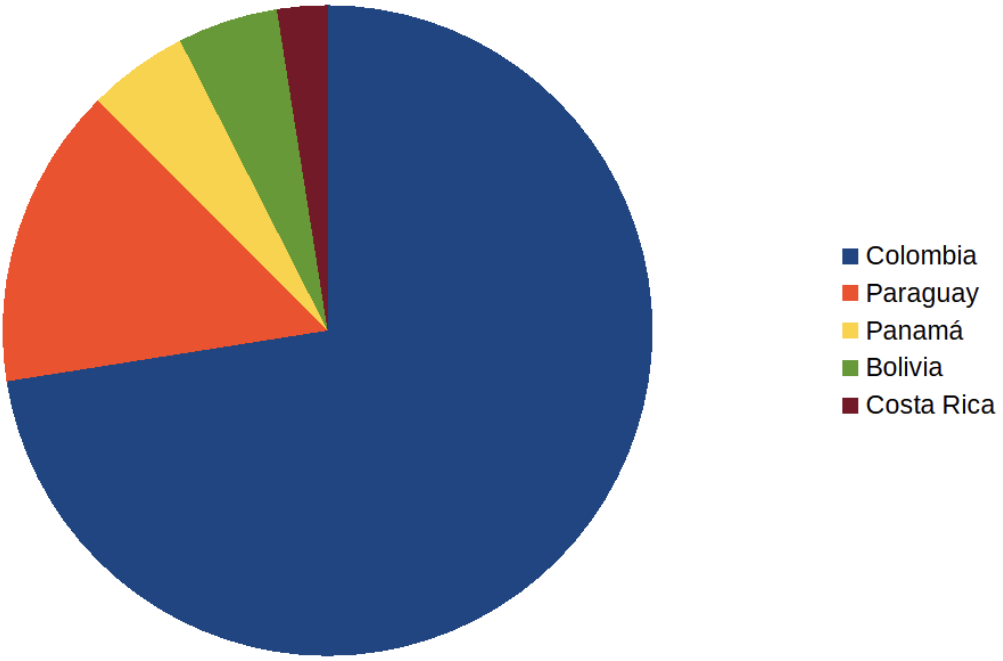
Revisando un poco, siempre tenemos más cosas que hacer.

Actividad en Telegram

Según nuestras detecciones, muchos de los packs de phishing están usando Telegram como medio para poder comunicar las credenciales obtenidas 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 mantener lo que estuvimos viendo en reportes anteriores[10][11], si revisamos todos los canales de Telegram que encontramos en los distintos sitios de phishing del mes 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.

[10] https://finsin.cl/2023/01/13/reporte-mensual-de-phishing-diciembre-2022/
[11] https://finsin.cl/2023/03/13/cumplimos-1-ano-de-reportes-de-phishing/

¿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.

Durante este mes hemos detectado bots que se publican información en los distintos tipos de chats:

Tipo Chat	Cantidad
Chats Privados	32
Grupos	5
Supergrupos	0
Canales	3

Curiosamente, ninguno de los bots se comunica con más de un chat.

Curiosamente, ninguno de los bots se comunica con más de un chat y un 80% de éstos son privados.

La gran mayoría de los bots más activos que hemos detectado, es decir, que están asociados a varias urls de phishing, tiende a centrarse en una sola institución.

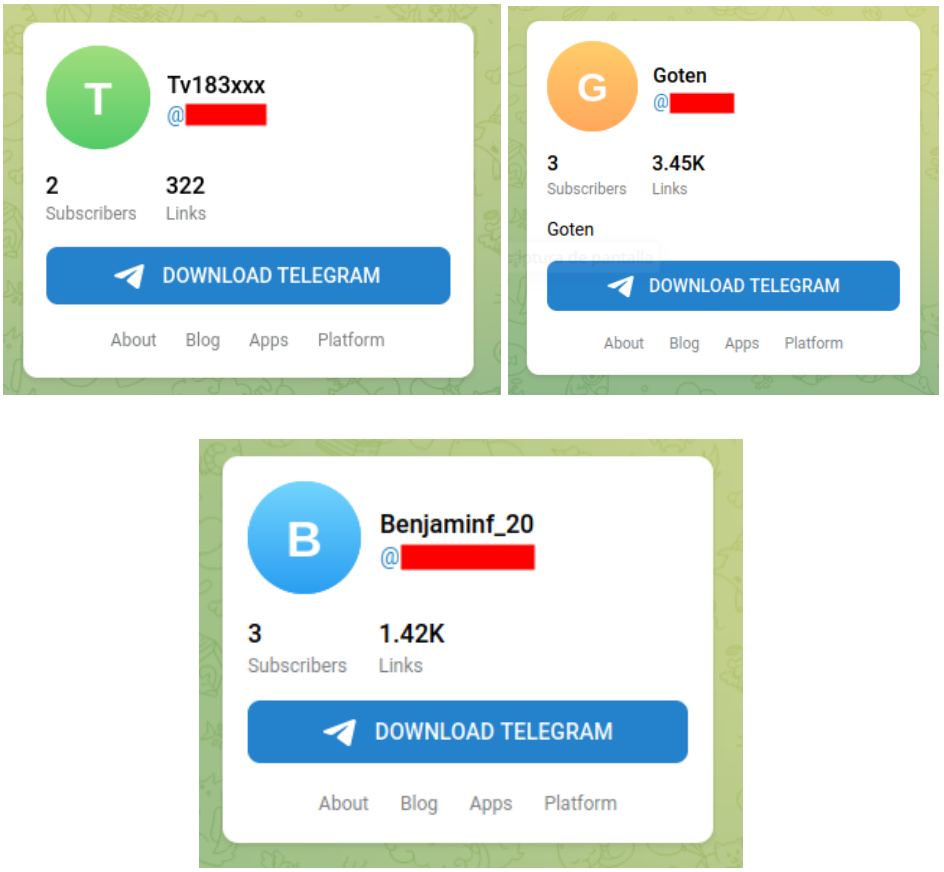
Cantidad URLs	Bot Username	Institución Afectada
10	Deyvgalicnewbot	Banco en Paraguay
6	colmenaress_bot	Banco en Colombia
6	Itaunewvalbot	Banco en Paraguay
6	itaumetbot	Banco en Paraguay
4	Luispersobot	Banco en Colombia
3	Michelroberti1_bot	Banco en Colombia
3	Bgeneral_bot	Banco en Panamá
3	NarajanXbot	Banco en Panamá

El bot “Deyvgalicnewbot” es el más activo de este mes con 10 urls asociadas, las cuales reportan al usuario de Telegram “DGarciafcb” en su chat privado. De la misma forma, “colmenaress_bot” se reporta al usuario “Luis Colmenares”. Mientras que “Itaunewvalbot” y “itaumetbot” se comunican con los usuarios “Elvis Prieto” y “Kalexandre” respectivamente.

La gran mayoría de estos bots fueron encontrados en phishings alojados en pantheonsite.io. Excepcionalmente, Luispersobot fue el único bot de este mes que fue asociado a phishings en 2 proveedores de hosting diferentes.

Los canales de Telegram

Este mes de marzo, hemos podido detectar 3 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.

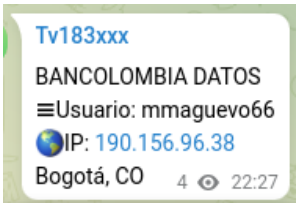


Como todos son canales públicos y permiten acceso directo a través de un navegador, basta con acceder a la vista previa del canal colocando la URL siguiente:

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

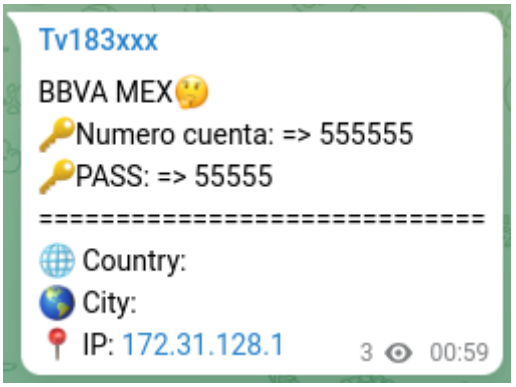
Con esto uno puede acceder fácilmente desde afuera a los canales y ver los datos que ahí han enviado.

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

	Canal 1	Canal 2	Canal 3
Nombre Bot	Tv183xxx	Goten	Benjaminf_20
Fecha Inicio	12 de Febrero 2023	03 de Enero 2023	18 de Noviembre 2022
Fecha Último Mensaje	13 de Abril 2023	17 de Abril 2023	09 de Abril 2023
# de Mensajes	322	3450~	1420~
Empresas Afectadas	Bancolombia BBVA México	Bancolombia Daviplata Banco Caja Social	Bancolombia Daviplata NaranjaX
Formato Mensaje con Datos Capturados			

Canal 1

Este canal es el más reciente de los 3 identificados durante el mes de marzo y destaca por ser el único en expandir operaciones fuera de Colombia, realizando campañas de phishing contra el Banco BBVA de México a partir del 10 de abril.



Como curiosidad, en el canal hay una IP que aparece en 21 mensajes, uno de ellos es el primer mensaje de todo el canal. Analizando los mensajes enviados es difícil determinar si se trata de alguien relacionado al phishing o una persona con mucho tiempo y ganas de molestar a los delincuentes.

Hora	Fecha	Usuario	IP	Ubicación
21:36	12/02/23	mmaguevo66	190.156.96.38	Bogotá, CO
21:11	14/02/23	mmaguevo66	190.156.96.38	Bogotá, CO
08:49	15/02/23	buenosdias	190.156.96.38	Bogotá, CO
12:08	15/02/23	mmaguevo66	190.156.96.38	Bogotá, CO
12:12	15/02/23	buenosdias	190.156.96.38	Bogotá, CO
22:30	16/02/23	buenosdias	190.156.96.38	Bogotá, CO
08:50	17/02/23	buenosdias	190.156.96.38	Bogotá, CO
23:12	17/03/23	Dame ese culo	190.156.96.38	Bogotá, CO
22:36	18/03/23	buenasnoche	190.156.96.38	Bogotá, CO
16:56	24/03/23	buenosdias	190.156.96.38	Bogotá, CO

En la tabla evitamos poner los mensajes repetidos que fueron enviados en el mismo instante, para evitar tanta monotonía. Pero se puede ver con claridad que los mensajes se enviaron por casi 5 días seguidos a diferentes horarios durante febrero y luego se toma una pausa de un mes para retomar con un comentario más "apasionado" que los anteriores.

Canal 2

Las campañas de phishing asociadas a este canal de Telegram parecen ser muy efectivas, puesto que en solo 3 meses tiene casi 3500 mensajes relacionados con posibles víctimas. Para poner los números en perspectiva, el canal 1 logró un 10% de esa actividad en 2 meses y el canal 3 tuvo menos de la mitad de mensajes en 5 meses.

El canal 2, en solo 3 meses, tiene casi 3500 mensajes relacionados con posibles víctimas

Además, la gran mayoría de los mensajes son referentes a la aplicación Daviplata del Banco Davivienda de Colombia, con solo 45 relacionados a Bancolombia y 4 al Banco Caja Social.

Al analizar los mensajes dentro del canal, es interesante ver cómo, en ocasiones, los delincuentes lo usan para comunicarse entre sí, por ejemplo, para establecer metas, indicar que los correos maliciosos no están llegando a la bandeja de entrada y probar si el sitio de phishing está capturando los datos correctamente.

Los mensajes enviados por los responsables del phishing tienen algunos antecedentes que pueden ser interesantes, por lo que trataremos de mostrarles la mayoría, evitando los repetidos.

Hora	Fecha	DOC	Clave	IP	Ubicación
16:45	03/01/23	angelica@hotmail.com	6666	181.59.2.35	Bogotá, CO
16:45	03/01/23	angelica	6666	181.59.2.35	Bogotá, CO
15:50	04/01/23	Prueba	666	181.59.2.35	Bogotá, CO
05:00	05/01/23	Hola	666	181.59.2.35	Bogotá, CO
05:08	06/01/23	Prueba	Esoes	181.59.2.35	Bogotá, CO

Hora	Fecha	DOC	Clave	IP	Ubicación
00:17	07/01/23	Sera	dalo	181.59.2.35	Bogotá, CO
20:50	08/01/23	1045106797	4383	181.59.2.35	Bogotá, CO
17:02	09/01/23	Esprueba	Activos	181.59.2.35	Bogotá, CO
17:02	09/01/23	Esprueba	Activos	181.59.2.35	Bogotá, CO
11:30	11/01/23	Hablaclaro	Estadandodavi?	181.59.2.35	Bogotá, CO
15:06	11/01/23	Es hora de coronar	1.000.000 es la meta	181.59.2.35	Bogotá, CO
19:17	11/01/23	Prueba	Esoes	181.59.2.35	Bogotá, CO
08:51	15/01/23	2 llones	Pa rumbear con el costeño	181.59.2.32	Bogotá, CO
17:00	20/01/23	Un millón es la meta	Pa que las cariñosas	181.59.2.32	Bogotá, CO
19:14	20/01/23	Es hora de coronar	1.000.000 pal monchi	181.59.2.32	Bogotá, CO
21:50	21/01/23	Hoy se corona	3 llones	181.59.2.32	Bogotá, CO
23:40	21/01/23	hola hola	hola hola	181.59.2.32	Bogotá, CO
12:29	25/01/23	te estan cayendo en no deseado	12369874	179.19.42.189	Bogotá, CO
15:31	25/01/23	Prueba	Esoes	181.59.2.126	Bogotá, CO
17:14	28/01/23	Es hora de coronar	Paqiefrao	181.59.2.126	Bogotá, CO
16:08	29/01/23	A hacer billete	Pa las perrillas	181.59.2.126	Bogotá, CO
13:16	03/02/23	AURUMWTF	666	181.59.2.126	Bogotá, CO
00:35	12/02/23	11111111111	1111	191.95.49.59	Bogotá, CO
19:57	12/02/23	Prueba	Esoes	181.59.2.104	Bogotá, CO
15:25	13/02/23	Hola	guapa	181.59.2.104	Bogotá, CO
08:47	18/02/23	Albita	666	181.59.2.104	Bogotá, CO
06:38	02/03/23	Albita Activo	Qlq	181.59.2.104	Bogotá, CO
06:33	05/03/23	Es hora de coronar	5 LLONES	181.59.2.104	Bogotá, CO

Algo que llama la atención al ver los mensajes, es el primero que se recibió posterior a la creación del canal, proveniente de la IP 181.59.2.35, que pertenece a

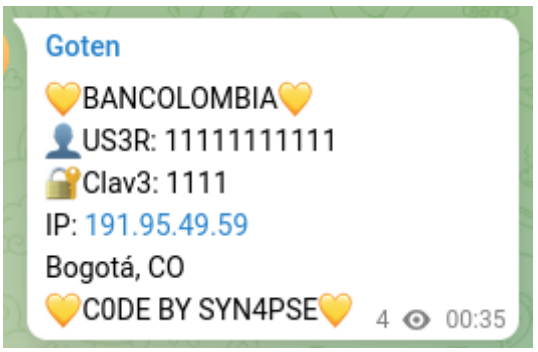
uno de los responsables del phishing y que contiene la dirección de correo electrónico “angelica@hotmail.com”, la que está asociada a una cuenta de TikTok con más de 5000 seguidores. Por supuesto, no hay ningún antecedente que sirva para vincular la cuenta y probablemente no tenga ninguna relación, pero al menos sirve para establecer los gustos musicales de alguno de ellos.

Otro dato notable es el horario en que operan, partiendo desde muy temprano en la mañana hasta la medianoche. Además de las referencias a personas, como Angélica, el Costeño, Mochi, guapa, Albita; llama la atención el uso que buscan darle al dinero robado.

Después de 3 meses los controladores del canal 2 acumularon 5 millones de pesos colombianos.

Pero posiblemente el dato de mayor interés sea que después de 3 meses acumularon 5 millones de pesos colombianos (cerca de $US 1130), equivalente a 4.3 salarios mínimos en Colombia. De modo que todo ese trabajo no es suficiente para darse una vida llena de lujos, pero tal vez alcance para “rumbear con el costeño”.

Como curiosidad, el 12 de febrero aparece un mensaje de prueba de un kit de phishing asociado a Bancolombia, el que contiene una especie de firma indicando que fue desarrollado por SYN4PSE.



Desde que empezamos a capturar información de Telegram, ésta es la segunda vez que vemos una referencia a SYN4PSE. La primera vez fue en noviembre del 2022, en un sitio de phishing que suplantaba a un Banco Chileno estaba configurado el bot Probatoriabot que reportaba al súper grupo llamado "Caidas", al que estaban suscritos dos usuarios: JCO (@SYN4PSE) y DATA Synapse (@datasyn4pse).

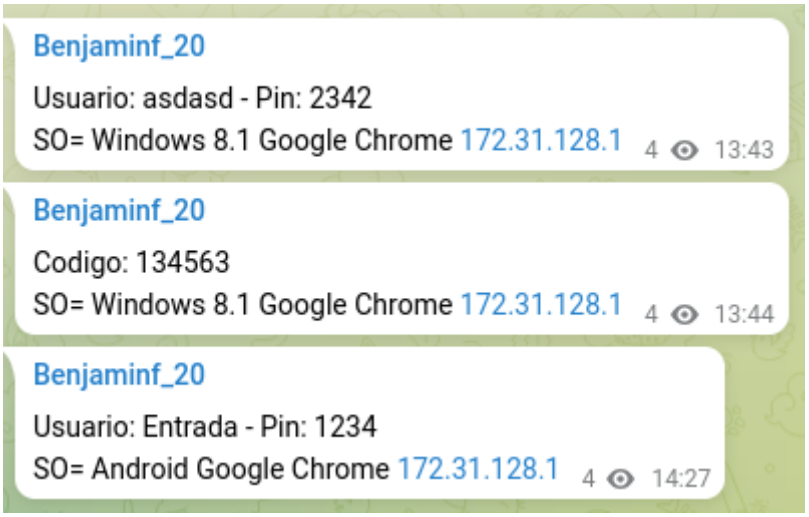
Canal 3

Este canal es el que tiene la historia más larga de los identificados este mes. Desde sus inicios, a mediados de noviembre del 2022, el canal ha ido evolucionando en el detalle de los mensajes recibidos.

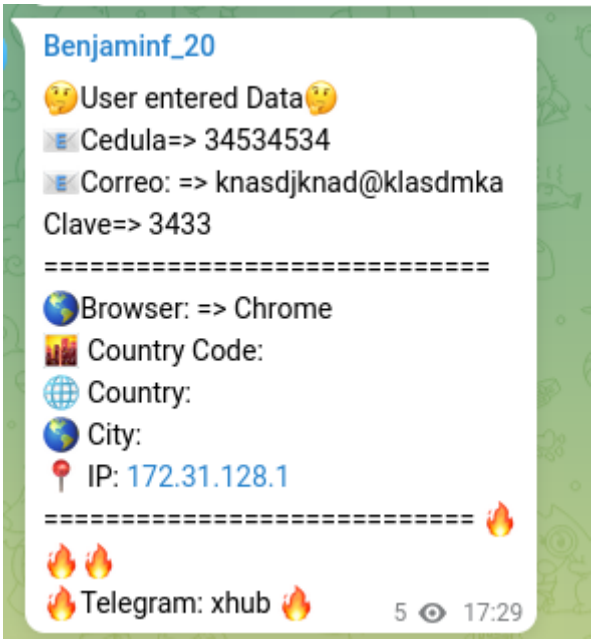
Los primeros dos meses, la gran mayoría de mensajes publicados por el bot "Rabbi123_bot" eran de prueba. Inicialmente solo tenían los datos más básicos, como usuario, clave e IP, aunque esta última siempre era la misma IP privada de clase B, que no puede ser ruteada por Internet.

Con el paso del tiempo le agregaron la versión de Sistema Operativo y Navegador, aunque seguían sin víctimas reales hasta la última semana de diciembre.

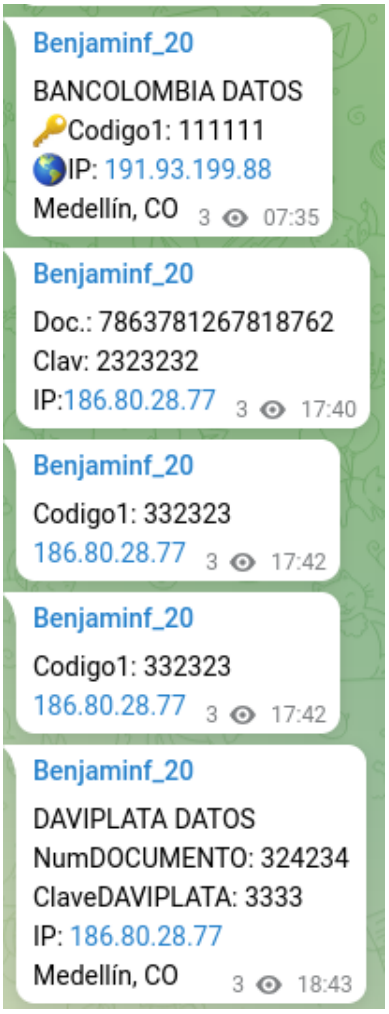
El canal 3 es el que tiene la historia más larga de los identificados este mes.



El 28 de enero empezaron las pruebas con un pack asociado a la fintech Naranja X, aunque no hubo más actividad relacionada hasta la fecha. Por suerte algo interesante ocurre el 4 de febrero, realizan la integración de otro pack, pero esta vez cada mensaje relacionado contiene la firma "🔥Telegram: xhub 🔥".



Un par de días después integran el pack de Bancolombia visto en los otros canales analizados previamente. Y, finalmente, el 30 de marzo se configura el bot en el pack de Daviplata, conviviendo con los otros.



Al analizar los mensajes del canal se pueden identificar algunos que fueron generados por los delincuentes responsables del phishing, la gran mayoría son mensajes de prueba, pero algunos corresponden a comunicación entre ellos que puede ser de algún interés. Vamos a omitir la mayoría de los mensajes de prueba, ya que aportan poco valor.

Hora	Fecha	Mensaje	IP	Ubicación
15:41	28/12/22	Linlinlin	172.31.128.1	
17:16	28/12/22	Rabbitplantilla23	172.31.128.1	
19:24	28/01/23	klasnckja@hotmail.com	172.31.128.1	
15:21	29/01/23	klasnckja@hotmail.com	2800:484:bb86:8866:d5ad:a39b:1346:7676	Medellín, CO

Hora	Fecha	Mensaje	IP	Ubicación
19:09	04/02/23	Linlinlin	186.102.45.221	Bogotá, CO
19:10	04/02/23	Rabbitplantilla23@hotmail.com	186.102.45.221	Bogotá, CO
22:11	07/02/23	232422	186.80.28.45	Medellín, CO
23:37	17/02/23	Decileaherna O a dirimo jajaja hay chamo	172.31.128.1	
21:12	20/02/23	Hola	186.80.28.45	Medellín, CO
14:53	04/03/23	Lalocarabi123	191.95.55.53	Bogotá, CO
20:31	04/03/23	Bellobello	186.29.182.96	Barrio San Luis, CO
01:05	05/03/23	Respondeelwhatsapp	186.29.182.96	Barrio San Luis, CO
01:33	05/03/23	Hola	181.32.159.79	Medellín, CO
01:33	05/03/23	Loca	186.29.182.96	Barrio San Luis, CO
18:09	16/03/23	holaq2312	186.80.28.79	Medellín, CO
17:39	23/03/23	Prueba	191.95.59.143	Barrio San Luis, CO

De la tabla se desprende que las comunicaciones ocurren entre personas que están en tres ubicaciones diferentes. Además, si consideramos que el bot que alimenta este canal se llama “Rabbi123_bot”, podríamos intuir que haya alguna relación con los mensajes “Rabbitplantilla23”, “Rabbitplantilla23@hotmail.com”, “Lalocarabi123” y “Loca”, aunque de momento no tenemos ningún antecedente para confirmarlo, por lo que no son más que supuestos.

Las comunicaciones del canal 3 ocurren entre personas que están en tres ubicaciones diferentes.

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, y pudiendo entregarles informes mensuales de los hallazgos.

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 y actividades en otros países de la región, 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 Febrero 2023:

- https://finsin.cl/2023/03/13/cumplimos-1-ano-de-reportes-de-phishing/

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/