FINSIN

Reporte de Phishing

Diciembre 2022

Indice

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 al parecer es un ataque muy barato, por lo que los ciberdelincuentes pueden generar muchas "copias" diariamente, y solamente tendrían que hacer que las personas visiten el sitio para poder engañarlas y robarles sus claves u otro tipo de información.

Al analizar algunos de estos sitios encontramos que tenían 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 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 que esta herramienta pueda detectar.

Ricardo Monreal Llop
Presidente FINSIN

TL;DR

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

El 80% de los kits detectados corresponden a sitios que intentan estafar a personas en Chile.

Solo con el top 2 de kits detectados ya tenemos más del 50% de las detecciones de la plataforma.

Los del pack "0009-5" se cambiaron a otro subdominio de ehloqservices.info, ¡el mismo usado por los FC-03!

Un 88% de todos los phishing que hemos detectado para Colombia se alojan en Replit.

A lo largo de estos 4 meses solo 2 bots de los Phishing de Colombia se repitieron, y solo 1 por un tiempo largo.

Esperamos que con estos datos les den ganas de seguir 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.

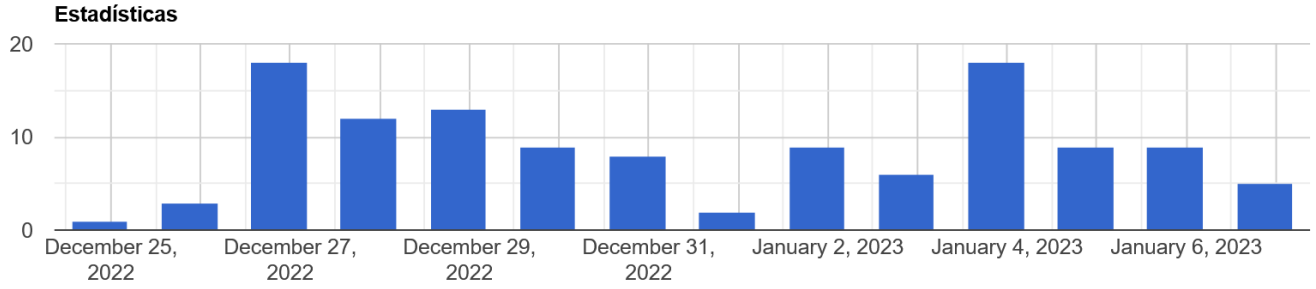
Phishing Checker

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, que basta con tener una URL y puedes 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.

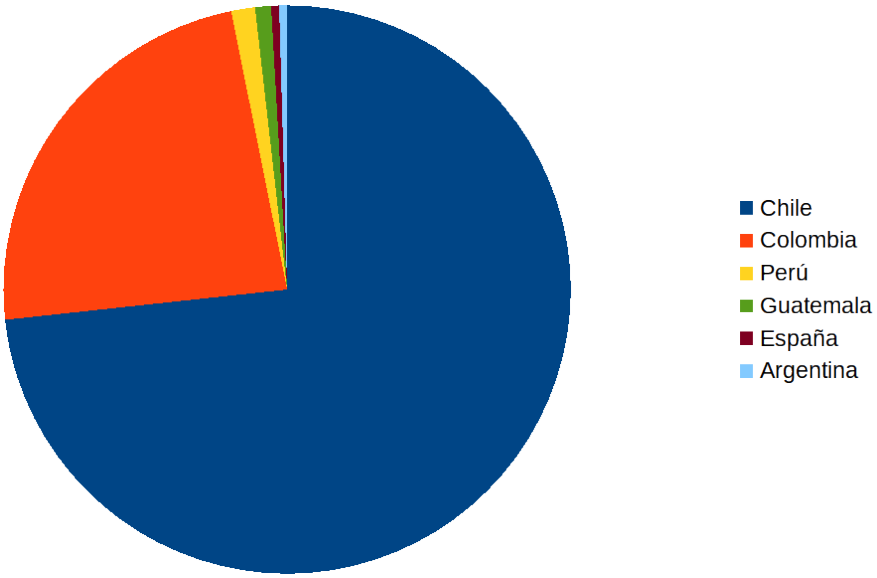
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Diciembre 2022

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[2]

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

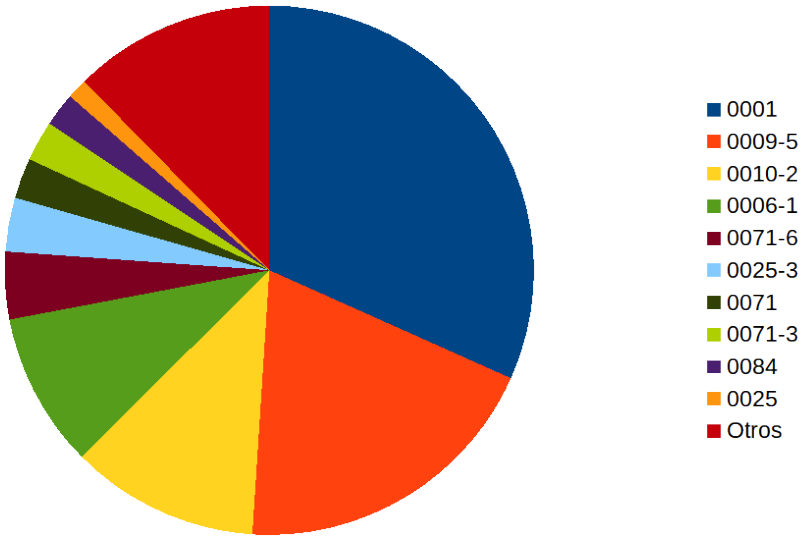


Pais	Porcentaje
Chile	80,49 %
Colombia	13,66 %
Perú	3,41 %
Gatemala	0,98 %
España	0,49 %
Argentina	0,49 %

2 Es la distribución de los phishing que fueron detectados por la plataforma, no corresponde al total real de Chile ni constituyen un ranking del mundo.

Datos de kits

En diciembre logramos agregar 3 kits nuevos y 8 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	31,69 %
0009-5	28,31 %
0025-3	16,87 %
0071-7	13,86 %
0010-2	6,02 %
0006-1	4,82 %
0070-7	3,61 %
0071-10	3,61 %
0071-3	3,01 %
0071-6	1,81 %
Otros	18,07 %

Solo con el top 2 de kits detectados ya tenemos más del 50% de las detecciones de la plataforma

El pack 0001 sigue siendo el dominador, como en muchos meses anteriores. Vuelven a aparecer los kits como el 0009-5[3], el 0025-3 y el 0071-7 que tienen más del 10% de las detecciones del mes cada uno. Y solo con el top 2 de kits detectados ya tenemos más del 50% de las detecciones de la plataforma.

Con esto podemos ver que hay kits antiguos (números más bajos) que mantienen su uso, pero también vemos una tendencia a usar muchas de las variantes del kit 0071 para estafas.

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

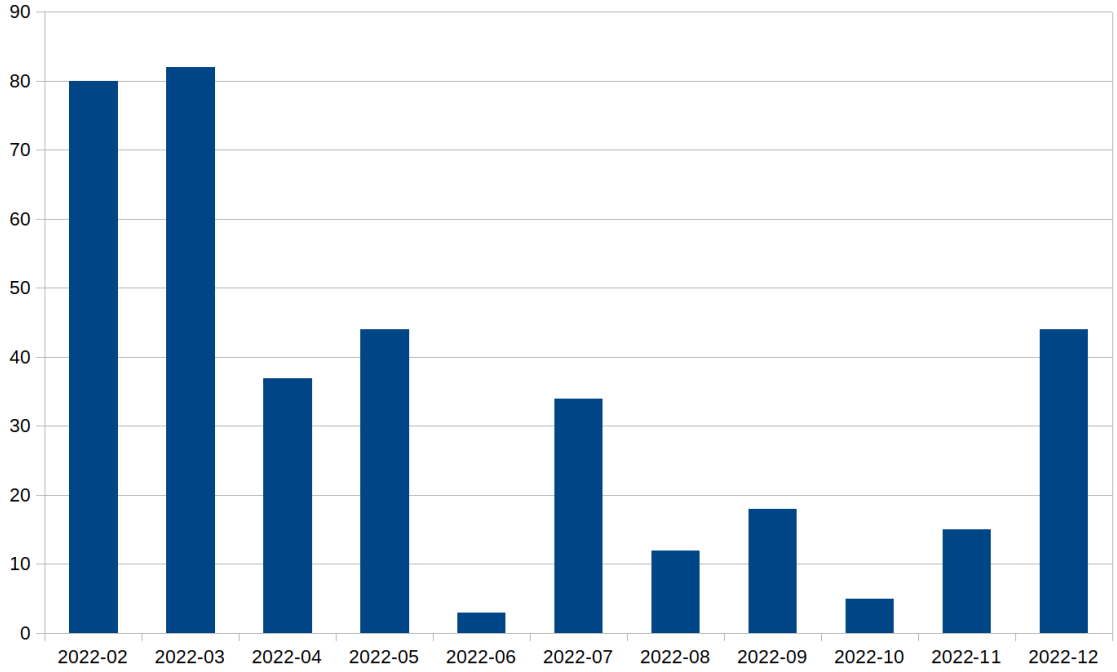
Actualización FC-01 y FC-03

Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos FC-01[4] y FC-03[5] que aunque tienen nombres parecidos tienen características muy distintas.

FC-01

Como hemos visto anteriormente 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.

En los últimos meses ha bajado su actividad, llegando a una actividad muy baja ahora en el segundo semestre, como podemos ver en el siguiente gráfico.



Como lo revisamos en el reporte del mes pasado, esperábamos que este grupo resurja y lo ha hecho, logrando llegar a más del doble de detecciones este mes.

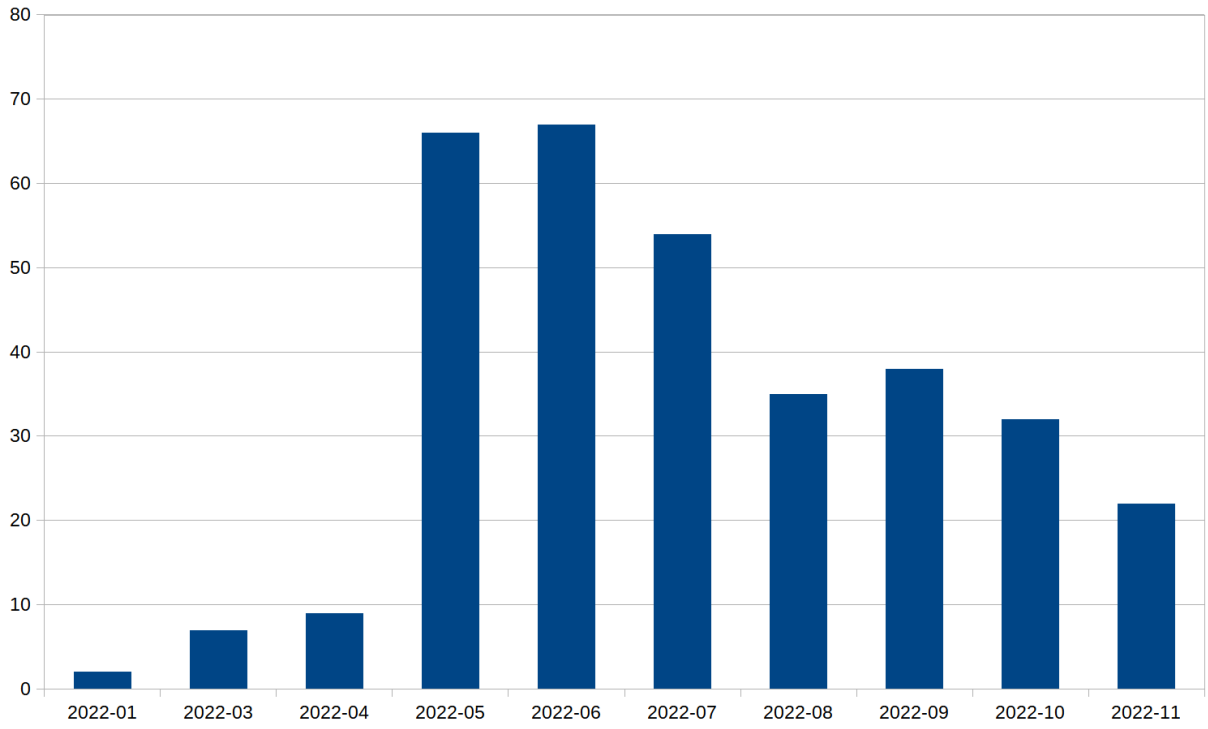
Aun no llega a los peaks vistos a principio de año, pero comienza a verse una remontada, estaremos monitoreando para ver si la tendencia creciente sigue.

4 Definido en el reporte de Febrero: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/

5 Definido en el reporte de Junio: https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

FC-03

El grupo FC-03 es de los que más se ha "mantenido en el tiempo", Como podemos ver, aún cuando en los últimos meses se ha visto una tendencia clara a la baja, siguen lanzando decenas de sitios de phishing mensualmente:



Creemos que su longevidad se debe a que principalmente es de los grupos con menor gasto para la generación de sus dominios.

- Siguen usando el mismo kit "0010-2" que es el kit que han usado desde fines de Mayo, por lo que su inversión en desarrollo sigue siendo 0.
- Siguen usando la plataforma Firebase de Google para levantar sus sitios en el nivel gratis, por lo que siempre son subdominios de .firebaseapp.com o .web.app.
- Siguen usando subdominios del dominio "ehloq.xyz" como base de datos externa para sus datos robados. Lo único que necesitan aquí es mantener sus costos de dominio y de servidores, por lo que sigue siendo barato.

Este mes no tuvimos tanta acción del grupo con el pack 0010-2, o por lo menos no tuvimos tantas detecciones del grupo, pero nos pareció interesante el hecho de cambiaran de dominio.

Dia	Pack	C2
2022-12-01	0010-2	https://main-fala.ehloq.xyz
2022-12-02	0010-2	https://worker-fala.ehloq.xyz
2022-12-06	0010-2	https://worker-fala.ehloq.xyz
2022-12-09	0010-2	https://worker-fala.ehloq.xyz
2022-12-12	0010-2	https://main-fala.ehloq.xyz
2022-12-30	0010-2	https://worker-fala.ehloqservices.info

Esto nos hace decir que el dominio “ehloq.xyz” ya les dejó de ser útil y ahora van a cambiar de dominio a otro similar “ehloqservices.info”.

Si investigamos el origen de este dominio nuevo podemos ver que fue registrado ahora a fin de año, el 20 de diciembre:

Registrar Info

Name	NameCheap, Inc.
Whois Server	whois.namecheap.com
Referral URL	https://www.namecheap.com/
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2023-12-20
Registered On	2022-12-20
Updated On	2022-12-25

El dominio nuevo y el antiguo tienen la misma raíz “ehloq”, y ambos fueron creados con Namecheap. Aunque esto no dice mucho, es parte de lo que nos queda como punto a revisar en un futuro.

Lo más interesante aparece cuando vemos el comportamiento de otro de los packs que ha estado muy utilizado en los últimos meses: el pack “0009-5”.

Día	Pack	C2
2022-12-01	0009-5	https://garyvideos.click
2022-12-02	0009-5	https://garyvideos.click
2022-12-03	0009-5	https://garyvideos.click
2022-12-04	0009-5	https://garyvideos.click
2022-12-05	0009-5	https://garyvideos.click
2022-12-06	0009-5	https://garyvideos.click
2022-12-07	0009-5	https://garyvideos.click
2022-12-08	0009-5	https://garyvideos.click
2022-12-09	0009-5	https://garyvideos.click
2022-12-13	0009-5	https://garyvideos.click
2022-12-14	0009-5	https://garyvideos.click
2022-12-15	0009-5	https://garyvideos.click
2022-12-17	0009-5	https://garyvideos.click
2022-12-20	0009-5	https://garyvideos.click
2022-12-21	0009-5	https://r4gn4r0kr4.ehloqservices.info
2022-12-22	0009-5	https://r4gn4r0kr4.ehloqservices.info
2022-12-24	0009-5	https://r4gn4r0kr4.ehloqservices.info
2022-12-26	0009-5	https://r4gn4r0kr4.ehloqservices.info
2022-12-27	0009-5	https://r4gn4r0kr4.ehloqservices.info
2022-12-29	0009-5	https://r4gn4r0kr4.ehloqservices.info
2022-12-30	0009-5	https://r4gn4r0kr4.ehloqservices.info
2022-12-31	0009-5	https://r4gn4r0kr4.ehloqservices.info

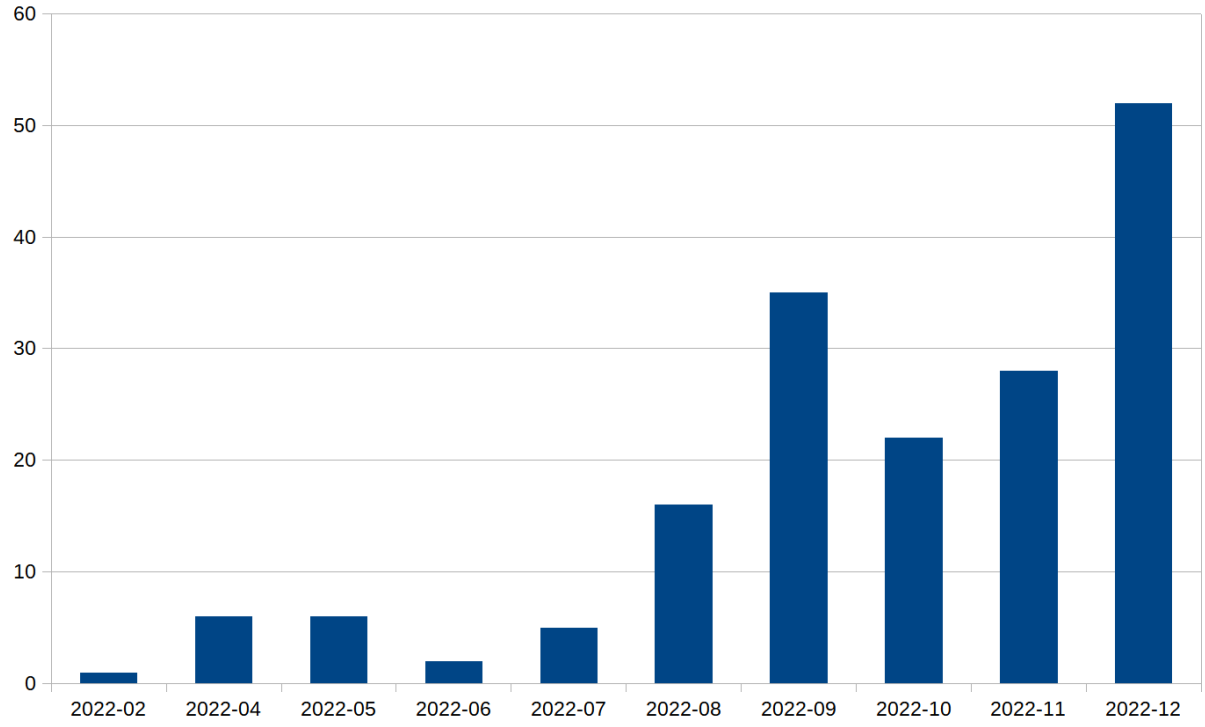
Revisando los dominios de C2 usados este mes de Diciembre tenemos que un poco antes de navidad cambiaron de dominio, ya no están usando el “clásico” https://garyvideos.click, sino que ahora se cambiaron a otro subdominio de ehloqservices.info, ¡el mismo usado por los FC.03!

Por ahora, lo único que podemos asumir que las personas detrás del phishing están compartiendo infraestructura desde el 21 de diciembre. Esto nos deja muchas dudas, por lo que de ahora en adelante tendremos que comenzar a revisar los cambios de comportamiento del pack 0009-5.

Ahora se cambiaron a otro subdominio de ehloqservices.info, ¡el mismo usado por los FC.03!

Actividad en Colombia

A través de los meses, hemos notado que otro de los países que tienen un problema bastante grande con el Phishing es Colombia. De hecho, nuestro gráfico de detección mensual para este país es el siguiente:



Como podemos ver en los últimos meses ha crecido mucho las detecciones que tenemos de Colombia, principalmente porque hemos encontrado cada vez más variantes de los pack usados para hacer phishing allá.

De hecho, si vemos la distribución de packs (y variantes) de este mes para Colombia tenemos lo siguiente:

Pack	Cantidad
0071-7	23
0070-7	6
0071-10	6
0071-3	5
0071-6	3
0070-3	2
0090	2
0070-4	1
0071-5	1
0071-9	1
0082-2	1
0086	1

Muchas detecciones para los packs “0070” y “0071” (con sus variantes), y unos pocos de otros packs.

Además, lo que mencionamos en el reporte anterior, el mayor dolor de cabeza sigue siendo los sitios de repl.co, o por lo menos ahí es donde nosotros encontramos la gran mayoría de estos sitios.

Un 88% de todos los phishing que hemos detectado para Colombia se alojan en Replit.

Si vemos la tabla de las detecciones por servicio:

Servicio	Cantidad
Repl.co	46
Pantheon	4
Otro	2

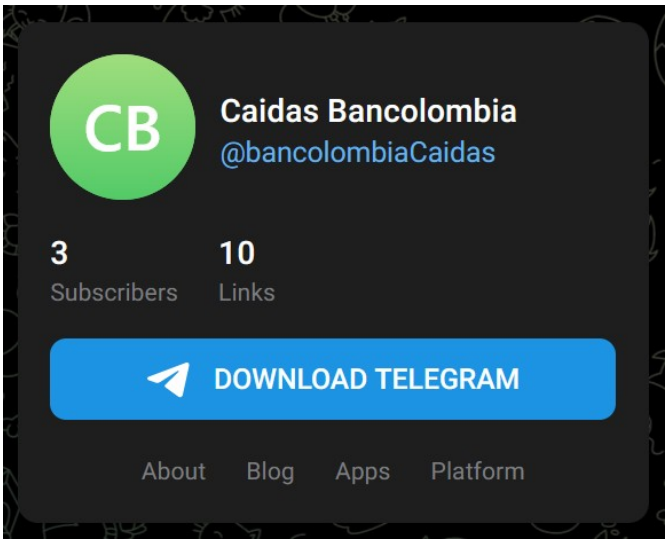
Un 88% de todos los phishing que hemos detectado para Colombia en diciembre están alojados en el servicio de Replit (repl.co). Aun cuando se dan de baja rápidamente se nota que es uno de los servicios populares para phishing en la banca en Latinoamérica.

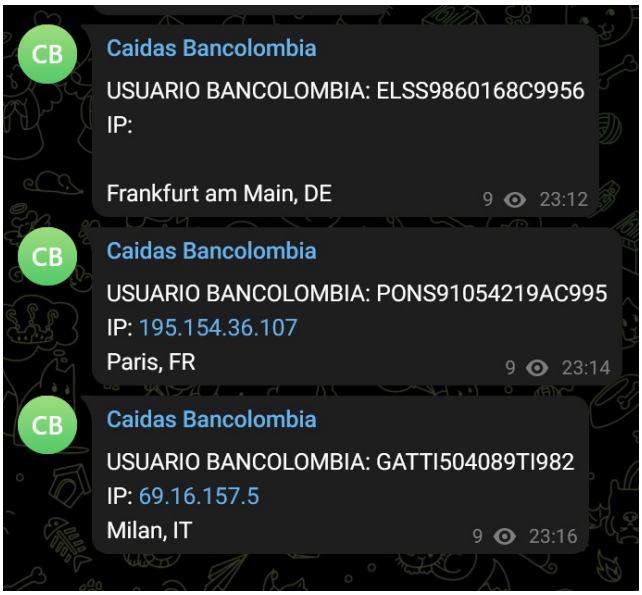
Ahora, dentro de algunos de estos packs podemos obtener información, como lo veíamos en el reporte de Septiembre[6]. Podemos obtener información muy importante relacionada a los bots de Telegram que usan para comunicarse y enviarse la información de las víctimas:

Esto es un muy mal ejemplo de como hacer un sitio web de scams, pero son muy buenas noticias para nosotros. Solo este mes tenemos los siguientes bots:

sitios	bot_id	chat_id	bot_name	bot_username
1	5533895401	5084615131	Bancacolombia9	Memelibancolbot
5	5556002571	5436603721	NUEVOBANCOLOMBIABOT	BANCONOTBOT
1	5626730792	5616051265	meriychicobancolombia	meriychicobancolombia_bot
1	5659416459	5666027011	bancolombianuevos	bancolombiiaabot
2	5676948056	5590169701	tocoganador	tocoganador_bot
6	5678035357	5520211995	bancolombia_real	bancolombia_real_bot
6	5724653637	5665788562	LOGOSBANCOLOMBIAAPP	bancoolombiaaaaaaabot
2	5766684849	-1001761500695	caidasbancolombia_bot	caidasbancolombiaabot
1	5959527985	5396808002	Bancolombia 01.bot	Bancolombia765_bot
8	5967584917	5739811226	empezar con fe	bancolombia_cuadro_bot

Uno de los resultados interesantes es el uso de un canal “abierto” como repositorio de las claves, lo que nos permite ir directamente y visitar el canal para obtener los resultados de las víctimas. El canal es el siguiente: https://t.me/s/bancolombiaCaidas





6 El reporte de Septiembre lo pueden encontrar en: https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/

Los datos anteriores no están ofuscados o tachados porque pensamos que no son datos reales. El hecho de ser de orígenes europeos con valores extraños que no recuerdan a ningún identificador de usuario para el banco afectado nos hace pensar que son bots de detección de phishing (interesante el procedimiento).

A lo largo de estos 4 meses solo 2 bots se repitieron, y solo 1 por un tiempo largo

Otra de las cosas que nos parecen interesantes es que los chats de telegram van mutando con el tiempo, si nos fijamos en los chats que han aparecido desde septiembre tenemos este historial:

Mes	Pack	Bot_ID	Chat_ID
2022-08	0070	5629982510	5650746250
2022-09	0070-3	5338068539	2078741853
2022-09	0070	5431518995	1831387398
2022-09	0070-3	5455554519	5118912146
2022-09	0070-2	5458731499	-706063848
2022-09	0070-3	5507577768	5447936478
2022-09	0070	5511957735	1502580135
2022-09	0070	5629982510	5650746250
2022-09	0070	5671800216	5000224470
2022-09	0070	5693490051	5652993221
2022-09	0070	5752707248	5573002586
2022-09	0070	5756261190	1502580135
2022-09	0070	5756261190	5677452420
2022-10	0070	5510145922	1237943893
2022-11	0070-5	5313524679	-1001182017096
2022-11	0070-5	5458731499	-706063848
2022-11	0070-6	5470878882	1428096676
2022-11	0070-5	5612595756	-680710397
2022-11	0070	5767273818	5678756454
2022-12	0071-7	5533895401	5084615131
2022-12	0070-7	5556002571	5436603721
2022-12	0070-7	5626730792	5616051265
2022-12	0071-7	5659416459	5666027011
2022-12	0070	5676948056	5590169701
2022-12	0071-7	5678035357	5520211995
2022-12	0071-7	5724653637	5665788562
2022-12	0070	5766684849	-1001761500695
2022-12	0071-7	5959527985	5396808002
2022-12	0071-7	5967584917	5739811226

Las repeticiones son muy pocas, y a lo largo de estos 4 meses solo 2 bots se repitieron, y solo 1 a través de un tiempo largo (septiembre y noviembre). Otro caso interesante es el del bot id 5756261190, porque este se comunicó con 2 chats, en el mismo mes, pero ahora está dado de baja, por lo que no podemos tener más información.

Para un futuro trabajo, otro de los puntos más interesantes es cuando un grupo no es tan abierto, pero tiene al bot como administrador del grupo. Con esto podemos generar links de invitación al chat o simplemente agregar al nuevo usuario, y agregarlo como administrador, y además pasarle todo el historial del grupo.

Palabras finales

Al igual que en otros reportes, 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 y que eso se traduzca tanto en la detección de nuevos kits como en el mejor entendimiento de éstos.

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 como Replit, Pantheon, Namecheap o cualquier otra, 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

- Reporte Noviembre:
  - https://finsin.cl/2022/12/12/reporte-mensual-de-phishing-noviembre-2022/
- Reporte Octubre:
  - https://finsin.cl/2022/11/14/reporte-mensual-de-phishing-octubre-2022/
- Reporte Septiembre
  - https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/
- Reporte Agosto
  - https://finsin.cl/2022/09/11/reporte-mensual-de-phishing-agosto-2022/
- Reporte Julio
  - https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/
- Reporte Junio
  - https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/
- Reporte Mayo
  - https://finsin.cl/2022/06/05/reporte-mensual-de-phishing-mayo-2022/
- Reporte Abril
  - https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/
- Reporte Marzo
  - https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/
- Reporte Enero-Febrero
  - https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/