FINSIN

Reporte de Phishing

Junio y Julio 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.

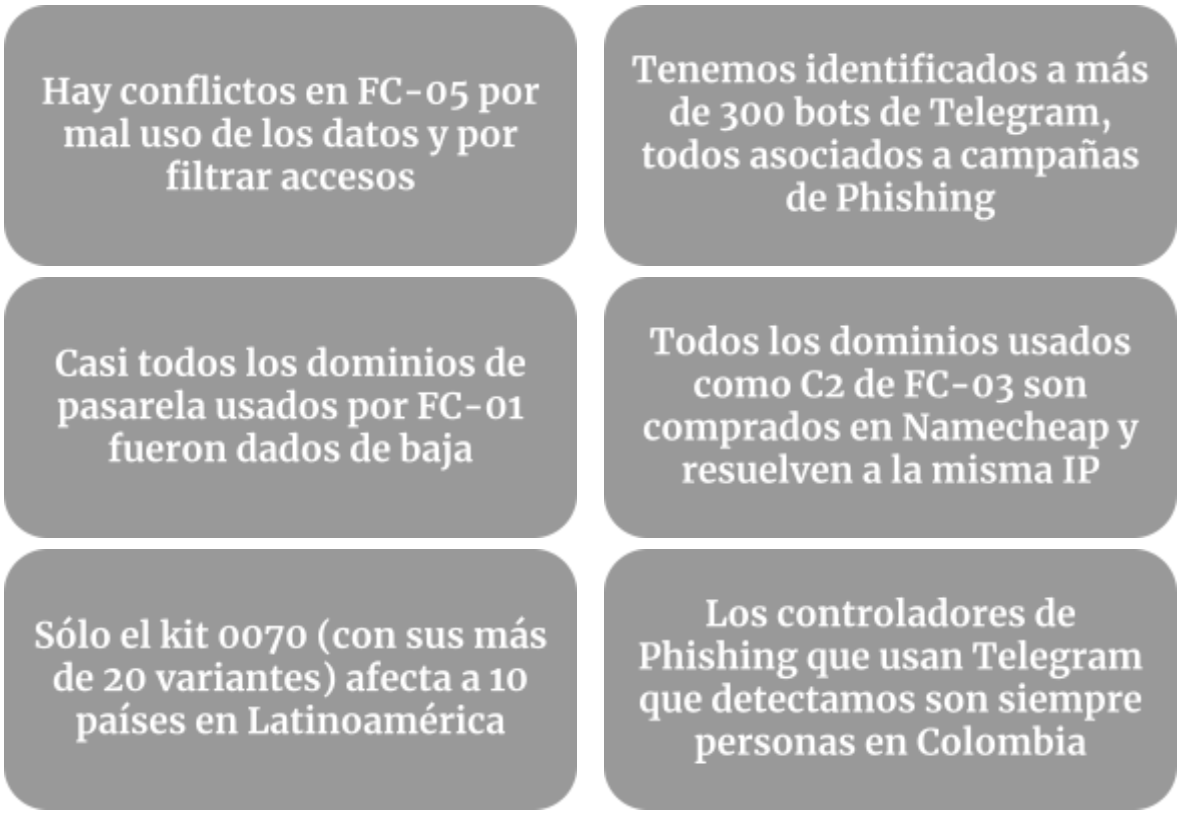
Para ello, decidimos generar un sistema automático con la capacidad de detectar, clasificar y agrupar los sitios de phishing que aparecen, logrando identificar patrones que nos permitan definir si un sitio es o no un Phishing y además a qué tipo de kit está asociado.

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 los meses de Junio y Julio[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.

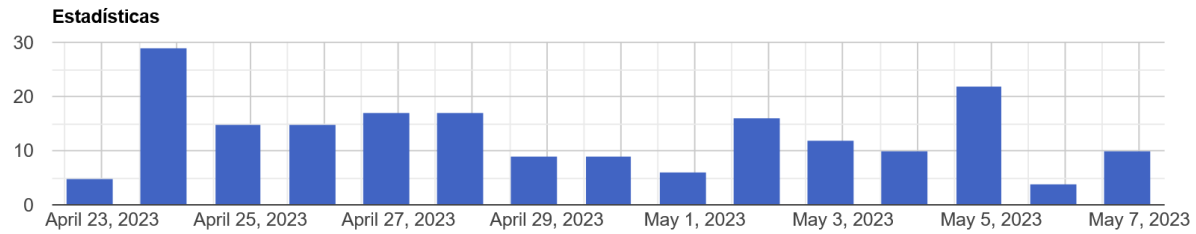
Phishing Checker

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.

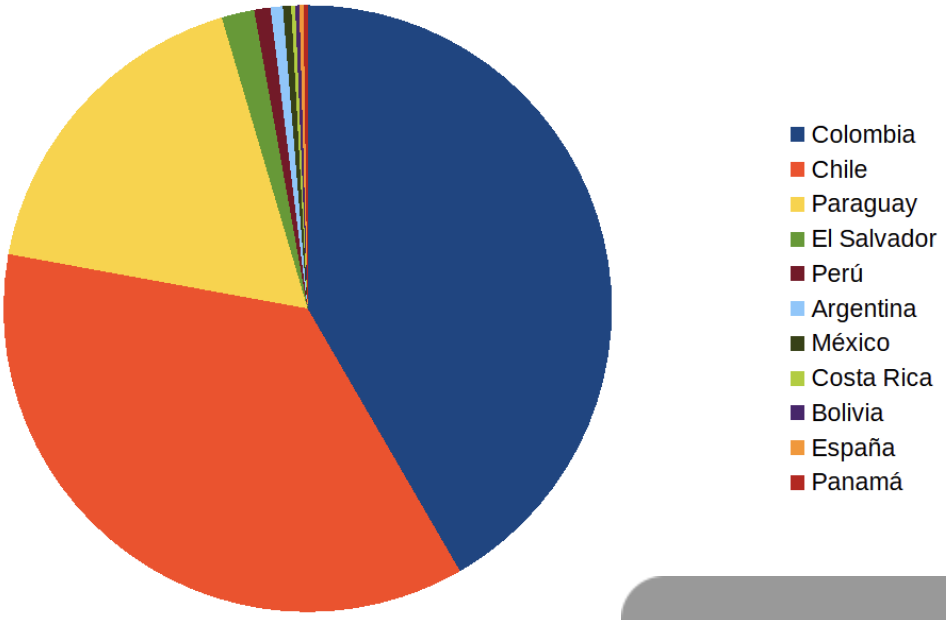
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Junio 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 detectados y en vez de revisar las instituciones afectadas, queremos analizar 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:



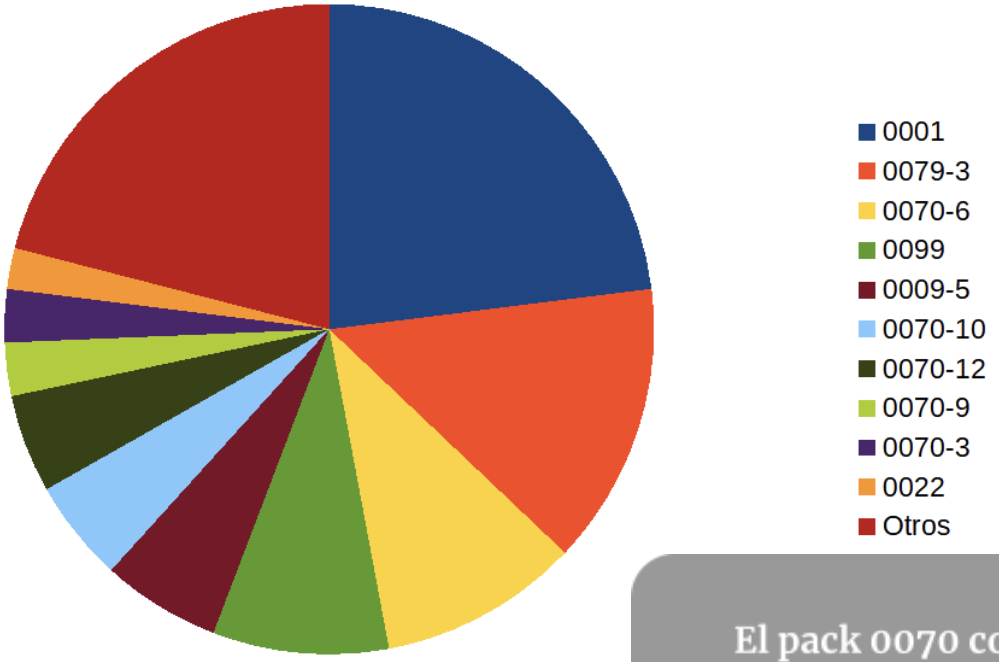
País	Porcentaje
Colombia	41,65 %
Chile	36,23 %
Paraguay	17,57 %
El Salvador	1,74 %
Perú	0,87 %
Argentina	0,65 %
México	0,43 %
Costa Rica	0,22 %
Bolivia	0,22 %
España	0,22 %
Panamá	0,22 %

Este mes tenemos 11 países distintos a los que les detectamos sitios de Phishing

¡Este mes tenemos 11 países distintos a los que les detectamos sitios de Phishing!

Datos de kits

Si graficamos los datos del mes asociados a los kits de phishing, podemos lo siguiente:



El pack 0070 con sus variantes ocupa 5 lugares del top 10 de este mes

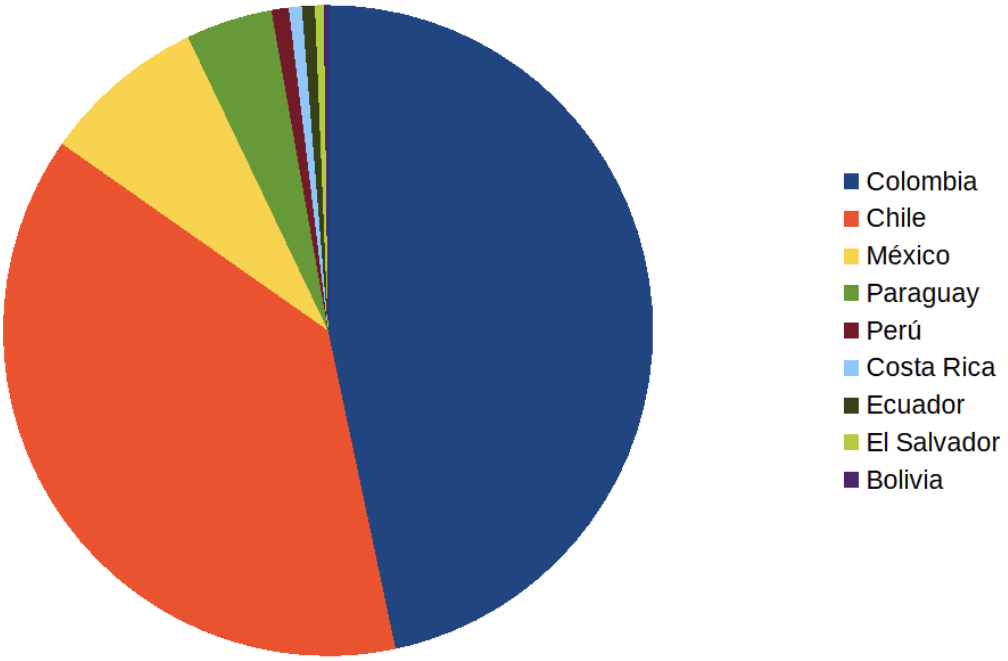
Pack	Porcentaje
0001	23,01 %
0079-3	14,05 %
0070-6	9,98 %
0099	8,76 %
0009-5	5,91 %
0070-10	5,09 %
0070-12	4,89 %
0070-9	2,65 %
0070-3	2,65 %
0022	2,04 %
Otros	20,98 %

El pack 0001, que afecta a la banca chilena sigue siendo el dominante con casi un cuarto de las detecciones. Además tenemos que el pack 0070 (con sus variantes) ocupan 5 de los 10 primeros lugares de la tabla.

Julio 2023

Datos de países

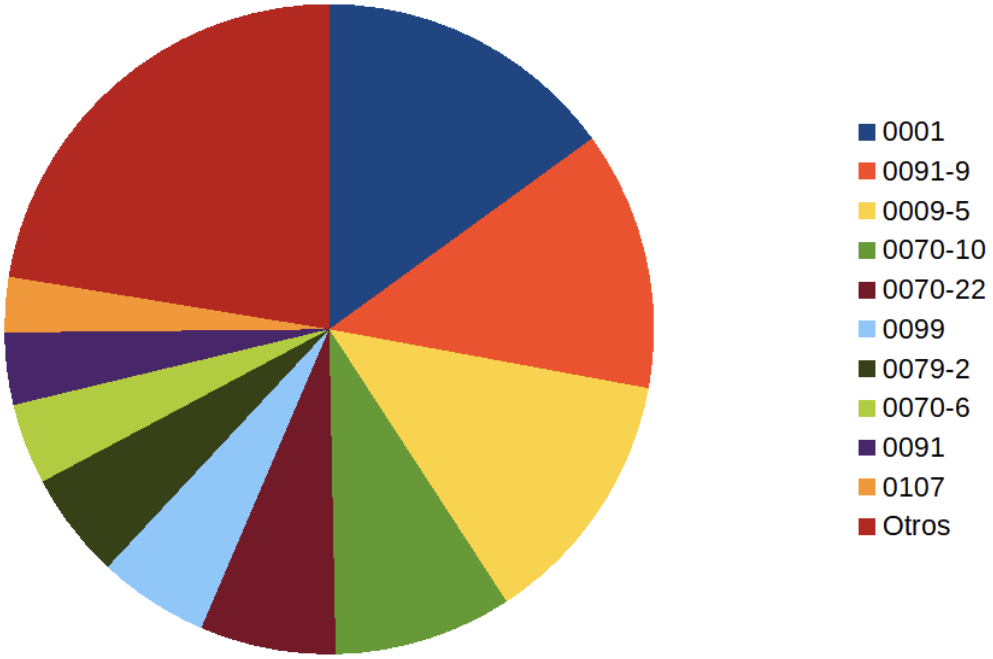
Si miramos los países de las marcas afectadas tenemos un gran cambio en las detecciones:



País	Porcentaje
Colombia	46,67 %
Chile	38,06 %
Costa Rica	8,17 %
Bolivia	4,30 %
El Salvador	0,86 %
Paraguay	0,65 %
Panamá	0,43 %
Perú	0,22 %

Datos de kits

Si graficamos los datos del mes asociados a los kits de phishing, podemos lo siguiente:



Pack	Porcentaje
0001	15,01 %
0091-9	12,90 %
0009-5	12,90 %
0070-10	8,88 %
0070-22	6,77 %
0099	5,50 %
0079-2	5,29 %
0070-6	4,02 %
0091	3,59 %
0107	2,75 %
Otros	22,41 %

En comparación con junio, en julio está todo mucho más distribuido, no existe un claro pack que lleve la delantera en las detecciones, y el pack 0070 “solamente” tiene 3 del top 10 del mes.

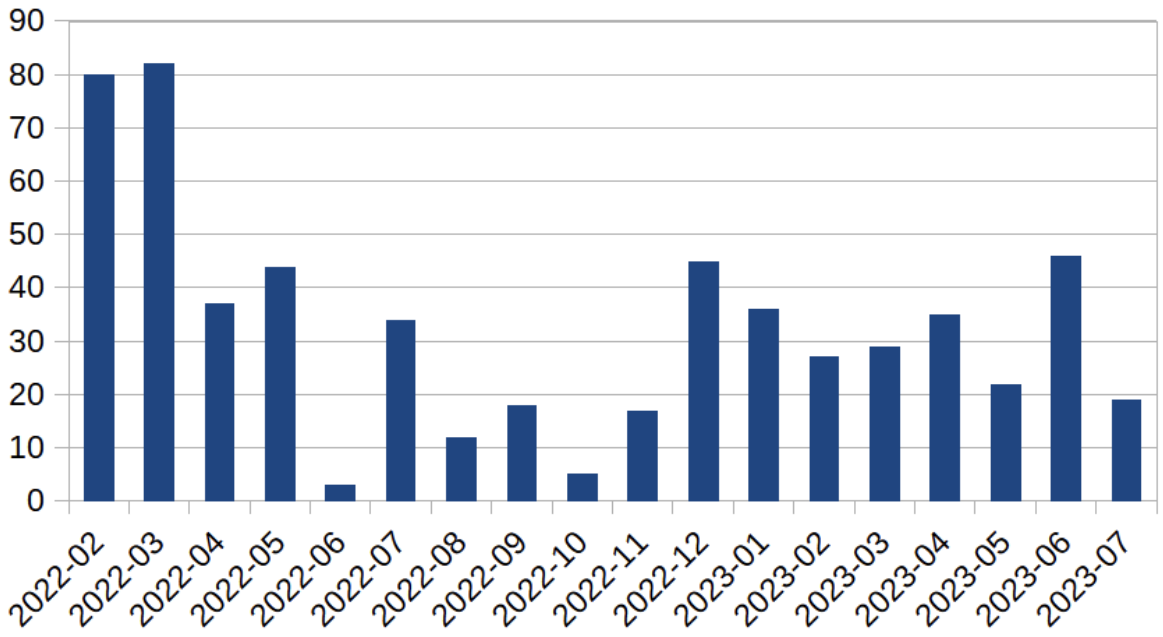
Actualización de Fishers Constantes (FC)

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, durante todo este 2023 los que están detrás del grupo están levantando por lo menos 20 sitios mensuales y un máximo de 46 en junio, lo que habla de su contínua producción, aun cuando sea un comportamiento conocido.

[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/

En estos meses pudimos seguir a este grupo por los patrones de los dominios, pero además por los dominios intermedios que usan, en este caso fueron los siguientes:

- amazon1234.com (dado de baja)
- avengerpatitos.com (dado de baja)
- eilders.nl (dado de baja)
- homefogastadp.info
- lagarnvalpa.com
- nationaltreasures.co.nz (dado de baja)
- reachercontact.com (dado de baja)
- wordpress.zuliatec.com.ve
- worthyproducts.nz (dado de baja)
- www.moothall.org.uk (dado de baja)

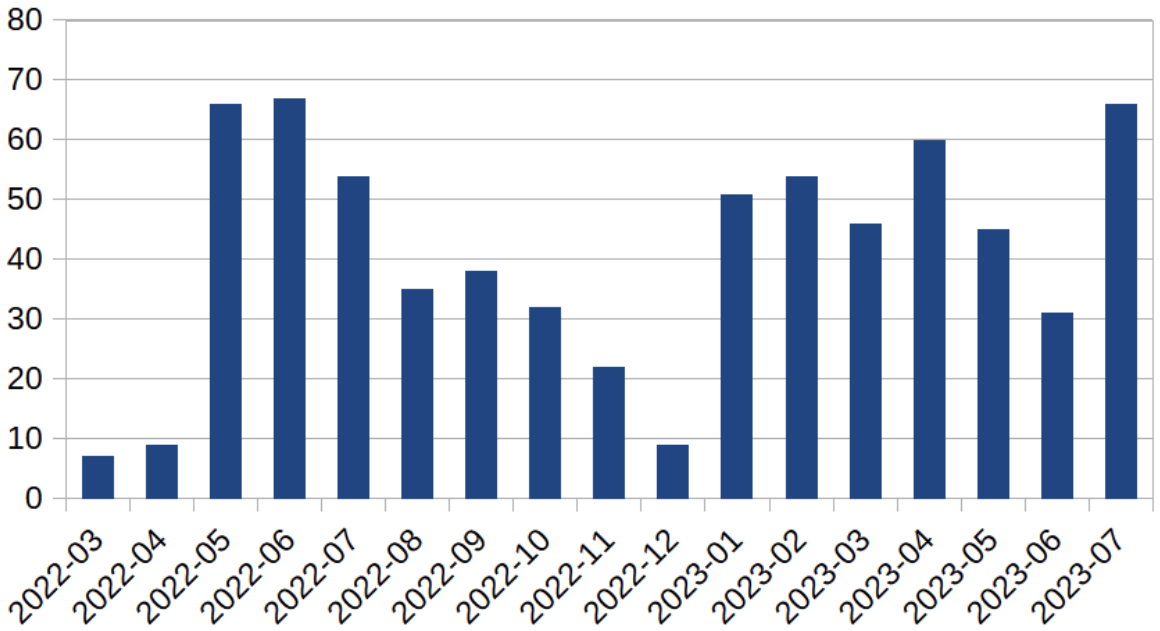
En junio y julio casi todos los dominios de pasarela fueron dados de baja

Al mantener un monitoreo constante sobre estos dominios, revisando la configuración del pack de redirección que tienen encima, podemos ir detectando cada cambio que los controladores realizan. De hecho, pudimos ver que en junio y julio casi todos los dominios de pasarela fueron dados de baja.

Al igual que en meses anteriores, se recomienda que dentro de la cadena de "takedown" de los sitios, no solo den de baja el inicio o el fin, sino que los puntos intermedios también.

FC-03

Como ya vimos en un reporte anterior[3], 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 junio podemos ver que este grupo bajó mucho su producción (y también nosotros les perdimos la pista), pero luego en julio retomaron la creación de sitios en gran medida a través del pack 0009.

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

Día inicio	C2
2023-04-13	https://r4gn4r0kr4.pescanet.info
2023-06-06	https://current-estado.info

Como habíamos visto en el reporte anterior, a principios de junio se hizo un cambio de dominio de C2 de "r4gn4r0kr4.pescanet.info" a "current-estado.info". Ambos son dominios comprados en Namecheap asociados a la misma IP: 66.29.146.71.

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

Ahora, si buscamos los dominios de C2, no tenemos tanta información, pero tenemos lo siguiente:

Día inicio	C2
2023-06-07	https://fala.current-pro.info
2023-07-18	https://fala.currentv3.info

Al analizar los C2 del pack “0010-5” vemos que tienen cierta relación con los anteriores. Todos los dominios son comprados en Namecheap y resuelven a la misma IP: 66.29.146.71.

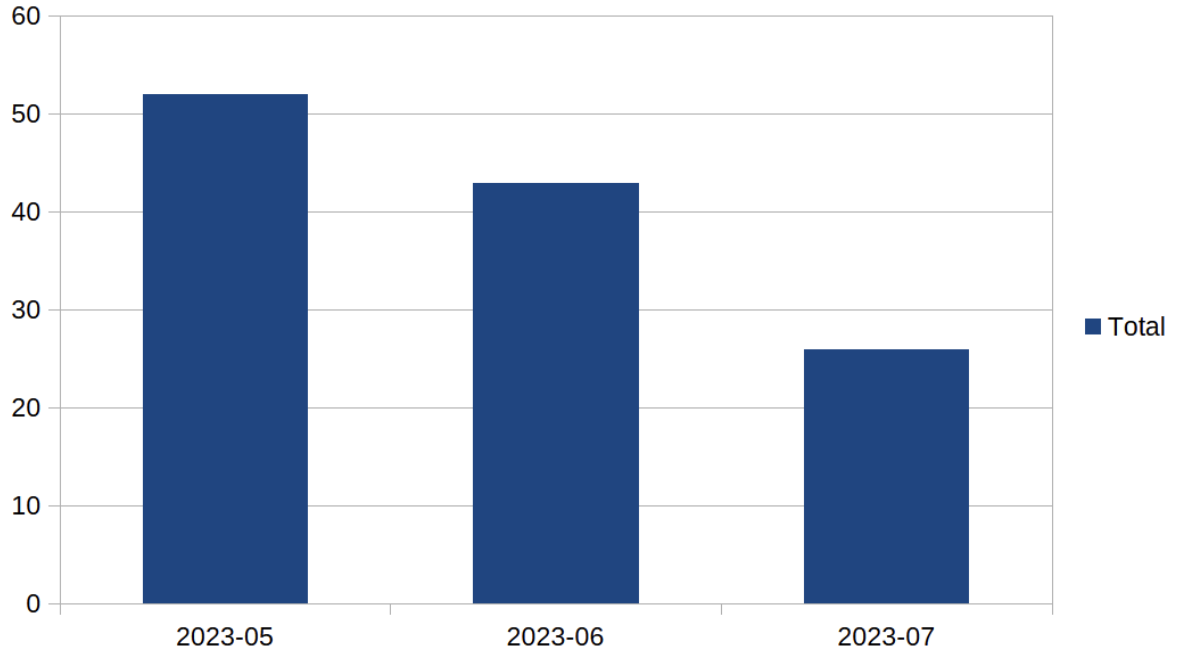
Vamos a mantener un monitoreo de esta IP para ver si es que aparecen más dominios que podrían estar asociados a campañas similares, pero se recomienda validar con el hosting para ver quién podría estar detrás de estos dominios.

Todos los dominios son comprados en Namecheap y resuelven a la misma IP: 66.29.146.71

FC-05

Como ya vimos en el reporte anterior[4], este grupo está usando solamente el pack 0099, y mantiene datos guardados en el Google Sheets a través de una única cuenta.

Al ver los datos de las detecciones de los meses de junio y julio podemos ver que han sufrido modificaciones:



Durante los meses de junio y julio se mantuvieron las detecciones, pero ahora se nota que han diversificado los dominios PaaS[5] a los cuales se están dedicando, por la baja cantidad de detecciones.

Dentro de los datos que pudimos detectar tenemos que:

- Casi todas las detecciones de ambos meses guardan los datos en la misma hoja de Google Sheets[6]
- Todas las interacciones con Google Sheets han sido con la misma cuenta y con las mismas credenciales (usuario, llave, etc.)
- El 67 % de las detecciones fueron en el servicio PaaS Replit, y el 13% fueron en el PaaS Vercel

[4] Reporte en el siguiente link: https://finsin.cl/2023/06/13/reporte-bimensual-de-phishing-abril-y-mayo-2023/

[5] PaaS significa "Platform as a Service", es un servicio de nube en el cual se provee plataforma para que los clientes suban código a ejecutar.

[6] El id de la hoja es: **1-ggHujA9RGqNbayYkgCNlexKF0mxdA8VyEeYfoZeXTg**

Esto no necesariamente quiere decir que los robos de credenciales bajaron, porque si vemos estos datos tenemos que a través del tiempo los datos han ido aumentando, y los "aliases" también:

Fecha	Total de datos	Total de aliases
2023-06-03	1870	12
2023-06-10	4270	25
2023-06-21	8076	27
2023-07-08	11652	32
2023-07-10	12286*	32
2023-08-05	29316*	40

Podemos ver que a través de los días los datos almacenados siempre van aumentando llegando a un total de casi 30.000 datos en el último cómputo para este informe.

Los datos almacenados siempre van aumentando llegando a un total de casi 30.000

Además, el total de aliases también va aumentando con el tiempo, y aunque se agregue un nuevo alias, no significa que haya más gente detrás de esta estafa, sí significa que van rotando los datos para que no se asocie necesariamente con solo usuario.

Podemos ver que tienen algún tipo de política de limpieza de los datos, porque entre el 29 y 30 de junio varios aliases[7] borraron todos los datos que habían guardado hasta el momento.

Otro suceso interesante, es que en algún momento entre el 08 y el 10 de julio un administrador de la estafa se enojó con el alias "MARCOBESTPANEL" porque en el spreadsheet que guarda los datos de ese alias colocó lo siguiente:

133690	51fbe9e0-1f5	### TUPUTAMADRE	0 TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	MARCOBESTPANEL	TUPUTAMADRE
133691	51fbe9e0-1f5	### TUPUTAMADRE	0 TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	MARCOBESTPANEL	TUPUTAMADRE
133692	51fbe9e0-1f5	### TUPUTAMADRE	0 TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	MARCOBESTPANEL	TUPUTAMADRE
133693	51fbe9e0-1f5	### TUPUTAMADRE	0 TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	MARCOBESTPANEL	TUPUTAMADRE
133694	51fbe9e0-1f5	### TUPUTAMADRE	0 TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	TUPUTAMADRE	MARCOBESTPANEL	TUPUTAMADRE
133695	51fbe9e0-1f5	### TUPUTAMADRE	0 QueCagada	JUMM	TantoParaNada	YDejandoTusDatos	QueTriste	SeriaQueLaPolicia	TeCoja	AunqueSeguro	YaEstasEnLaCarcel	MARCOBESTPANEL	TUPUTAMADRE
133696	51fbe9e0-1f5	### TUPUTAMADRE	0 QueCagada	JUMM	TantoParaNada	YDejandoTusDatos	QueTriste	SeriaQueLaPolicia	TeCoja	AunqueSeguro	YaEstasEnLaCarcel	MARCOBESTPANEL	TUPUTAMADRE
133697	51fbe9e0-1f5	### TUPUTAMADRE	0 QueCagada	JUMM	TantoParaNada	YDejandoTusDatos	QueTriste	SeriaQueLaPolicia	TeCoja	AunqueSeguro	YaEstasEnLaCarcel	MARCOBESTPANEL	TUPUTAMADRE
133698	51fbe9e0-1f5	### TUPUTAMADRE	0 QueCagada	JUMM	TantoParaNada	YDejandoTusDatos	QueTriste	SeriaQueLaPolicia	TeCoja	AunqueSeguro	YaEstasEnLaCarcel	MARCOBESTPANEL	TUPUTAMADRE
133699	51fbe9e0-1f5	### TUPUTAMADRE	0 QueCagada	JUMM	TantoParaNada	YDejandoTusDatos	QueTriste	SeriaQueLaPolicia	TeCoja	AunqueSeguro	YaEstasEnLaCarcel	MARCOBESTPANEL	TUPUTAMADRE
133700	51fbe9e0-1f5	### TUPUTAMADRE	0 QueCagada	JUMM	TantoParaNada	YDejandoTusDatos	QueTriste	SeriaQueLaPolicia	TeCoja	AunqueSeguro	YaEstasEnLaCarcel	MARCOBESTPANEL	TUPUTAMADRE

Como no sé si se va a alcanzar a leer de la imagen, coloco el texto:

[7] Los aliases son: NEJOQWERT, ALEJOPANELQWE, MARCUTOQWERT, ALEJOPANELQWERT, ALEJOUJIUHYTGRFDEWSDH, CALAMARASD, NEJOZXCV, CALAMARASDX.

“TUPUTAMADRE QueCagada JUMM TantoParaNada YDejandoTusDatos QueTriste SeriaQueLaPolicia TeCoja AunqueSeguro YaEstasEnLaCarcel MARCOBESTPANEL TUPUTAMADRE”

Lo interesante del texto, fuera del enojo, es que se repite (ese o sencillamente todas las celdas con TUPUTAMADRE), por **133.748** celdas, tapando los datos antiguos que tenía ese alias.

También aparece una sigla “JUMM” que puede ser las iniciales del nombre de alguien o sencillamente una expresión de enojo. Faltaría averiguar más, pero no tenemos cómo llegar con más información.

A pesar de este percance, los demás aliases siguen con la recolección de datos normal.

Entre el 08 y el 10 de julio un administrador de la estafa se enojó con el alias “MARCOBESTPANEL”

Uso de Telegram en estafas de Latinoamérica

Como lo habíamos visto en reportes anteriores nuestros[8][9] y además ya se ha reportado en publicaciones de medios masivos[10], Telegram es una gran plataforma tanto para distribuir kits como para almacenar los datos de este tipo de estafas.

Para comenzar, tenemos que explicar qué son los **bots** en Telegram.

Los bots son aplicaciones pequeñas que viven solamente en la aplicación de Telegram. Los usuarios interactúan con los bots a través de interfaces que permiten desarrollar cualquier servicio. Hoy en día Telegram tiene más de 10 millones de bots creados.

Estos bots, al igual que las cuentas normales, se pueden comunicar con usuarios de la aplicación, tanto como respuesta de una consulta, como a través de la API de Telegram.

Al igual que las cuentas normales, las cuentas de bot se pueden agregar a grupos o a cualquier modo de chat. Para esto, necesitamos explicar que en Telegram, tenemos distintos tipos dentro de la definición de "chats":

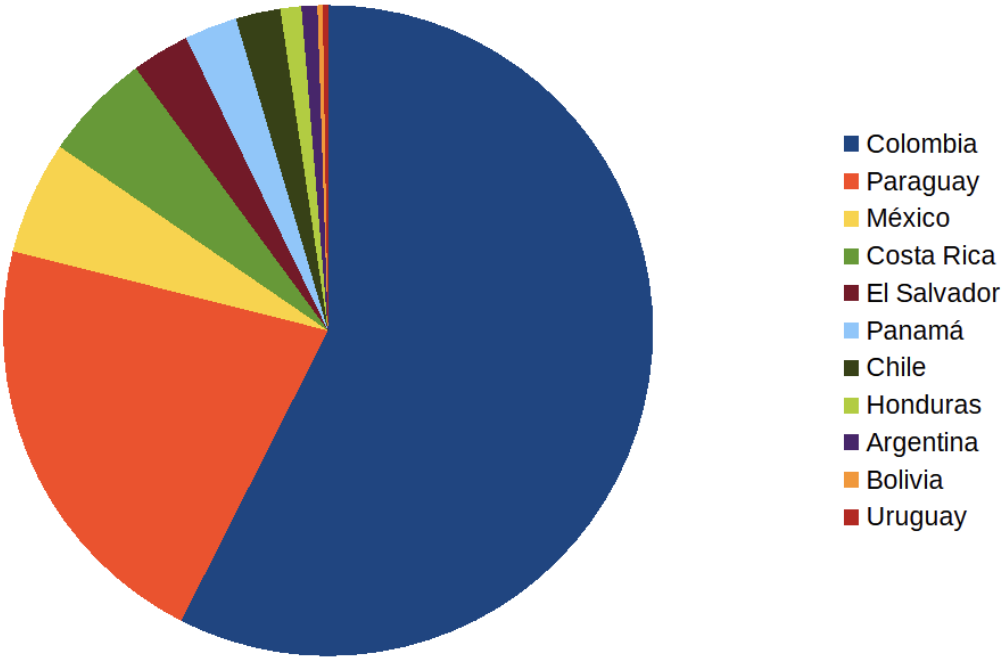
- **Chats Privados**: Es una conversación directa con otro usuario en Telegram. En este caso es una conversación entre el bot (que envía los datos) y el receptor o administrador del scam.
- **Grupos**: Son chats en donde se puede enviar un mismo mensaje a varias cuentas a la vez. Tiene un número máximo 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.

En este reporte nuevamente queremos ver el uso que estos scammers le dan a Telegram para sus estafas y cuán masivo este tipo de comunicación, no solo enfocado en una sola víctima o enfocado a un mercado, sino que a través de toda Latinoamérica.

[8] https://finsin.cl/2023/03/13/cumplimos-1-ano-de-reportes-de-phishing/
[9] https://finsin.cl/2023/04/18/reporte-mensual-de-phishing-marzo-2023/
[10] https://securelist.com/telegram-phishing-services/109383/

En estos meses hemos ido recolectando información de distintas estafas, y tenemos que múltiples instituciones en distintos países están siendo afectadas por Phishing que usan la infraestructura de Telegram.

A nivel de países tenemos que son 11 países los afectados:



Dentro de lo que hemos detectado, tenemos que Colombia lidera ampliamente el uso de este tipo de kits que Telegram por detrás, seguido de Paraguay y luego terminar con México.

Si lo vemos a nivel de "Kits", los que usan este tipo de comunicación son varios:

- 0070 y sus variantes
- 0091 y sus variantes
- 0096 y sus variantes
- 0100 y sus variantes

Uno de los datos interesantes, es que solo el kit 0070 (con sus más de 20 variantes) afecta a 10 países en Latinoamérica.

Sólo el kit 0070 (con sus más de 20 variantes) afecta a 10 países en Latinoamérica

[11]

Una de las cosas que tienen en común estos casos de Phishing es que la comunicación siempre es desde la víctima que envía la comunicación hacia el bot de Telegram, el cual le hace llegar la información al ciberdelincuente.

Cada navegador que está en el sitio de phishing genera una comunicación del bot asociado al ciberdelincuente, y cómo esta información está siendo usada por el navegador, nosotros podemos almacenarla también.

Debido a esto podemos hacer un análisis de dónde se envían esas comunicaciones.

[11] Presentación hecha para Womcy, video completo en: https://youtu.be/F2TksQC66e4

¿Qué tipo de datos hemos ido almacenando?

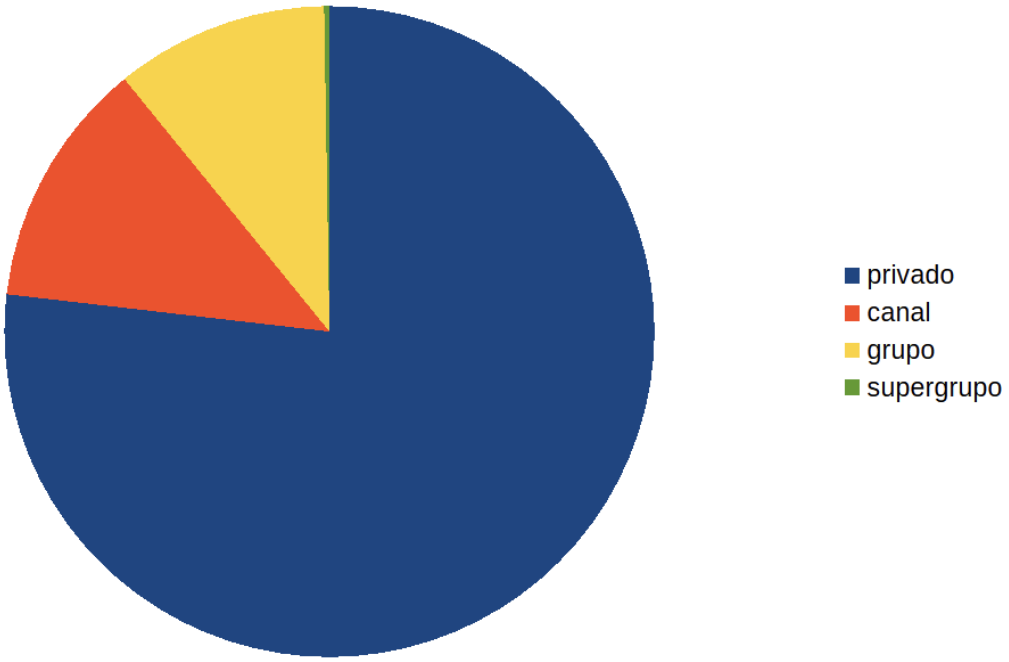
Durante todos estos meses hemos recolectado mucha información, tanto de bots, como de chats hacia donde éstos están mandando la información.

Debido a todos los sitios de estafas que hemos visto tenemos identificados a más de 300 bots, todos asociados a campañas de Phishing.

Tenemos identificados a más de 300 bots, todos asociados a campañas de Phishing

Datos recolectados	
Phishings	760
Bots	330
Chats	290

Estos bots envían los datos a ciertos chats, cada uno identificado por su “chat id”, y podemos ver la distribución de los destinos en el siguiente gráfico:



En general usan chats privados para enviar la información directamente a la cuenta controlada por el ciberdelincuente.

Uso de chats privados

Como datos interesantes tenemos que:

- Ningún bot se ha “cambiado de chat privado”, o sea, no se han reutilizado bots con más de 1 cuenta.
- Hay bots que se han usado para distintas estafas
    - Son 14 bots que han estado en phishing de 2 instituciones distintas
    - Son 3 bots que han estado en phishing de 3 instituciones distintas

Son 3 bots que han estado en phishing de 3 instituciones distintas

Este análisis nos trae datos interesantes, por ejemplo, estos son los bots de Telegram que están involucradas en estafas a 3 instituciones distintas:, con sus chats asociados:

Chat Id	Bot Id	Afectado 1	Afectado 2	Afectado 3
5440849170	5917531492	Banco 1 (CO)	Banco 1 (CR)	Banco 2 (CO)
5744855859	5640882403	Banco 1 (CO)	Banco 2 (CO)	Banco 3 (CO)
6164205956	6018228266	Banco 1 (CO)	Banco 1 (SV)	Banco 1 (AR)

Todas estas cuentas tienen estafas a “Banco 1” de Colombia, pero no siempre se quedan solamente con ese tipo de estafas, también pueden estar ligadas a estafas en otros países como, por ejemplo, el chat con id “6164205956” está ligada con estafas a bancos tanto en Colombia como en el Salvador y en Argentina.

De las cuentas de Telegram (chat_id), tenemos los nombres que les ponen a las cuentas, pero como son aliases, y no necesariamente representan a una persona, habría que buscar por fuera si es que este alias hace alguna relación a alguien.

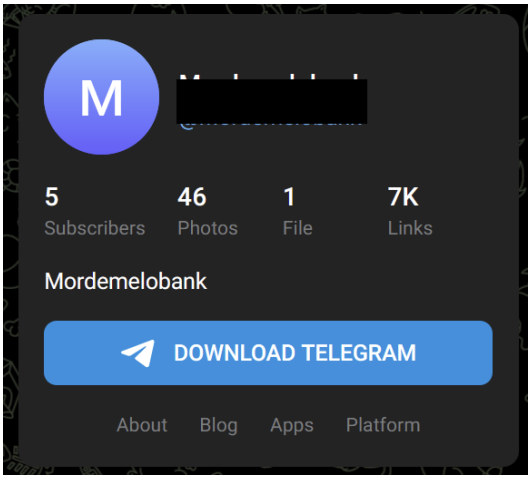
Uso de canales públicos

Si nos enfocamos en los canales que los bots están usando, tenemos que desde abril a fines de Julio tenemos un total de 39 canales con información. Estos son el repositorio de la información que los bots obtienen, siendo un punto crítico para revisar y analizar.

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.



Fecha de inicio	2023-01-12
Fecha de detección	2023-04-20
Fecha de último mensaje	2023-05-11
Cantidad de mensajes	7530 ~

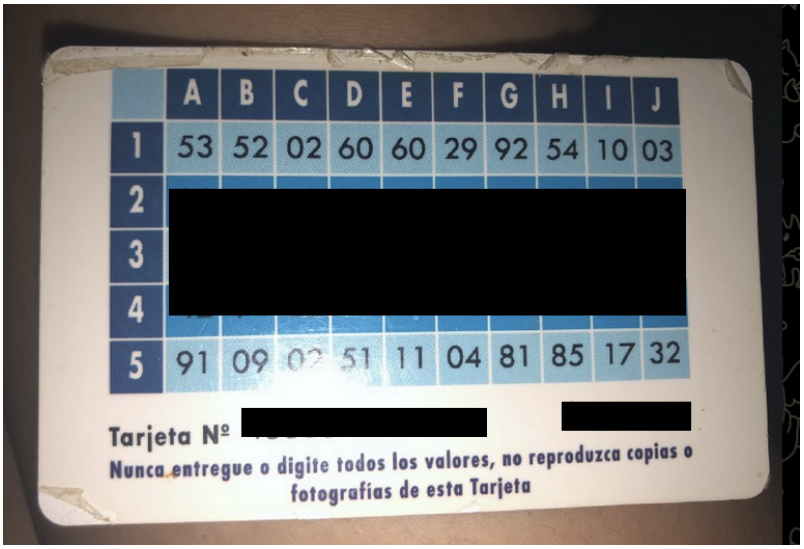
Queremos hacer un análisis en profundidad de todos los datos que hemos guardado, pero eso lo vamos a dejar para una siguiente oportunidad. En este reporte queremos ver unos casos que son de lo más interesantes.

Caso 1) Canal de Phishings en Centroamérica

El primer caso interesante es el de este canal, el que lo detectamos como parte de la comunicación de por lo menos 2 sitios de phishing en abril, uno de un banco en Costa Rica y otro de un banco en Colombia.

Pero si vemos los datos que han sido guardados en el canal tenemos que ha sido parte de muchos más scams de Phishing que incluyen otra institución financiera en Costa Rica y otra en Colombia, una de Ecuador, una de Honduras y varias otras más.

Además, otro dato interesante, es que en el resumen del canal, vemos que tienen enviadas 46 fotos. Eso es porque usan el kit 0096, que en este caso afecta a un banco de Costa Rica. En este kit le piden al usuario subir una foto de su tarjeta de coordenadas, y hay varios clientes que lo hicieron, por ejemplo:

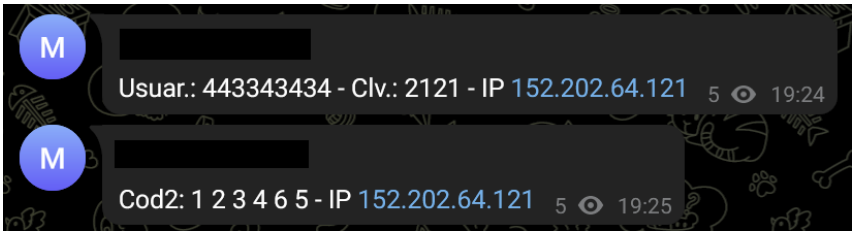
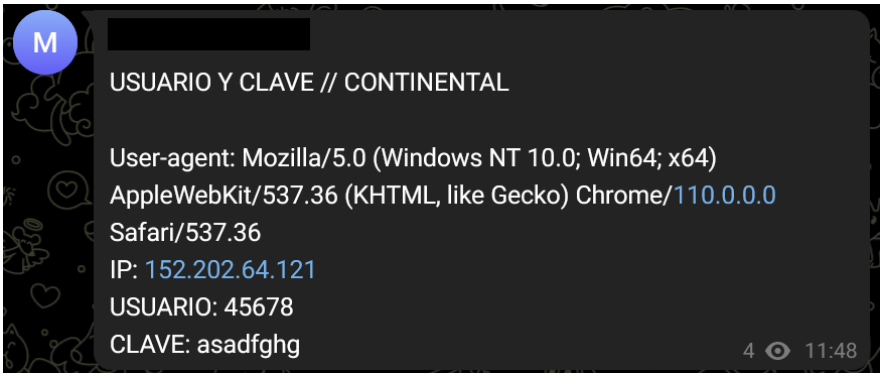
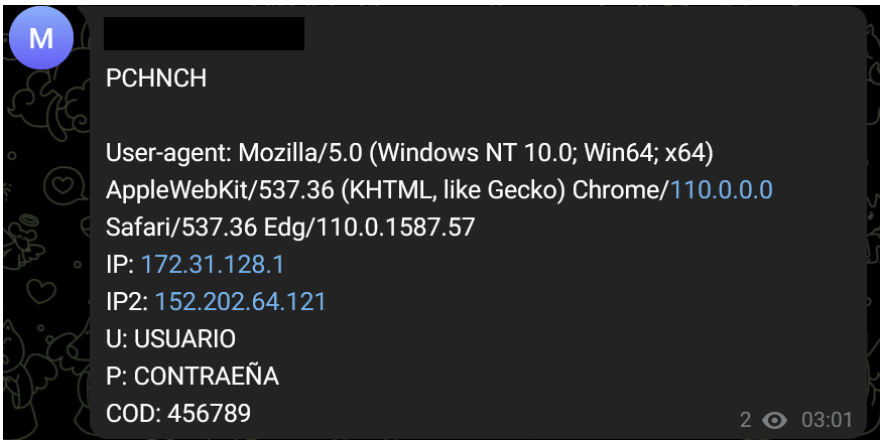


En la tarjeta dice: "Nunca entregue o digite todos los valores, no reproduzca copias o fotografías de esta Tarjeta"

¡Y en la tarjeta dice "**Nunca entregue o digite todos los valores, no reproduzca copias o fotografías de esta Tarjeta**"! Falta leer ese mensaje.

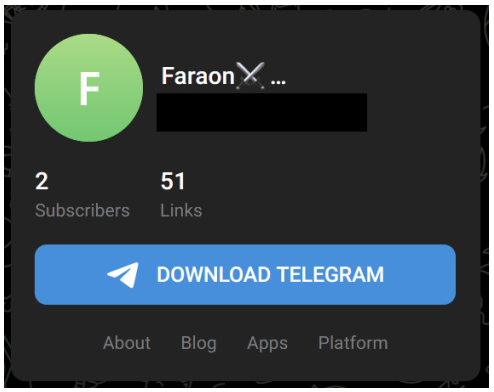
En este canal se ven bastantes mensajes entre los ciberdelincuentes, y los interesantes son los que podrían delatar su ubicación, por ejemplo, tenemos que la IP 152.202.64.121 se repite bastante en los mensajes, y en mensajes que no tienen mucha relevancia.

Por ejemplo:

Fecha	Mensaje
24 de febrero	
25 de febrero	
01 de marzo	

Estos mensajes parecen ser de prueba, principalmente por los datos “basura” que envía y porque están al inicio de la vida del canal. Creemos que detrás de esa IP está uno de los controladores del canal.

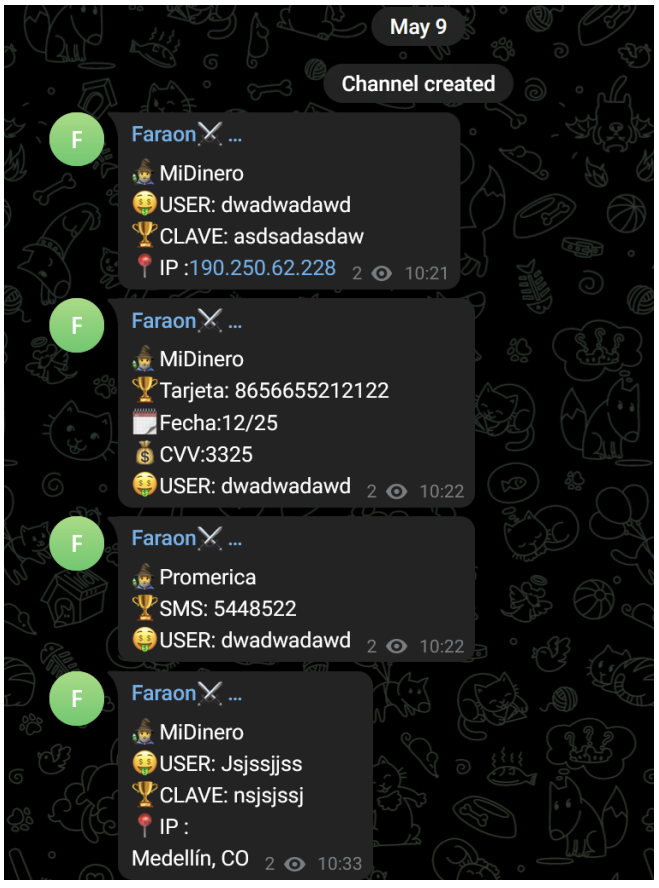
Caso 2) Canal de Phishings para víctimas de Uruguay



Fecha de inicio:	2023-05-09
Fecha de detección	2023-05-11
Fecha de último mensaje	2023-05-18
Cantidad de mensajes:	72

Este caso es interesante, no tanto por la cantidad de víctimas, sino que por el origen de los controladores.

Este es un canal que es parte de la comunicación de sitios de Phishing que apuntan a una institución financiera en Uruguay, pero lo interesante son los primeros mensajes, lo que se asume que son de prueba:



En estos mensajes se puede ver que los datos no son correctos ni relevantes, pero un dato que salta a la vista es que la IP en cuestión no es de Uruguay, sino que es de Colombia.

Todas las demás IPs son de personas en Uruguay, por lo que se asume que es de los controladores.

Otro dato interesante, es que los mensajes tienen el título de la institución afectada, y están en sets de a 3:

1. envío de usuario y password
2. envío de datos de tarjeta
3. envío de datos de SMS y correo de usuario

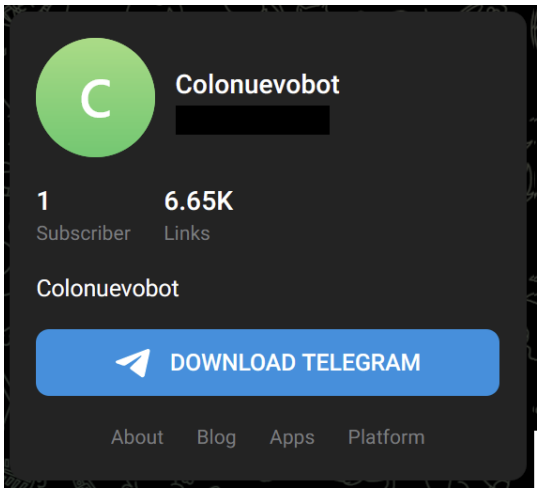
En este caso el tercer paso no tiene el nombre de la institución afectada, de hecho reutiliza el nombre de una institución financiera de Costa Rica.

Se puede asumir con alto grado de confianza que este Phishing estuvo organizado por una persona en Colombia contra una institución uruguaya reutilizando un kit que fue usado para atacar una institución en Costa Rica.

Este Phishing estuvo organizado por una persona en Colombia contra una institución uruguaya

En los mensajes salen datos potencialmente reales de los clientes, por lo que es importante que la institución afectada haga la investigación para validar que éstos no sean utilizados por terceros.

Caso 3) Canal de Phishing reanimado

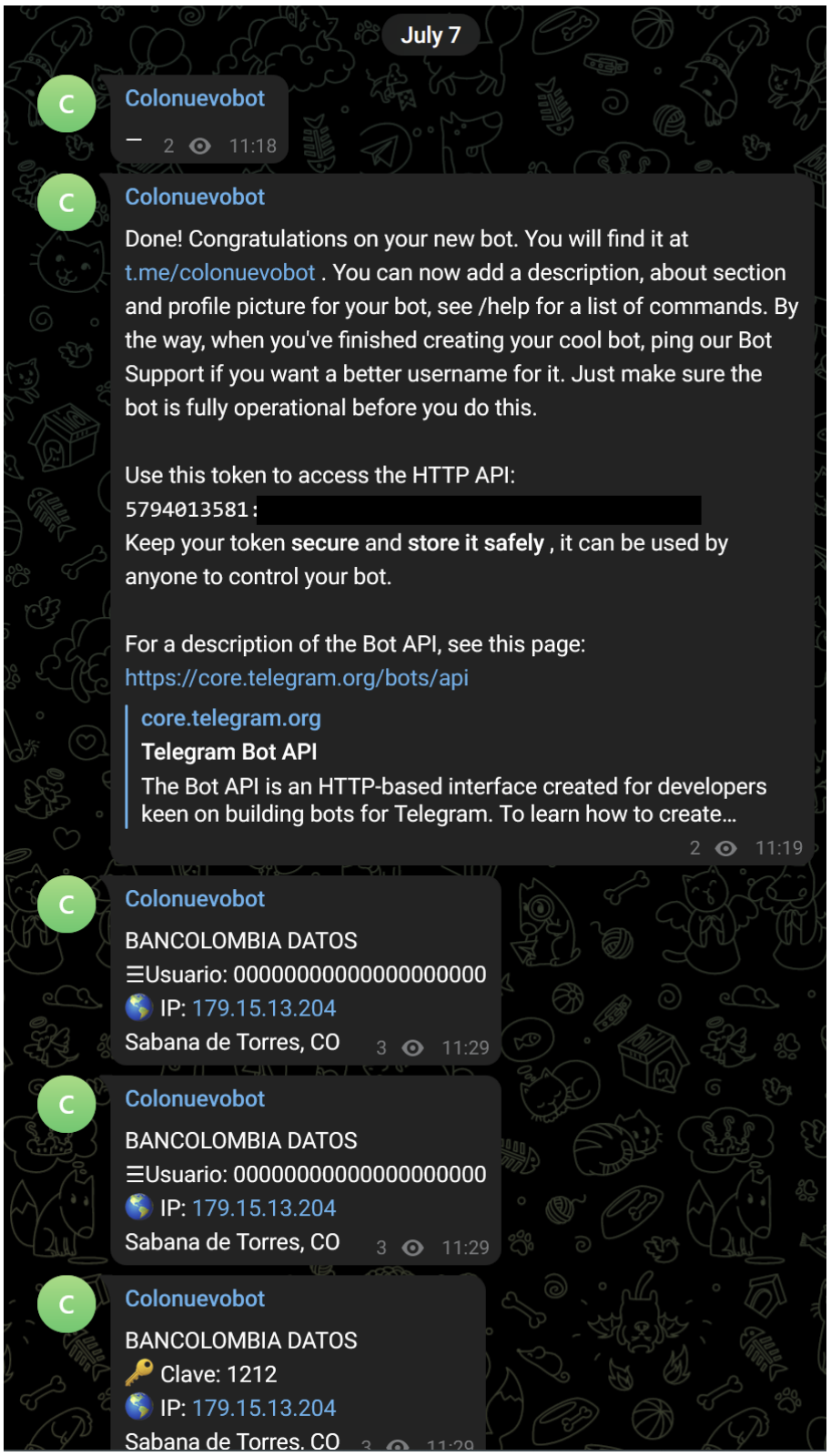
<table>
<tr>
<td rowspan="4"> 
</td>
<td>Fecha de inicio:</td>
<td>2022-11-04
2023-07-07</td>
</tr>
<tr>
<td>Fecha de detección</td>
<td>2022-11-24
2023-07-22</td>
</tr>
<tr>
<td>Fecha de último mensaje</td>
<td>2023-08-06</td>
</tr>
<tr>
<td>Cantidad de mensajes:</td>
<td>6600~</td>
</tr>
</table>

Este caso es interesante, porque es un canal que comenzó a finales del 2022, pero duró poco, y a principios del 2023 tuvo una pausa en el contenido. En esta primera etapa usan un kit genérico, que no estamos seguros a qué institución están afectando, pero luego de aproximadamente 100 datos extraídos deja de recibir información.

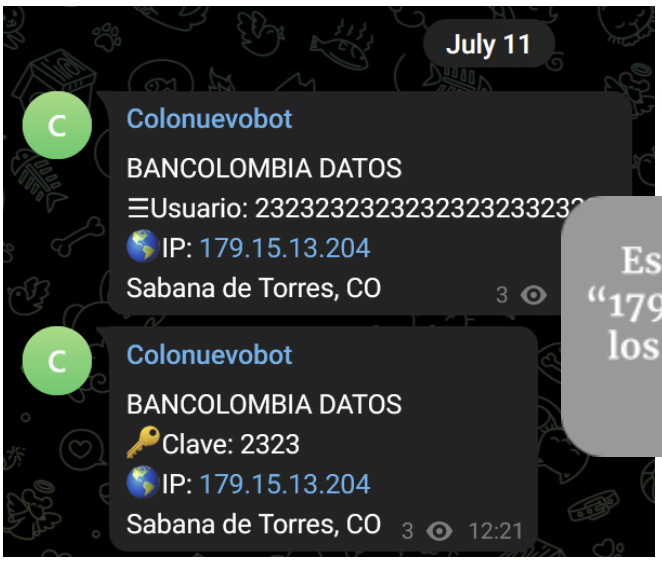
Luego, a principios de julio, aparece un mensaje con texto anómalo, seguido de una respuesta muy típica luego a la creación de un bot con @BotFather[12], que es el mismo bot que está publicado en el sitio de estafa.

Después de ese mensaje aparecen varios mensajes asociados al kit de Phishing dirigido a la institución financiera en Colombia. Asumimos entonces que el canal se reactivó con este nuevo kit, y nuevamente al revisar los primeros mensajes después de este cambio vemos que se puede distinguir claramente unos mensajes que no son de víctimas, son de prueba:

[12] https://sendpulse.com/knowledge-base/chatbot/telegram/create-telegram-chatbot



Este caso nos dice que es muy probable que la IP "179.15.13.204" sea de uno de los controladores detrás de esta estafa.. Más aún si buscamos otras instancias en donde esté la misma IP, los datos también parecen ser de prueba:



Descontando los mensajes de prueba, tenemos que en el período de 20 días, tiene 6500 datos de personas que usaron sus sitios web.

IPs interesantes

Si analizamos las IPs anteriores tenemos lo siguiente:

- Para la IP **152.202.64.121** (Bogotá, Colombia) del caso 1, sólo existe dentro del contexto del primer canal, si es parte de los controladores de esa estafa, no está ligada a ninguna otra, por lo que baja su probabilidad.
- Para la IP **190.250.62.228** (Ibagué, Colombia) del caso 2, también sólo existe dentro del contexto del segundo canal, si es parte de los controladores de esa estafa, no está ligada a ninguna otra, por lo que baja su probabilidad.
- Para la IP **179.15.13.204** (Sábana de Torres, Colombia) del caso 3, ésta sí fue identificada como parte de otros canales y de otras estafas. Está presente en por lo menos otros 3 canales, con distintos tipos de entidades afectadas: principalmente de Colombia con 2 instituciones distintas, pero también de México. Todos los mensajes son entre el 01 y el 28 de julio, y todos son de prueba o con datos irrelevantes.

Como tenemos acceso a muchos de los datos de los canales aquí expuestos nos dedicamos a ver las otras IPs que más se repetían con mensajes tipo prueba y nos aparecieron otras como:

- La IP **206.84.81.12** (Medellín, Colombia), está presente en 7 canales distintos de estafas (entre ellos los mismos 4 que la IP del caso 3), todos con mensajes de prueba. Esto podría hablar de que ambas IPs tienen personas relacionadas por detrás.
- La IP **206.84.81.121** (Medellín, Colombia), está presente en 3 canales distintos de estafas (de los cuales se repite en 2 con los anteriores). Esto también habla de que la IP es parte de la comunidad de estafas, además que siendo de la misma ciudad que la anterior (y en diferencia solamente de un octeto) habla de que probablemente vivan cerca y/o se conozcan.

Tenemos varias IPs interesantes que se van repitiendo, y queremos partir con el análisis de estas 5, porque todas tienen mensajes de prueba en los canales.

Esto habla de una mala administración de la estafa, porque están exponiendo su IP de casa (o de celular) personal para hacer las pruebas, lo que haría mucho más fácil una investigación policial.

Además se puede concluir que los ciberdelincuentes, o por lo menos, los controladores de este tipo de estafa son siempre personas en Colombia, aunque los phishing están dirigidos a personas de otros países.

Se puede concluir que los controladores de este tipo de estafa son siempre personas en Colombia

Palabras finales

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 Abril-Mayo 2023:

- https://finsin.cl/2023/06/13/reporte-bimensual-de-phishing-abril-y-mayo-2023/

Reporte Marzo 2023:

- https://finsin.cl/2023/04/18/reporte-mensual-de-phishing-marzo-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/