FINSIN

Reporte de Phishing

Enero 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 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.

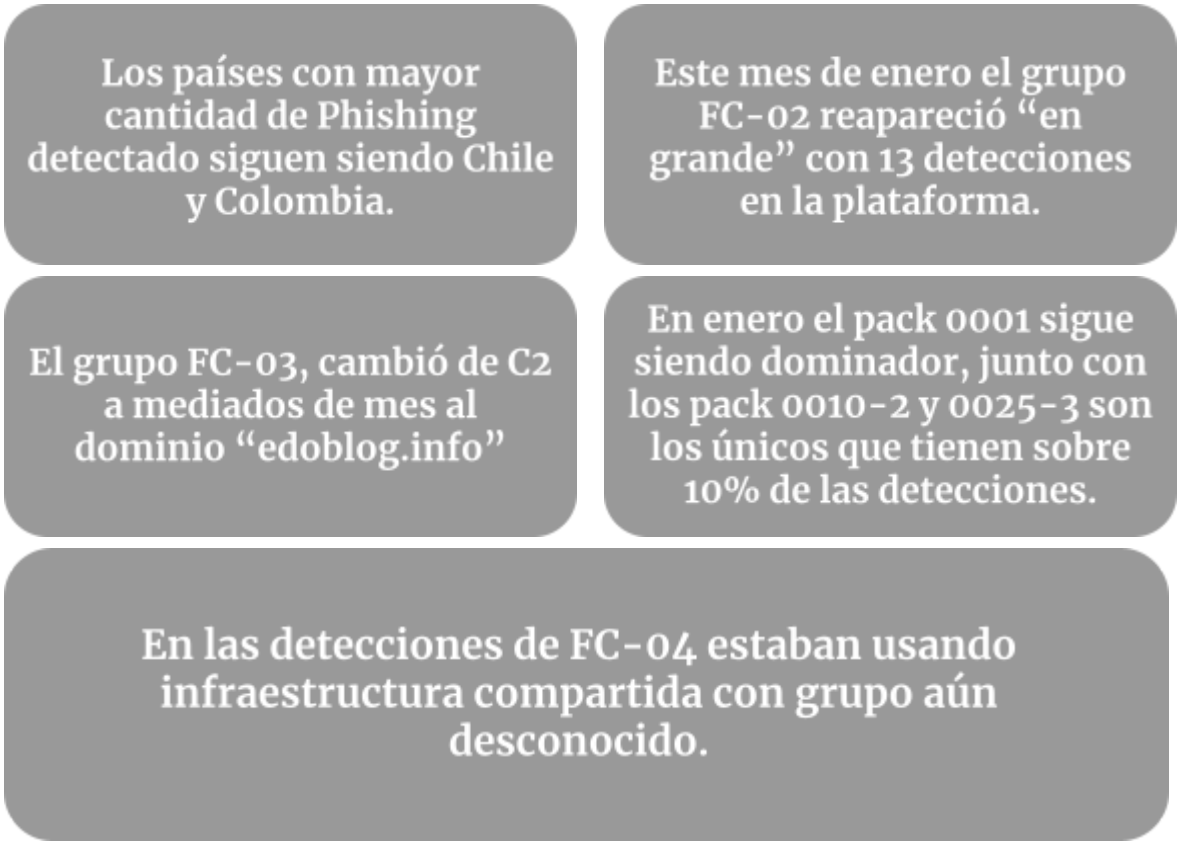
Para ello, decidimos generar un sistema automático con la capacidad de detectar, clasificar y agrupar los sitios de phishing que aparecen, logrando identificar patrones que nos permitan definir si un sitio es o no un Phishing y además a qué tipo de kit está asociado.

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 Enero[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

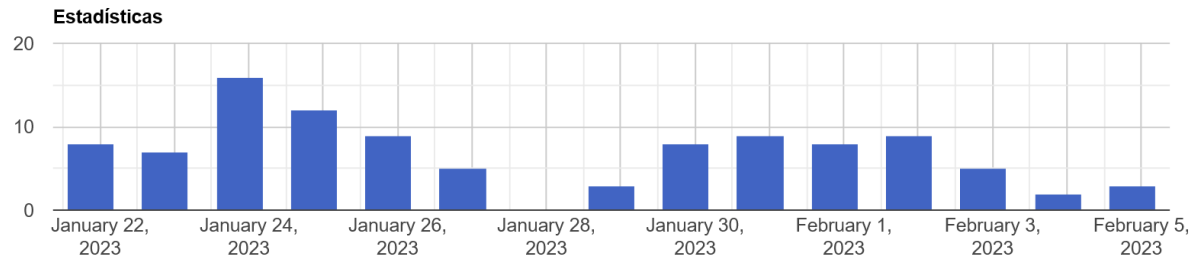
Phishing Checker

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.

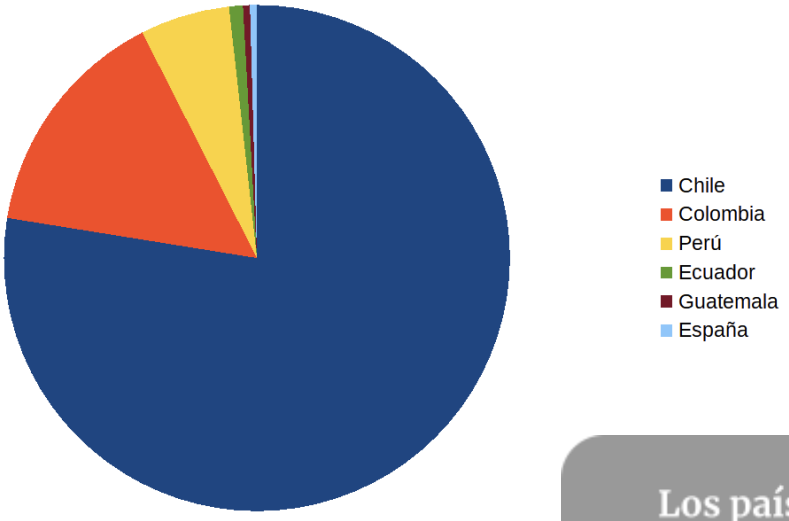
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Enero 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 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

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



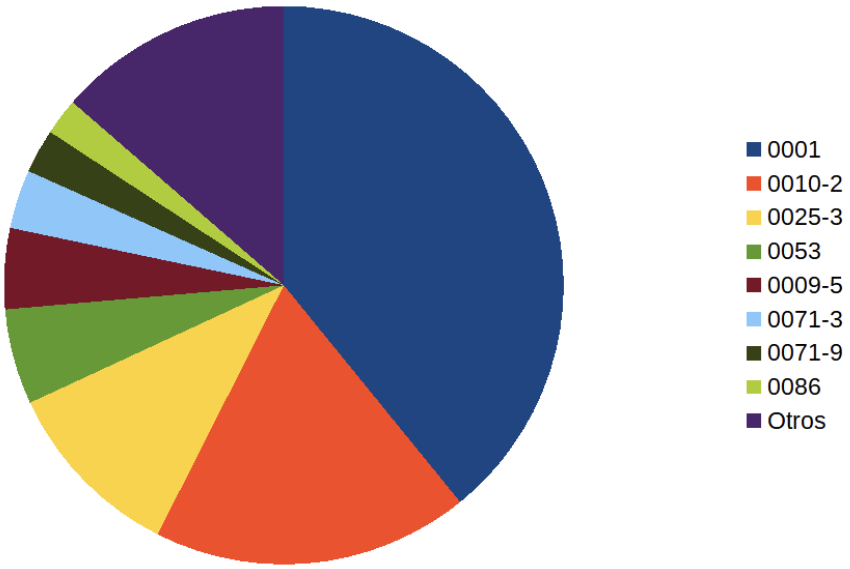
País	Porcentaje
Chile	77,53%
Colombia	14,98%
Perú	5,73%
Ecuador	0,88%
Guatemala	0,44%
España	0,44%

Los países con mayor cantidad de Phishing detectado siguen siendo Chile y Colombia.

Podemos ver que se mantiene la tendencia de que los países con mayor cantidad de Phishing detectados siguen siendo Chile y Colombia.

Datos de kits

En enero logramos agregar 3 kits nuevos y 8 variantes nuevas de Phishing que ya conocíamos antes. Si graficamos los datos del mes asociados a los kits de phishing, podemos ver que queda un poco parecido a los meses anteriores:



Pack	Porcentaje
0001	39,15%
0010-2	30,07%
0025-3	17,48%
0053	9,09%
0009-5	7,69%
0071-3	5,59%
0071-9	4,20%
0086	3,50%
Otros	22,38%

El pack 0001 sigue siendo el dominador, como en muchos meses anteriores, pero cada vez por menos. Vuelve a aparecer el kit 0010-2 con casi un tercio de las detecciones, y junto con el 0025-3 son los únicos que tienen más del 10% de las detecciones del mes.

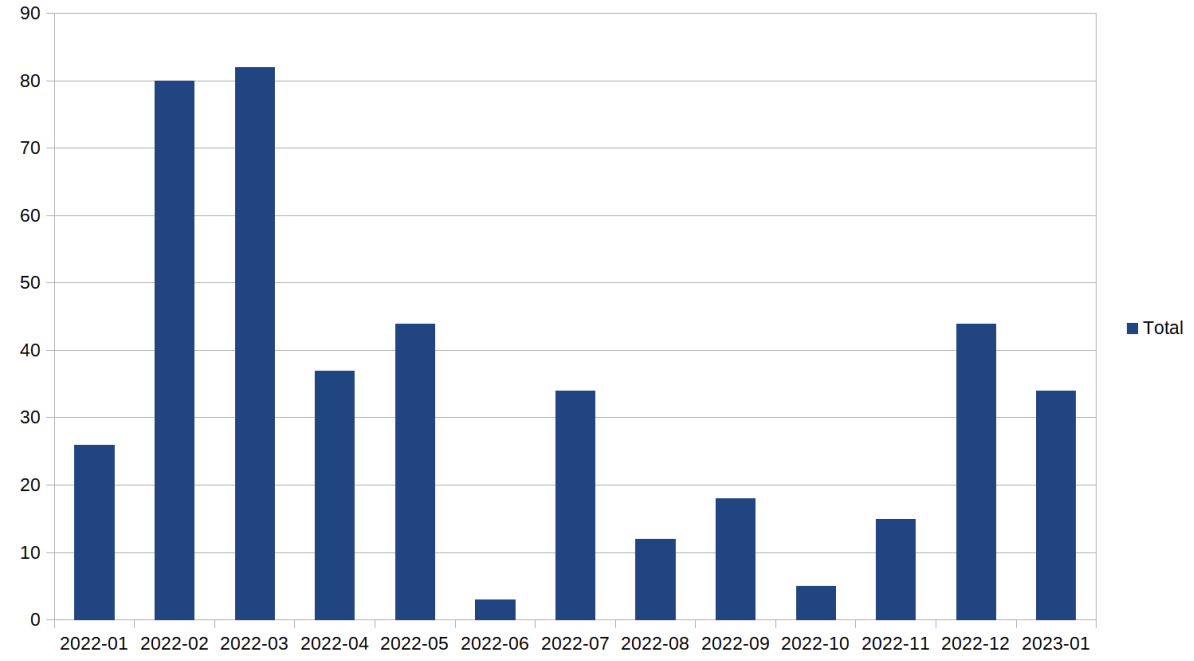
Actualización de Fishers Constantes (FC)

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



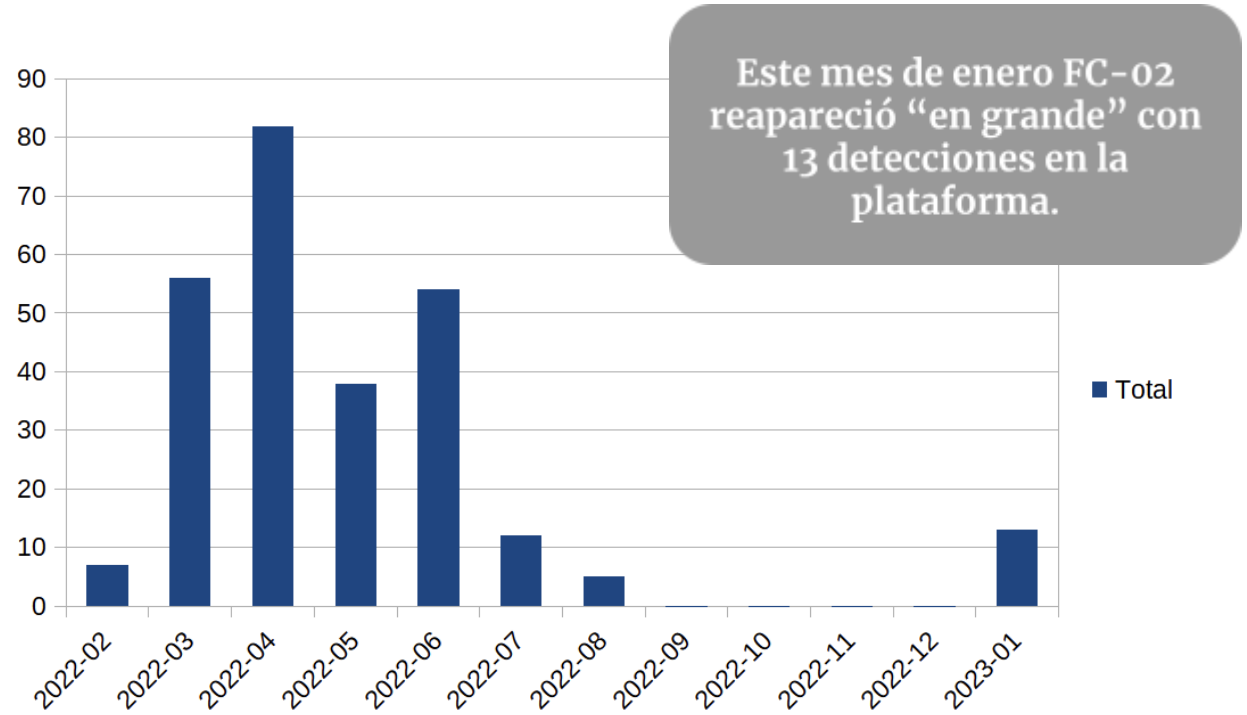
El grupo se ha mantenido en los últimos meses con sobre 30 detecciones al mes, y sigue usando la misma arquitectura y los mismos kits de redirección y de phishing.

Todavía no llega a los peaks vistos a inicios del 2022, pero se espera que este grupo continúe su actividad por varios meses más.

[2] Este grupo fue definido en el reporte de febrero: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/

FC-02

Este grupo que revisamos en el reporte de abril[3] no tiene mucha actividad, de hecho desde agosto no lo veíamos. Este mes de enero reapareció "en grande" con 13 detecciones en la plataforma.



Aparte de lo impresionante de encontrar el mismo patrón de comportamiento, encontramos también nuevos dominios de pasarela usados con su resolución de DNS Pasivo de Virustotal:

Dominio	**Resolución de DNS Pasivo**
imperios.top	Solo IPs de Cloudflare: 172.64.80.1, 172.67.215.24 y 104.21.78.22
aztecamusica.com	IPs de Cloudflare recientemente: 172.64.80.1, 104.21.20.232 y 172.67.194.192; y el 2018 otra IP 195.149.84.109
surlimpieza.com	Solo IPs de Cloudflare: 172.64.80.1, 172.67.169.193 y 104.21.27.213
maletines.life	Solo IPs de Cloudflare: 172.67.213.234 y 104.21.37.222

[3] El reporte está aquí:
https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/

El hecho de que se esté usando IPs de Cloudflare, solo nos indica que son usuarios de ese servicio, pero nada más.

La gracia de estos dominios es que, al ser usados de pasarela, solo eran parte de la arquitectura. Tenemos ejemplos de uso con distintos scripts, por ejemplo:

Todos estos dominios mencionados, ahora no están prestando servicios

El 25 de enero[4] tenemos que se usan 2 de estos dominios antes de llegar al sitio de scam final:

N° Redirección	URL Redirección
0	https://aztecamusica.com/santa.php
1	https://offilimpio.info/santa.php
2	https://offilimpio.info/index.php
3	https://bancosantander-cl.net-sms-cl.info/
4	https://bancosantander-cl.net-sms-cl.info/1674649642/portada/personas/home.asp

Ambos dominios se usan para llegar al siguiente, pero el dominio final es el de phishing, el cual también está detrás de Cloudflare (¿deberían hacer algo al respecto, no?).

En otro ejemplo, el 24 de enero[5], se usan otros 2 de estos dominios para las redirecciones:

N° Redirección	URL Redirección
0	https://surlimpieza.com/itau.php
1	http://aztecamusica.com/itau
2	http://aztecamusica.com/itau/
3	https://bencoitau.cl-ets.top/
4	https://bencoitau.cl-ets.top/1674589160/wps/portal/newolb/ ... 2dBISEvZ0FBIS9nQSEh

Como vemos, estos dominios se usan con un script en php al final o con una ruta, que gracias al .htaccess también resuelven a un script .php, y finalmente se llega al sitio de scam.

---

[4] Link al reporte completo:
https://phishing.finsin.cl/list.php?query=111b098cf23225690b6ace5fdb43670999b498e401ca274897cf3e6797d8fb86

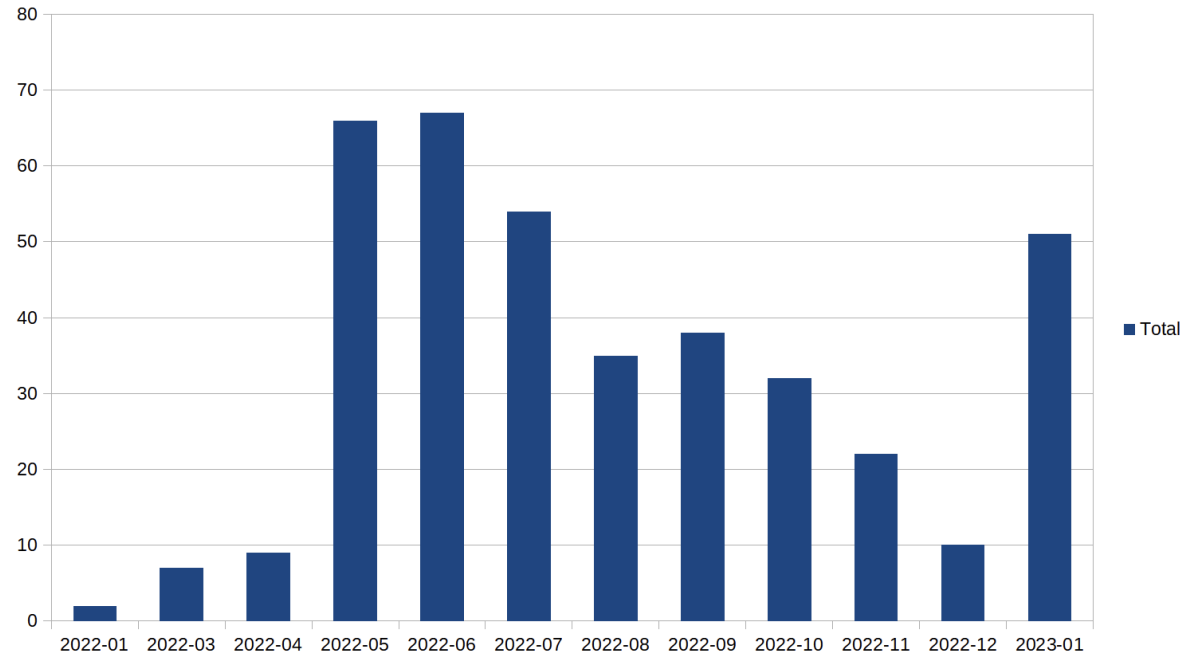
[5] Link al reporte completo:
https://phishing.finsin.cl/list.php?query=1dce5e9a850066a2ed6d857a4e1eb4c59cb5dec1a4f0ceea737f60c3f34f2cd0

Todos estos dominios mencionados, ahora no están prestando servicios, por lo que tenemos que esperar a que volvamos a encontrar más de estos mismos.

Aunque este comportamiento no lo vimos "en masa" este mes, tuvimos un resurgimiento de un comportamiento que no veíamos hace mucho tiempo. Tendremos que esperar un poco más para ver si siguen activos, o vuelven a esconderse.

FC-03

Como ya vimos en el reporte anterior[6], este grupo está usando 2 packs: el 0009 y el 0010 (con sus respectivas variantes), si vemos sus acciones este mes, podemos ver que subieron mucho las detecciones.



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

2023-01-01	0009-5	C2	https://r4gn4r0kr4.ehloqservices.info
2023-01-02	0009-5	C2	https://r4gn4r0kr4.ehloqservices.info
2023-01-04	0009-5	C2	https://r4gn4r0kr4.ehloqservices.info
2023-01-09	0009-5	C2	https://r4gn4r0kr4.ehloqservices.info
2023-01-11	0009-5	C2	https://r4gn4r0kr4.ehloqservices.info
2023-01-16	0009-5	C2	https://r4gn4r0kr4.edoblog.info
2023-01-17	0009-5	C2	https://r4gn4r0kr4.edoblog.info

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

2023-01-20	0009-5	C2	https://r4gn4r0kr4.edoblog.info
2023-01-24	0009-5	C2	https://r4gn4r0kr4.edoblog.info

Podemos ver que hubo un cambio alrededor del 16 de enero (no tuvimos detecciones todos los días del kit), pasaron de "r4gn4r0kr4.ehloqservices.info" a "r4gn4r0kr4.edoblog.info".

Es interesante que dejaran el dominio que habían creado justamente el mes pasado para llegar ahora a "edoblog.info", y como anteriormente, siguen usando el mismo subdominio "r4gn4rokr4". Al igual que en casos anteriores, el dominio está inscrito en Namecheap con protección de identidad[7], por lo que no podemos tener más información.

Si buscamos los dominios de C2, pero en las variantes del pack 0010 encontramos algo más interesante:

2023-01-02	0010-2	C2	https://worker-fala.ehloqservices.info
2023-01-04	0010-2	C2	https://worker-fala.ehloqservices.info
2023-01-05	0010-2	C2	https://worker-fala.ehloqservices.info
2023-01-06	0010-2	C2	https://worker-fala.ehloqservices.info
2023-01-07	0010-2	C2	https://new-main.ehloqservices.info
2023-01-09	0010-2	C2	https://new-main.ehloqservices.info
2023-01-10	0010-2	C2	https://new-main.ehloqservices.info
2023-01-11	0010-2	C2	https://new-main.ehloqservices.info
2023-01-16	0010-2	C2	https://pro21-mainfala.edoblog.info
2023-01-17	0010-2	C2	https://pro21-mainfala.edoblog.info
2023-01-22	0010-2	C2	https://pro21-mainfala.edoblog.info
2023-01-23	0010-2	C2	https://pro21-mainfala.edoblog.info
2023-01-25	0010-2	C2	https://pro21-mainfala.edoblog.info
2023-01-31	0010-5	C2	https://new-falav2.edoblog.info

[7] ¿A alguien le sirve el whois estos días para perseguir actores delictivos?

Podemos ver que a mediados de mes (el mismo 16 de enero), cambian al mismo dominio anterior “edoblog.info”, pero usando distintos subdominios.

Además, tenemos que a finales de mes hubo un cambio en la forma que detectamos a este kit, porque ahora (por lo menos hasta la edición de este reporte) estamos usando el pack 0010-5. No es un cambio mayor en la funcionalidad (por eso no usamos un número nuevo), sino que es solamente un cambio estético del kit.

El grupo FC-03, cambió de C2 a mediados de mes al dominio “edoblog.info”

Veamos un poco más detalladamente los dominios (sin subdominios) usados por FC-03 como parte de sus C2, con esto tenemos los siguientes:

Duración de dominio	**Dominio usado**
2022-05 a 2022-07	herokuapp.com
2022-07 a 2022-12	ehloq.xyz
2022-12 a 2023-01	ehloqservices.info
2023-01 a la actualidad	edoblog.info

El dominio de herokuapp.com, es de un servicio PaaS (Platform as a Service) conocido, por lo que no lo podemos asociar al grupo, pero los demás sí.

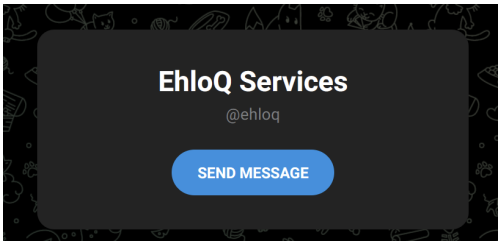
De hecho, llama la atención que se repita “ehloq” en 2 de esos dominios, porque es un alias que hemos estado siguiendo. De hecho, gracias al apoyo de investigadores aliados, podemos tener un poco más de información sobre este alias.

El usuario @ehloq

Este usuario es bastante interesante, porque al parecer es "importante" a nivel de este tipo de estafas, como tiene varios dominios asociados a su alias, pensamos que puede estar proveyendo esto como algún tipo de servicio.

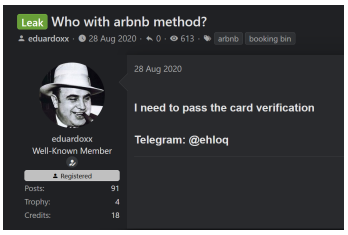
No tenemos este usuario completa o correctamente identificado, pero tenemos algunos datos interesantes. Si nos guiamos por el usuario @ehloq[8] de Telegram, tenemos la siguiente información:

- Asocia su cuenta a servicios, no tenemos claro necesariamente qué tipo de servicios



El usuario @ehloq parece ser un carder conocido a nivel latinoamericano.

- Fue asiduo al sitio "pandora.to", un foro de carding en español ahora difunto[9]. En este foro, tenía el alias de "tito2", pero en sus mensajes dejaba el contacto de Telegram anterior "@ehloq"[10].
- Mantiene cuenta para hacer sitios de phishing y estafas en foro FSSQUAD[11] ex-Fraudsters Crew, en donde deja su contacto de Telegram "@ehloq".



Lamentablemente, no tenemos mucha más información concreta sobre el alias, pero si este tipo de información le sirve a alguien, nos complace proveerla.

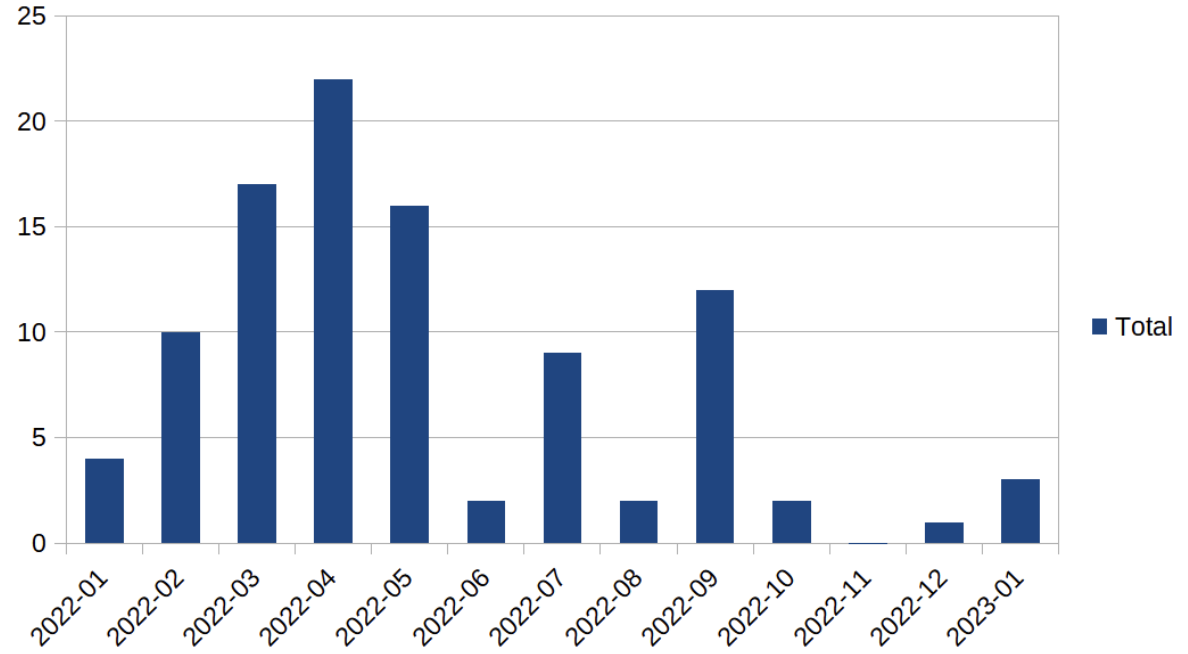
---

[8] Se puede ver acá: https://t.me/ehloq
[9] Se puede ver la última copia del sitio guardado en archive.org en: https://web.archive.org/web/20221007020325/https://pandora.to/
[10] Un ejemplo está en el cache de Google: https://webcache.googleusercontent.com/search?q=cache:yDJW6cdHN3wJ:https://pandora.to/members/wirldread.41348/&cd=2&hl=es-419&ct=clnk&gl=cl&client=firefox-b-d
[11] Se puede ver su historial en: https://fssquad.com/members/eduardoxx.61999/#recent-content

FC-04

Este grupo que revisamos en el reporte del mes de octubre[12] no tiene mucha actividad, pero es muy interesante la información que podemos tener de ellos.

Si vemos su actividad en los últimos meses del año, en noviembre no tuvimos ningún sitio con su kit y en diciembre solo 1:



En enero tuvimos solo 3 detecciones:

Num	Fecha	Sitio detectado
1	2023-01-24	https://surfsantnder.info/pagina/UI.Web.Login/login.asp
2	2023-01-19	https://aranzazanew.top/pagina/UI.Web.Login/login.asp
3	2023-01-19	https://kulikuliplop.club/pagina/UI.Web.Login/login.asp

Lo asociamos a este grupo porque están usando el kit 0003-2 (una variante del kit que sabemos que usan). Estas detecciones fueron todas muy similares, porque usan el mismo kit, y están clonando la misma página del mismo banco en Chile.

[12] El reporte está en el siguiente link:
https://finsin.cl/2022/11/14/reporte-mensual-de-phishing-octubre-2022/

Si vemos los datos de los implicados tenemos unos correos conocidos.

Num	Correos asociados
1	akimicash@gmail.com,logosami2022@gmail.com
2	akimicash@gmail.com,logosami2022@gmail.com
3	akimicash@gmail.com,logosami2022@gmail.com

Tenemos los mismos correos que habíamos visto anteriormente, y se repiten en las 3 detecciones, reforzando que estos correos están activos y siendo usados para este tipo de estafas.

Lo interesante de estas detecciones, es que estaban usando infraestructura compartida con otro grupo. Por ejemplo, si vemos los sitios de redirección (para ver la infraestructura usada) del reporte de la detección número 3:

En nuestras detecciones de FC-04, estaban usando infraestructura compartida con grupo aún desconocido.

N° Redirección	URL Redirección
0	https://ucmstudio.info/cuentas/cuenta-test/
1	https://kulikuliplop.club/
2	https://kulikuliplop.club/pagina/UI.Web.Login/login.asp

Vemos que usan el dominio "ucmstudio.info", como redirección, de hecho, en ese dominio está el kit que nosotros llamamos "0006-1", el cual solamente es una pasarela para la redirección al sitio final de scam.

Si buscamos en la plataforma las detecciones tenemos con este dominio[13] tenemos que siempre ha sido usado igual, como pasarela de redirección, y que ha estado activo por lo menos desde el 12 de diciembre.

[13] Para buscar en la plataforma utilizamos la barra de búsqueda dentro de la página principal.

Phishing (Reporte)	Query: https://ucmstudio.info/cuentas/cuenta-test/ Final: https://newbailando.com/1671500772/imagenes/_perso...	172.67.135.231	Terminado 19-12-2022, 22:46:33
Phishing (Reporte)	Scam: https://ucmstudio.info/	213.136.93.164	Terminado 12-12-2022, 22:54:38
Phishing (Reporte)	Query: https://ucmstudio.info/activacion/cuenta-aotq/ Final: https://celebrafans.com/1670896332/imagenes/_perso...	104.21.4.90	Terminado 12-12-2022, 22:52:41

Como este dominio es solamente una pasarela, y mientras esté funcionando podemos monitorearlo, hemos seguido sus cambios, y tenemos bastante evidencia de su uso. Pero el uso que se le estaba dando era totalmente distinto, era para redirigir a sitios que llevan a scams de otro banco en Chile, con un kit que nosotros detectamos cómo "0001".

Es un caso muy extraño, porque no se había visto una intersección de infraestructura así anteriormente, no se cruzaban los grupos/kits para este tipo de estafas, lo cual lo hace muy interesante.

Como en este caso no pudimos extraer mucha información de los scams que usan el pack "0001", no podemos asociarlos directamente y decir que son los mismos que están detrás, pero sí levantan muchas sospechas.

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 Namecheap, Cloudflare 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 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/