FINSIN

Reporte de Phishing

Agosto, Septiembre y Octubre 2023

Índice

Introducción

En nuestros análisis como fundación de ciberseguridad encontramos que uno de los principales problemas que afectan a la comunidad en estos temas es la desinformación y los engaños.

Dentro de estos engaños el más prevalente y uno de los que tiene impacto más directo sobre la población en general es el "Phishing".

Este tipo de ataques es muy generalizado y es un ataque muy barato, porque los ciberdelincuentes pueden generar muchos sitios de estafas diariamente, y al hacer que las personas visiten el sitio pueden engañarlas y robarles sus claves u otro tipo de información.

Analizando algunos de estos sitios encontramos que tienen patrones comunes de comportamiento, y que habían varios hechos de la misma forma, con archivos muy similares que provenían todos de un mismo "kit de phishing".

Nos dimos a la tarea de clasificar y agrupar los sitios que íbamos encontrando de manera "manual", pero luego tuvimos la problemática de que la cantidad de sitios crecía mucho y el tiempo que podíamos dedicarle a esa investigación se mantenía igual y muy reducido.

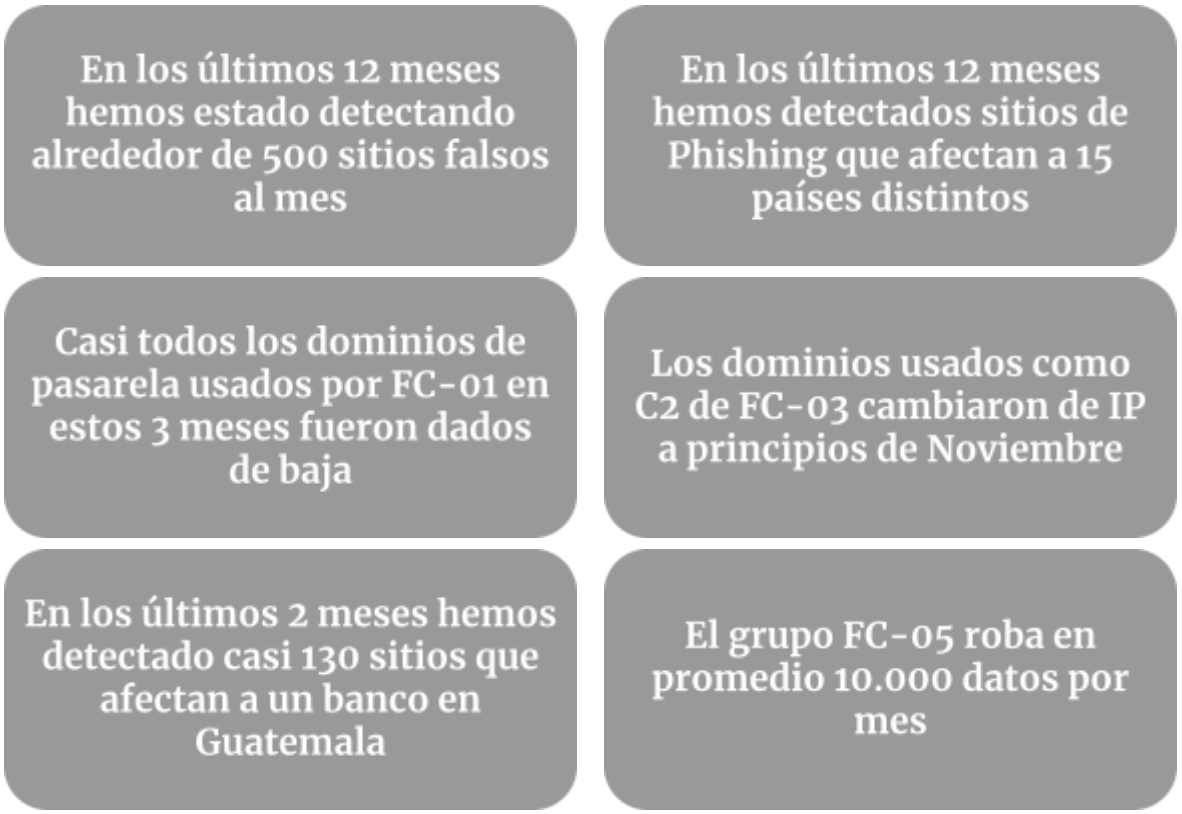
Para ello, decidimos generar un sistema automático con la capacidad de detectar, clasificar y agrupar los sitios de phishing que aparecen, logrando identificar patrones que nos permitan definir si un sitio es o no un Phishing y además a qué tipo de kit está asociado.

Con lo anterior, a principios de Febrero del 2022 lanzamos la plataforma "Phishing Checker" de FINSIN para detectar de manera automatizada los sitios que afectan a la comunidad en Chile y también expandir un poco esta detección a los demás países en Latinoamérica.

Ricardo Monreal Llop
Presidente FINSIN

TL;DR

A modo de resumen, tenemos los siguientes resultados para los meses de Junio y Julio[1]:



Esperamos que con estos datos sigan leyendo el documento.

[1] Cuando se habla de sitios (o kits) detectados implica que fueron detectados por la plataforma, no corresponde al total real de Chile ni del país nombrado.

Phishing Checker

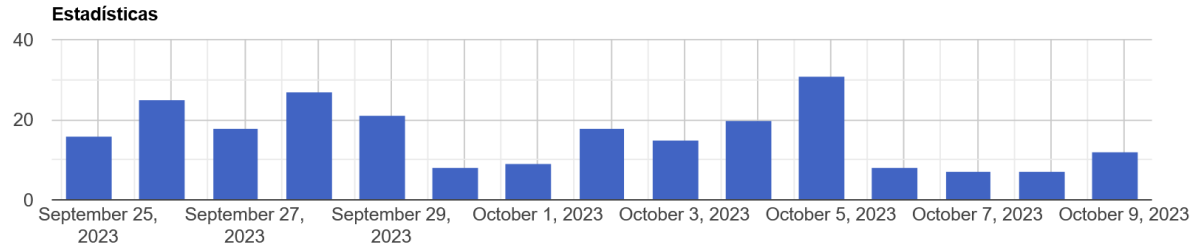
La plataforma "Phishing Checker" de FINSIN es un sitio web que ayuda tanto a "usuarios promedio" como a investigadores de ciberseguridad a tener información sobre los sitios de Phishing que están rondando hoy en Chile y algunos en Latinoamérica.

Queremos hacer una plataforma sencilla, donde basta con tener una URL para saber si es que esa URL es Phishing o no, y también "por qué" es Phishing con la clasificación de tipo/familia/pack a la que pertenece.

Para acceder a la plataforma se puede ingresar por el siguiente link: https://phishing.finsin.cl/stats.php

Para conocer mejor su funcionamiento pueden consultar el manual de uso en el siguiente link: https://finsin.cl/plataforma-phishing-checker/

Estadísticas de Phishings de la últimas semanas.



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.

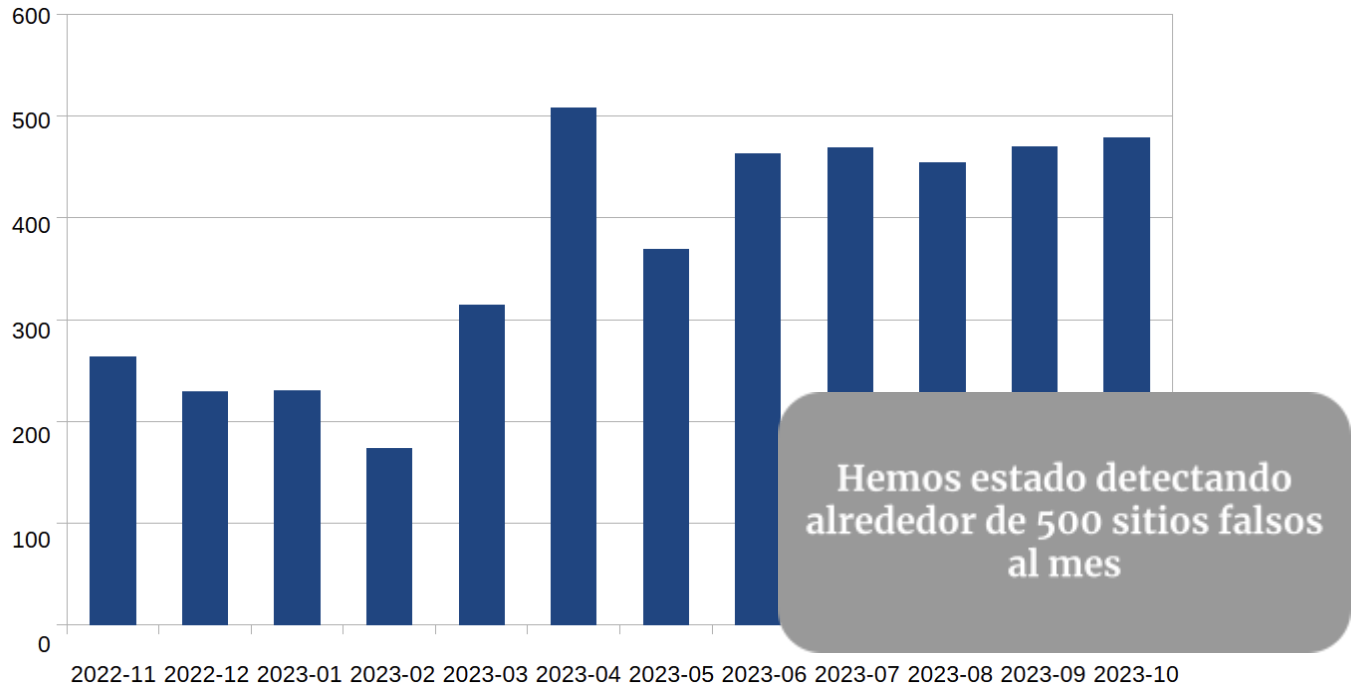
Los últimos 12 meses

Queremos en este momento revisar lo que han sido los últimos 12 meses de la plataforma para ver cómo hemos ido creciendo, tanto en detecciones de kits de Phishing pero también cómo éstos se han distribuido a través de Latinoamérica.

Con una vista general tenemos los siguientes datos:

Datos	Cantidad
Detecciones totales de Phishing	4427
Packs y variantes detectadas	152
Instituciones afectadas por Phishing	59
Países afectados por Phishing	15

El gráfico de las detecciones totales de los últimos 12 meses es el siguiente:



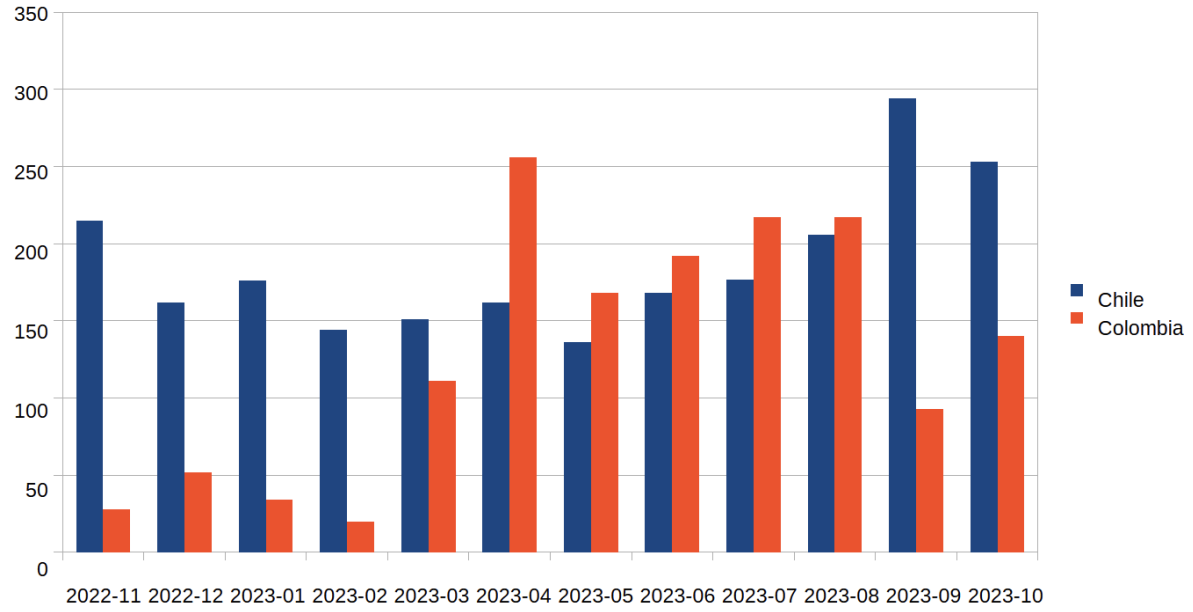
De aquí podemos decir que la detección de este tipo de estafas se ha estancado en estos últimos meses y hemos estado detectando alrededor de 500 sitios falsos al mes. Aunque hemos aumentado la cantidad de kits detectados, el total de phishing se mantiene igual.

Si vemos los totales de Latinoamérica por país, tenemos en los últimos 12 meses los siguientes datos:

País	Detecciones
Chile	2244
Colombia	1528
Paraguay	171
Guatemala	135
Costa Rica	55
México	55
Argentina	39
Perú	35

País	Detecciones
El Salvador	29
Ecuador	21
España	20
Panamá	20
Bolivia	16
Honduras	8
Uruguay	2

Si tomamos solo Chile y Colombia (los países con más cantidad de detecciones) tenemos el siguiente gráfico histórico:



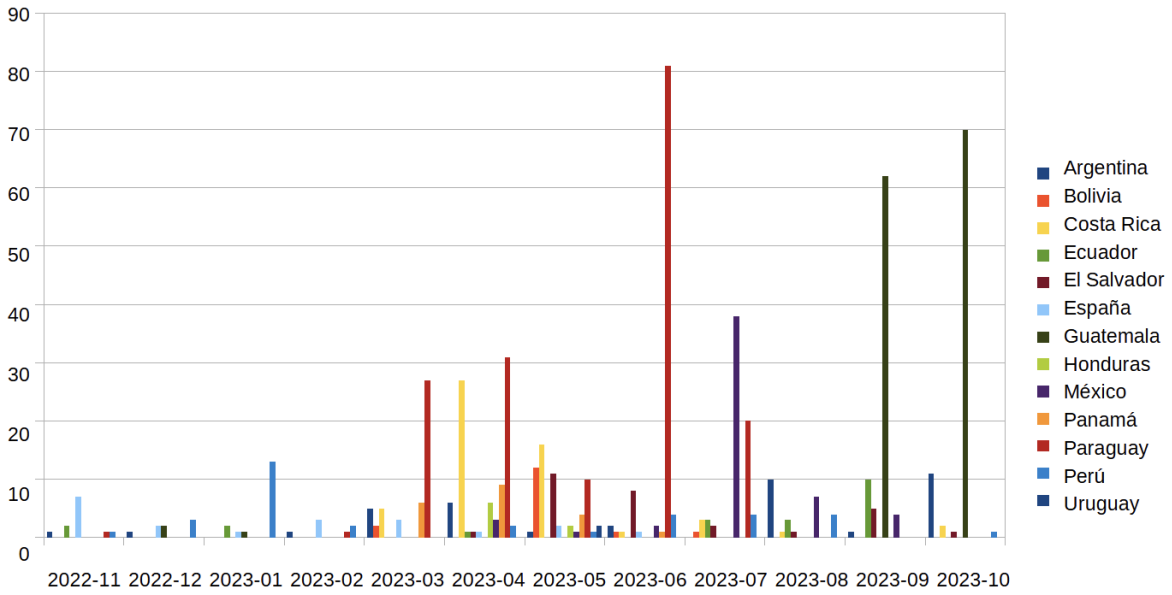
En septiembre y octubre han subido muchísimo las detecciones de phishing en Chile, y las de Colombia han bajado del promedio de 200 que estaban teniendo los meses anteriores.

La subida de detecciones en Chile se debe a la automatización de nuevas pasarelas de phishing del grupo FC-01[2] que antes no habíamos detectado, que nos proporcionan muchos dominios nuevos.

La bajada de detecciones en Colombia no lo tenemos muy claro, pero lo más probable es que los actores detrás de estos sitios se hayan cambiado de hosting o de PaaS[3] y no estamos detectando ese cambio aún.

Las detecciones de los otros países son más erráticas, y solo aparecen en ciertas detecciones automáticas:

[2] hay más información al respecto más adelante
[3] PaaS: Platform as a Service



Un caso interesante es el de Guatemala, el que generó muchas detecciones en los últimos 2 meses, por un alza muy grande en los ataques a una institución bancaria del país que analizaremos un poco más adelante.

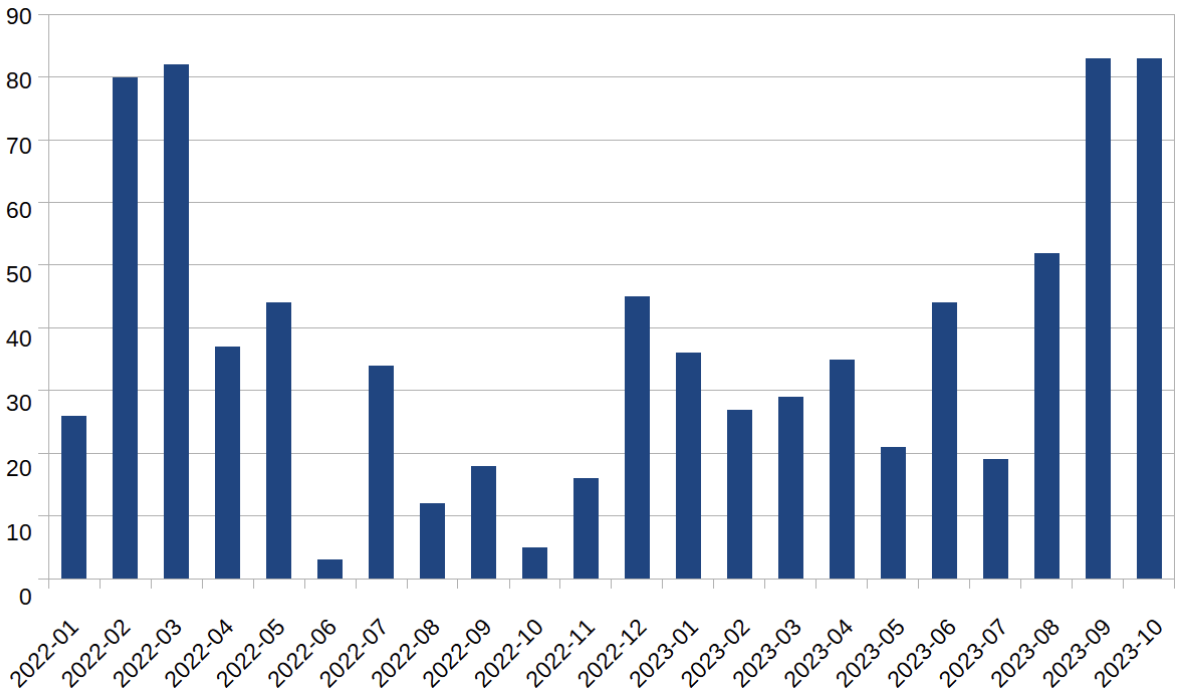
Actualización de Fishers Constantes (FC)

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[4], FC-01 tiene una actividad muy característica, usa varias capas y varias redirecciones para montar su infraestructura. Su "modus-operandi" no ha cambiado mucho, pero tampoco hemos podido asignarle más datos al comportamiento que hemos observado de ellos.

El comportamiento de este grupo a través de los meses ha sido un poco errático, como lo vemos en el siguiente gráfico:



Como vemos, durante todo este 2023 los que están detrás del grupo están levantando por lo menos 20 sitios mensuales y una vuelta a un máximo "histórico" este septiembre y octubre con 83 detecciones, lo que habla de su contínua producción, aun cuando sea un comportamiento conocido.

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

En los últimos meses, hemos mejorado significativamente nuestro monitoreo del grupo al expandir nuestra vigilancia a una mayor cantidad de dominios de redirección. Este enfoque nos ha brindado acceso a numerosos dominios nuevos, permitiéndonos obtener una visión más detallada y precisa de sus actividades.

En estos meses pudimos mantener monitoreados los siguientes dominios:

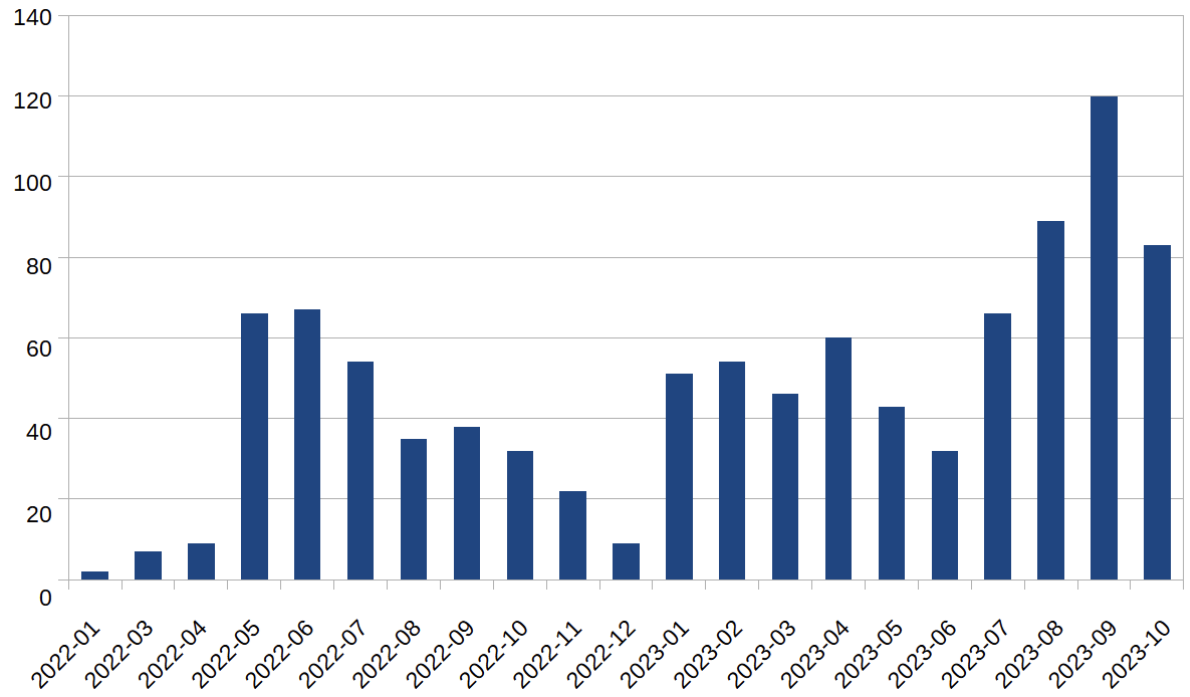
Dominios	Status
beefvalpa.com	Down
clinicposhesh.ir	Down
codesmstado.info	Down
codeundestado.com	Down
doradobetcontact.com	Down
homefogastadp.info	Down
humanbalance.com.co	Down
labarcavalpa.site	Down
lagarnvalpa.com	Down
lineastadohome.info	Down
maacmalleswaram.com	UP
nationaltreasures.co.nz	Down
prevemed.com.ar	Down
promezclas.com	Down
sam-tech.jp	UP
sempel.com.br	Down
senstadolinea.info	Down
smscodeundestado.info	Down
tritannorthstar.com	Down
wordpress.zuliatec.com.ve	Down
zongfagape.com	Down

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

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

FC-03

Como ya vimos en un reporte anterior[5], este grupo está usando 2 packs: el 0009 y el 0010 (con sus respectivas variantes), si vemos sus acciones este mes, podemos ver que las detecciones de este grupo han estado creciendo constantemente.



En junio podemos ver que este grupo bajó mucho su producción (y también nosotros les perdimos la pista), pero después de julio retomaron la creación de sitios en gran medida a través del pack 0009.

En estos meses el grupo solo mantiene 1 variante activa: la 0009-5, y estos últimos meses han habido muchas detecciones de este pack, solo en septiembre son 120 las detecciones hechas por nuestro sistema. ¡Están muy activos!

Si investigamos los centros de comando y control (C2) que usaron durante estos meses, tenemos los siguientes:

Día inicio	C2
2023-06-06	https://current-estado.info
2023-08-21	https://currentv2-estado.info

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

2023-09-07	https://currentv3-stado.info
2023-09-19	https://currentv4-estado.info
2023-10-24	https://currentv5-estado.info
2023-11-01	https://currentv6-estado.info

Como habíamos visto en el reporte anterior, a este grupo le gusta ir cambiando el dominio de C2, pero estos meses se han ido enfocando en mantener el patrón, todos son similares a "current-estado.info".

Igual que "siempre" todos éstos son dominios comprados en Namecheap asociados a la misma IP: 66.29.146.71, con 1 excepción porque el último (currentv6-estado.info) está asociado a la IP: 66.29.146.90. Esto nos hace pensar que han estado cambiando el comportamiento porque la IP de C2 que tenían estaba siendo más monitoreada.

Esto nos hace pensar que han estado cambiando el comportamiento porque la IP de C2 que tenían estaba siendo más monitoreada.

En relación al pack 0010, ahora tenemos unas variantes nuevas, que afectan a 2 instituciones financieras distintas, pero por detrás siguen siendo el mismo kit. Entonces vamos a separar la revisión para verlo por institución más que por kit:

Día inicio	C2 de Institución 1
2023-07-18	https://fala.currentv3.info
2023-08-07	https://pro-gennials.info
2023-09-05	https://currentv3-gennials.info
2023-10-26	https://workerv1.info
2023-10-29	https://currentv3-gennials.info
2023-10-31	https://workerv1.info

Vemos que tienen cierta relación con los anteriores, principalmente al comenzar a usar el current*.info en los dominios. Todos esos dominios son comprados en Namecheap y resuelven a la misma IP: 66.29.146.71.

Lo interesante es cuando a finales de octubre aparece el dominio “workerv1.info” que también es registrado en Namecheap, pero cambia la IP porque ahora, al igual que con el kit 0009, usan la: 66.29.146.90

Ahora al ver a la segunda empresa afectada por el kit 0010 tenemos lo siguiente:

Día inicio	C2 de Institución 2
2023-09-04	https://currentv2-prosanta.info
2023-10-16	https://currentv3-santa.xyz

Al igual que antes, tenemos que ambos dominios fueron registrados en Namecheap y que resuelven a la IP: 66.29.146.71.

Podemos concluir que los controladores han ido mutando su comportamiento y adaptándose con nuevos C2 dependiendo de la fecha, y hoy podemos dar cuenta de un nuevo cambio:

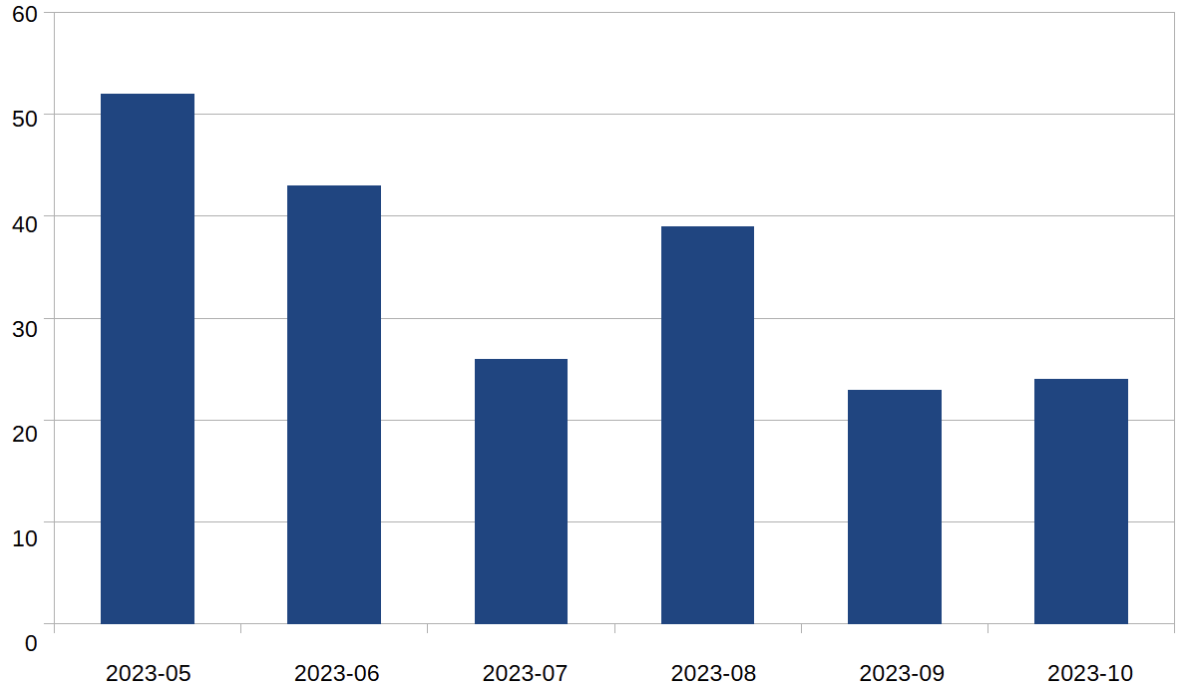
IP de C2	Fecha inicio
162.0.209.127	2022-07-17
199.188.200.52	2022-12-01
66.29.146.71	2023-01-16
66.29.146.90	2023-11-01

Vamos a mantener un monitoreo de estas IPs para ver si es que aparecen más dominios que podrían estar asociados a campañas similares, pero se recomienda el bloqueo de las comunicaciones por HTTP(s) con estas IPs y validar con el hosting para ver quién podría estar detrás de estos dominios.

FC-05

Como ya vimos en el reporte anterior[6], este grupo está usando solamente el pack 0099, y mantiene datos guardados en el Google Sheets a través de una única cuenta.

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



Durante los meses de agosto y septiembre se mantuvieron las detecciones. Dentro de los datos que pudimos detectar tenemos que:

- Todas las detecciones de ambos meses guardan los datos en la misma hoja de Google Sheets[7]
- Todas las interacciones con Google Sheets han sido con la misma cuenta y con las mismas credenciales (usuario, llave, etc.)
- El 100% de las detecciones fueron en el servicio PaaS Replit
- Integraron nuevas empresas con el "mismo" kit

Uno de los datos "interesantes" es que en la misma IP del servicio de Replit (35.186.245.55) pudimos detectar que no solo subieron sitios asociados al banco en Colombia que había sido la tónica de las detecciones anteriores.

[6] Reporte en el siguiente link:
https://finsin.cl/2023/06/13/reporte-bimensual-de-phishing-abril-y-mayo-2023/
[7] El id de la hoja es: **1-ggHujA9RGqNbayYkgCNlexKF0mxdA8VyEeYfoZeXTg**

Ahora agregaron por lo menos 2 víctimas más, un servicio postal colombiano y una institución bancaria de Guatemala. Aunque las empresas afectadas no tuvieron muchos dominios asociados (solamente 2 sitios de phishing cada una) podemos asumir que este kit les está dando buenos resultados como para intentar ampliar su alcance, pero al parecer estas incursiones son solamente a modo de prueba.

Aunque en números totales hemos bajado en la cantidad de detecciones esto no necesariamente quiere decir que los robos de credenciales bajaron, porque si vemos estos datos tenemos que a través del tiempo tanto los datos robados como los "aliases" han ido aumentando constantemente:

Fecha	Total de datos	Total de aliases
2023-08-01	165870	38
2023-08-09	169133	40
2023-08-17	172014	45
2023-09-02	177204	50
2023-09-12	180764	52
2023-09-20	183176	56
2023-09-29	187098	56
2023-10-05	188512	56
2023-10-20	194034	59
2023-10-31	195042	59

Podemos ver que a través de los días los datos almacenados siempre van aumentando llegando a un total de casi 200.000 datos en el último cómputo para este informe.

De esos datos "sólo" 30.000 son nuevos, agregados en estos 3 meses, por lo que tenemos un promedio de 10.000 datos extraídos por mes.

Tenemos un promedio de 10.000 datos robados por mes

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

Entre agosto y octubre se han agregado 21 nuevos aliases, y la gran mayoría son variantes de los aliases antiguos. Nuestra teoría es que son los mismos controladores anteriores, pero que van cambiando los aliases. Por ejemplo: "ALEJOPANELQWE" debería ser el mismo que "ALEJOBESTPANEL" o que "ALEBESTPANELENVIOSDOS" solo que este último alias está asociado a packs que afectan al servicio postal colombiano.

Esta vez no se detectó alguna anomalía dentro de la planilla de Google, la subida de datos ha sido bastante pareja, y no parece haberse enviado un mensaje entre los controladores como lo visto en el reporte anterior[8].

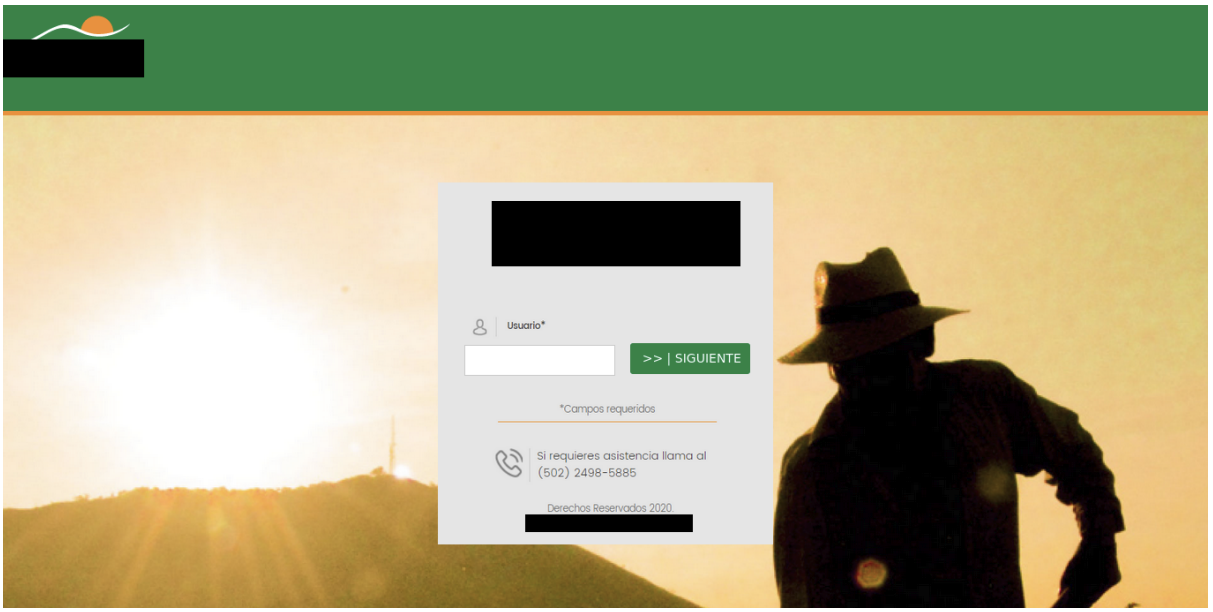
Este grupo parece querer ampliar las víctimas que puede abarcar agregando nuevas variantes del kit para poder abarcar a nuevas instituciones, pero todavía como a modo de prueba por lo que se espera que en los siguientes meses podamos ver si es que estas pruebas fueron exitosas o no.

[8] El reporte se encuentra aquí:
https://finsin.cl/2023/08/25/reporte-de-phishing-junio-y-julio-2023/

Varios packs afectan a banco en Guatemala

En estos últimos meses hemos detectado varias instituciones que están siendo afectadas por múltiples packs distintos, pero una aparición que nos llamó la atención fue una institución bancaria en Guatemala.

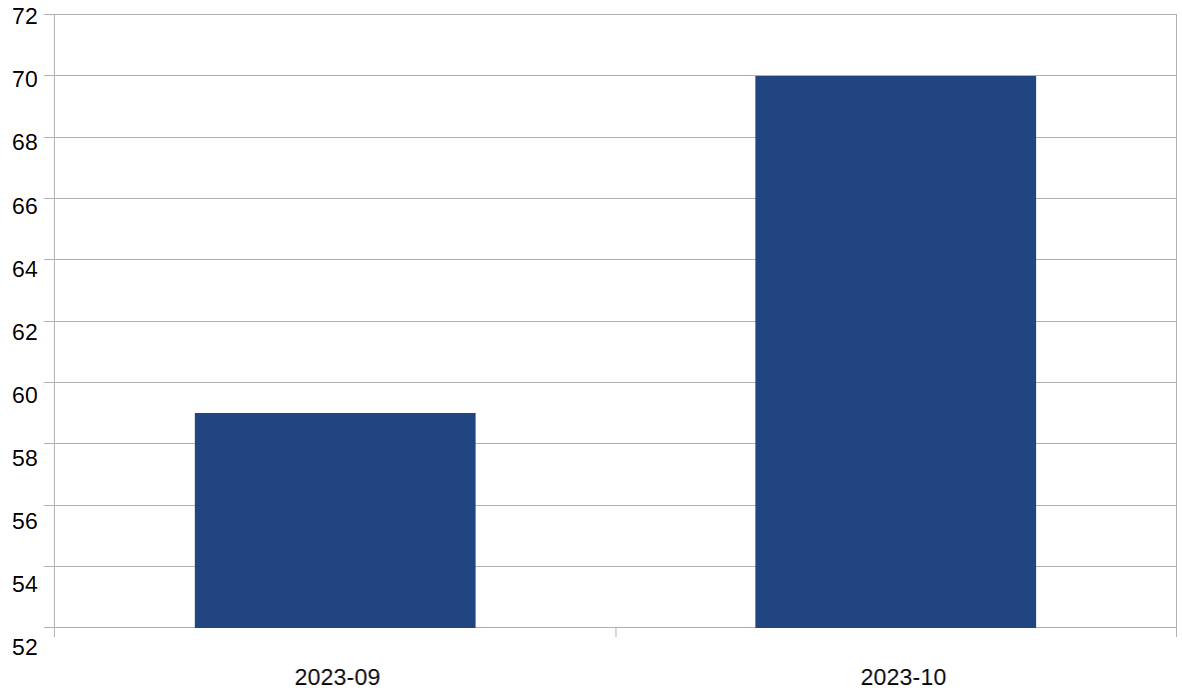
Tenemos casi 130 detecciones de la institución en los últimos 2 meses



A través de los meses no habíamos detectado nada de esta institución, pero a principios de septiembre aparecieron varios sitios de phishing que tenían patrones muy parecidos.

Uno de los patrones detectados es que la página parece tener la declaración de derechos reservados del año 2020, o sea, está atrasada 3 años y como esto nos pareció muy raro comenzamos a identificar el kit y a guardar toda la información que pudiéramos.

Tenemos casi 130 detecciones de la institución en los últimos 2 meses, siendo que antes no habíamos detectado nada relacionado con ellos. Solo en octubre tenemos 70 detecciones.



Lo otro interesante, es que principalmente usan los kits 0120 y 0121 (en 2 variantes), pero también intentaron usar el kit 0091 y el 0099. Por este análisis sabemos que prefieren el uso de Telegram como medio de envío de credenciales de vuelta.

Una revisión rápida de estos kits[9] nos entrega la siguiente información:

Id Kit	Tipo de mensaje	Donde sacar la info
0091	Telegram	Archivo .js con configuración
0099	Google Sheets	Archivo .js con configuración
0120	Sin información	Sin información
0121	Telegram	Incrustado en el mismo .html

Si analizamos solamente lo que tiene que ver con Google Sheets tenemos que fue solamente una prueba muy acotada, porque los registros guardados son de datos "sin valor":

[9] Si quieren información más completa sobre estos kits nos pueden contactar

Id	Fecha	Usuario	Contraseña	Dinamica	Tarjeta	Mes	Año	Cvv	Email	Clave email	Celular	Ip	User
1d961c60-545e-11ee-82c7-575b015380ad	2023-09-16 1:56:55	234234	123wqeewq	322433								206.84.81.68	
298e27c0-563d-11ee-b9f0-13d1b0f9de91	2023-09-18 11:05:45	78374844	jsjxjdjeM6									206.84.81.61	
263a4ff0-568c-11ee-9365-6f8586286dfd				123456									
db5770c0-5713-11ee-b085-0dcd8b3111b5	2023-09-19 12:42:26	7277373	najsdi72M									206.84.81.61	
78173710-5cce-11ee-9e8d-373f0e5a3207	2023-09-26 19:41:11	35434534534	fest54545									206.84.81.61	
47138d10-5d29-11ee-bd89-b180eb9bd2a3	2023-09-27 17:01:09	4545454545	45454545	656565								116.74.159.94	
7e42d6e0-5d3a-11ee-8e71-69b6bc0c1358	2023-09-27 19:05:30	565674567	564567567									116.74.159.94	
14c1c180-5d3b-11ee-bdf1-c75b0cc6f813	2023-09-27 19:08:13	354545454545	5445454545	876546								116.74.159.94	

Lo único de valor en este caso serían las IPs de los que hacen las pruebas:

- 206.84.81.61: Medellín, Colombia
- 116.74.159.94: Pune, India

En este caso no nos sorprende mucho la IP de Colombia, pero sí nos sorprende que haya una IP en India realizando las pruebas, puede ser un hosting/VPS, pero nos quedamos con la duda.

También podemos ver que muchos de esos sitios de Phishing usan chats de Telegram para enviar los datos de las víctimas de vuelta a los controladores. Si nos enfocamos en estos chats, hemos detectado 53 con la plataforma, y son usados por 13 bots.

De los 53 tenemos la siguiente división: 3 son “supergrupos”, 47 son “grupos” y 2 son “chats privados” (o sea que el bot se comunica con un usuario directamente).

Tipo chat	Cantidad
supergrupos	3
grupos	47
chat privados	2

Como tenemos esta información podemos saber algo más de esos grupos, y si analizamos los usuarios (que no son bots) que son/fueron parte de estos grupos, aparece un patrón muy interesante:

User Id	First Name	Last Name	Username	Total Chats
6287201847	**havzo**	**NULL**	**NULL**	**39**
6107634613	Havcx	NULL	NULL	4
453773135	Jhonny	Zambrano	JhonnyzambranoFX	1
1839917055	Cris	Melendi	Crisusdt	1
5465439223	Jo	Er	dael1711	1
5492429481	Trader	NULL	Elvis_usdt	1

5569944550	H1JO	PR0D1G0	SaciucY	1
5706902714	Yoel	NULL	NULL	1
5720745930	Lizmar	Navarro	NULL	1
5855915906	KHAPRIT	NULL	NULL	1
5911461534	Luis	Mendez	NULL	1
6383984167	LaMafia	China	NULL	1

Aquí se nota claramente que el usuario havzo (id 6287201847) es el que más participa de los chats. De los 53 identificados, ese usuario es parte de 39, por lo que podemos asumir que es por lo menos parte importante del grupo que podría estar detrás de estos sitios.

De los 53 chats identificados, ese usuario es parte de 39

No tenemos mucha más información de las personas detrás de los usuarios nombrados, porque esa es parte de una investigación mucho más en profundidad que hoy no tenemos las capacidades de realizar.

Invitamos a la institución afectada o a las policías adecuadas a levantar información sobre esta persona para dar de baja este tipo de ataques.

Palabras finales

Queremos agradecer a quienes nos han apoyado en la plataforma. A través de todos estos meses siempre es bonito y refrescante poder recibir las palabras de apoyo con el proyecto.

Aunque somos una fundación con base en Chile, tenemos bastante información relacionada con kits y actividades en otros países de la región, la que podemos compartir con la gente afectada, y además queremos ir potenciando esta información día a día con la ayuda de todos ustedes.

El "problema del Phishing" es algo que requiere una acción constante y hay que llegar un poco más allá para poder buscar el fondo del asunto. Cada institución afectada tiene el derecho de contactarse con empresas y/o con policías para identificar y denunciar este tipo de abusos, cosa de que no solo sea el takedown una vez, sino que una investigación más a profundidad en conjunto.

Con FINSIN estamos buscando llegar más allá y creemos que con este tipo de plataformas podemos dar más información tanto para las empresas afectadas, para los servicios de takedown, como para las policías que podrían buscar nexos entre estas estafas. Nuestra intención siempre es ayudar a la comunidad en general.

Muchas gracias por el apoyo y nos leemos en el siguiente reporte.

Reportes anteriores

2023

Reporte Abril-Mayo 2023:

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

Reporte Marzo 2023:

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

Reporte Febrero 2023:

https://finsin.cl/2023/03/13/cumplimos-1-ano-de-reportes-de-phishing/

Reporte Enero 2023:

- https://finsin.cl/2023/02/13/reporte-mensual-de-phishing-enero-2023/

2022

Reporte Diciembre 2022:

- https://finsin.cl/2023/01/13/reporte-mensual-de-phishing-diciembre-2022/

Reporte Noviembre 2022:

- https://finsin.cl/2022/12/12/reporte-mensual-de-phishing-noviembre-2022/

Reporte Octubre 2022:

- https://finsin.cl/2022/11/14/reporte-mensual-de-phishing-octubre-2022/

Reporte Septiembre 2022:

- https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022

Reporte Agosto 2022:

- https://finsin.cl/2022/09/11/reporte-mensual-de-phishing-agosto-2022/

Reporte Julio 2022:

- https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/

Reporte Junio 2022:

- https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

Reporte Mayo 2022:

- https://finsin.cl/2022/06/05/reporte-mensual-de-phishing-mayo-2022/

Reporte Abril 2022:

- https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/

Reporte Marzo 2022:

- https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/

Reporte Enero-Febrero 2022:

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