FINSIN

Reporte de Phishing

Noviembre 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 Noviembre[1]:

El 80% de los kits detectados corresponden a sitios que intentan estafar a personas en Chile.

El mayor dolor de cabeza que detectamos para las instituciones colombianas es el servicio de Replit.

Los FC-03 Siguen usando los mismos 2 sub-dominios para C2 como lo habíamos visto en reportes anteriores.

El C2 del kit 0009-5 sigue "online" y sigue siendo el mismo para el 100% de las detecciones.

La única forma de parar el phishing que usa plataformas de redirección, es dando de baja toda la arquitectura.

Esperamos que con estos datos les den ganas de seguir 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.

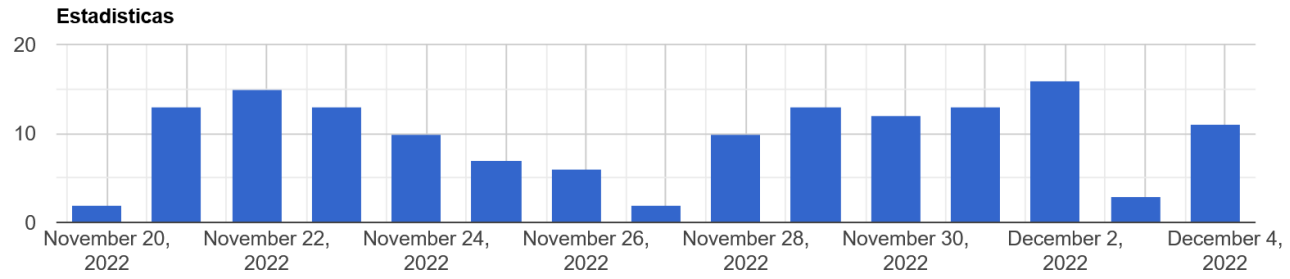
Phishing Checker

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.

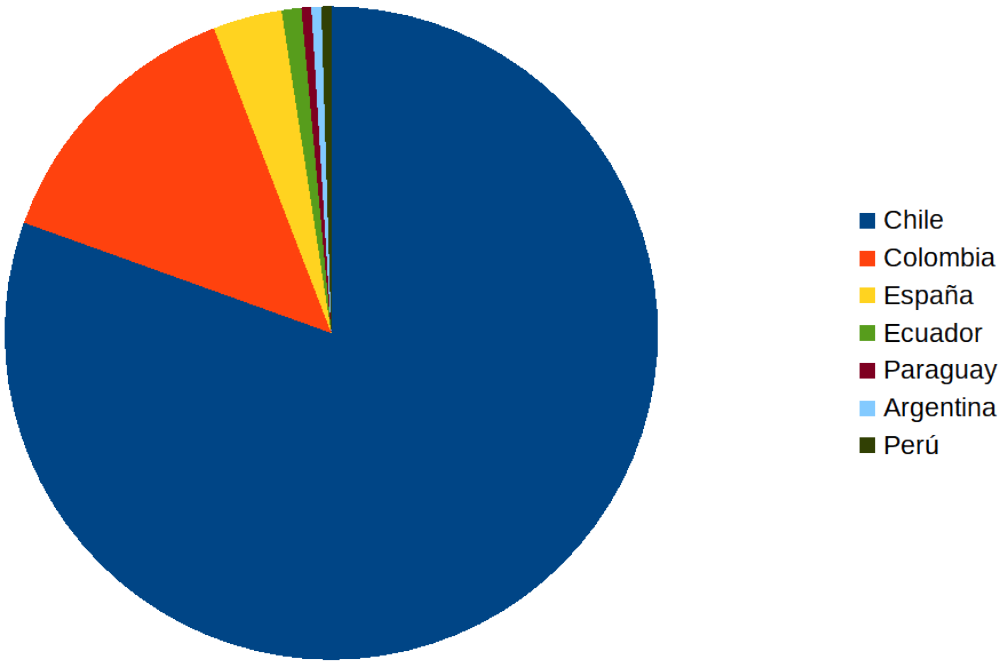
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Noviembre 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[2]

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

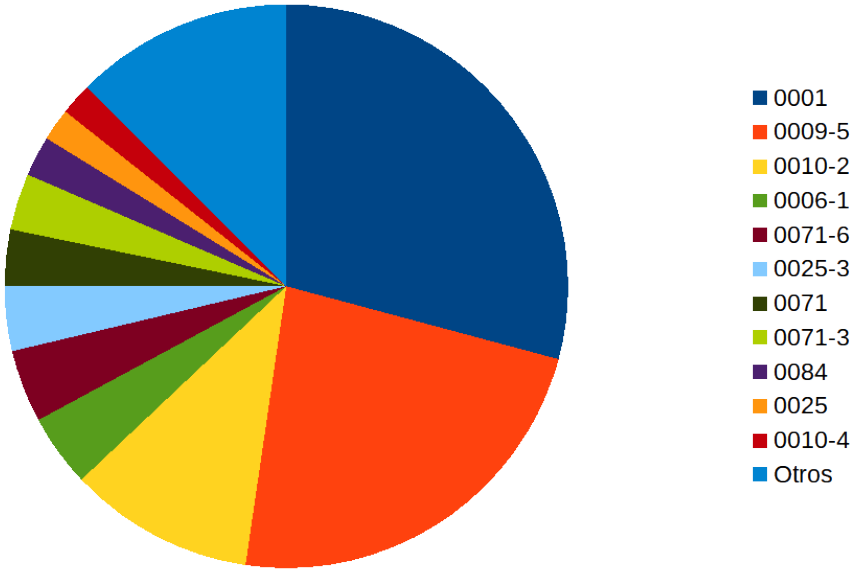


Pais	Porcentaje
Chile	80,49 %
Colombia	13,66 %
España	3,41 %
Ecuador	0,98 %
Argentina	0,49 %
Paraguay	0,49 %
Perú	0,49 %

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

En octubre logramos agregar 4 kits nuevos y 4 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	34,05 %
0009-5	23,15 %
0010-2	10,65 %
0006-1	4,17 %
0071-6	4,17 %
0025-3	3,70 %
0071	3,24 %
0071-3	3,24 %
0084	2,31 %
0025	1,85 %
0010-4	1,85 %
Otros	12,50 %

Y vuelven a aparecer los kits como el 0009-5[3] y el 0010-2[4] que tienen más del 10% de las detecciones del mes cada uno. Esto nos hace validar que los kits "nuevos" que estamos detectando están para quedarse.

3 Revisado en: https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/
4 Revisado en: https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

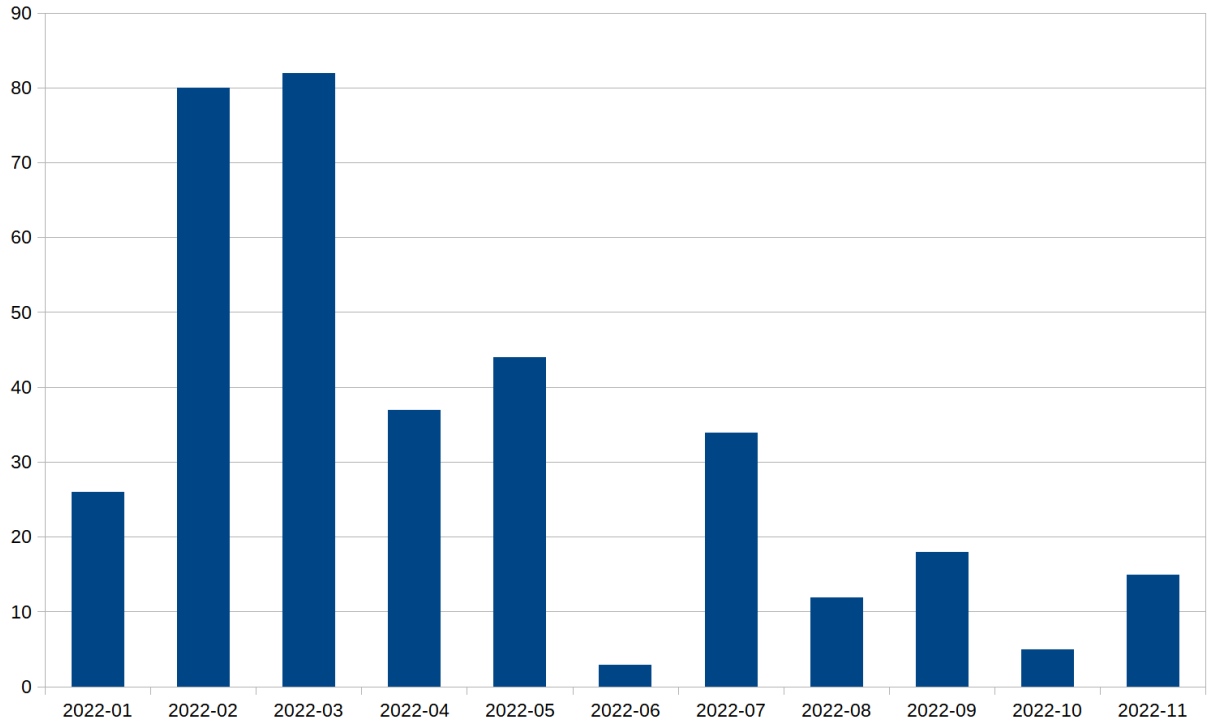
Actualización FC-01, FC-03 y otros

Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos FC-01[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, llegando a una actividad muy baja ahora en el segundo semestre, como podemos ver en el siguiente gráfico.



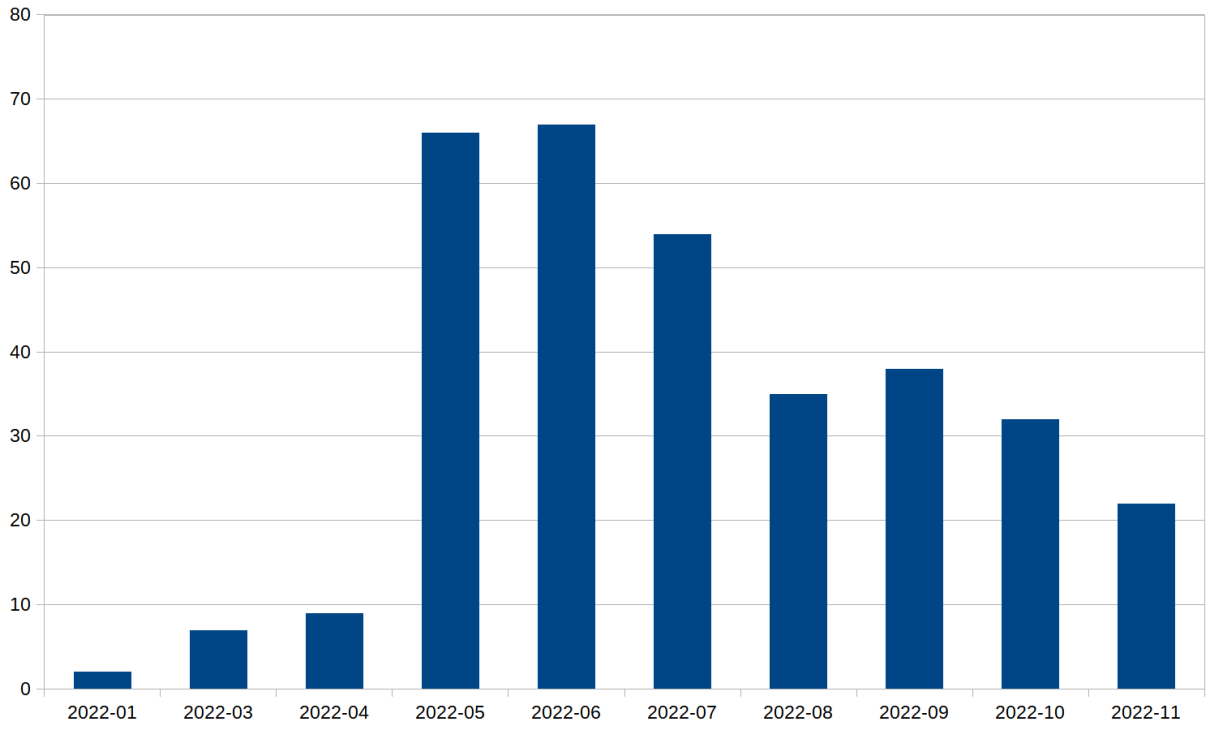
Esperamos que este grupo resurja con nuevos dominios en los meses venideros (ojalá después de las fiestas de fin de año), pero ya no como los meses de febrero y marzo, que llegaron a su peak.

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

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

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 una tendencia clara a la baja, siguen lanzando decenas de sitios de phishing mensualmente:



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.

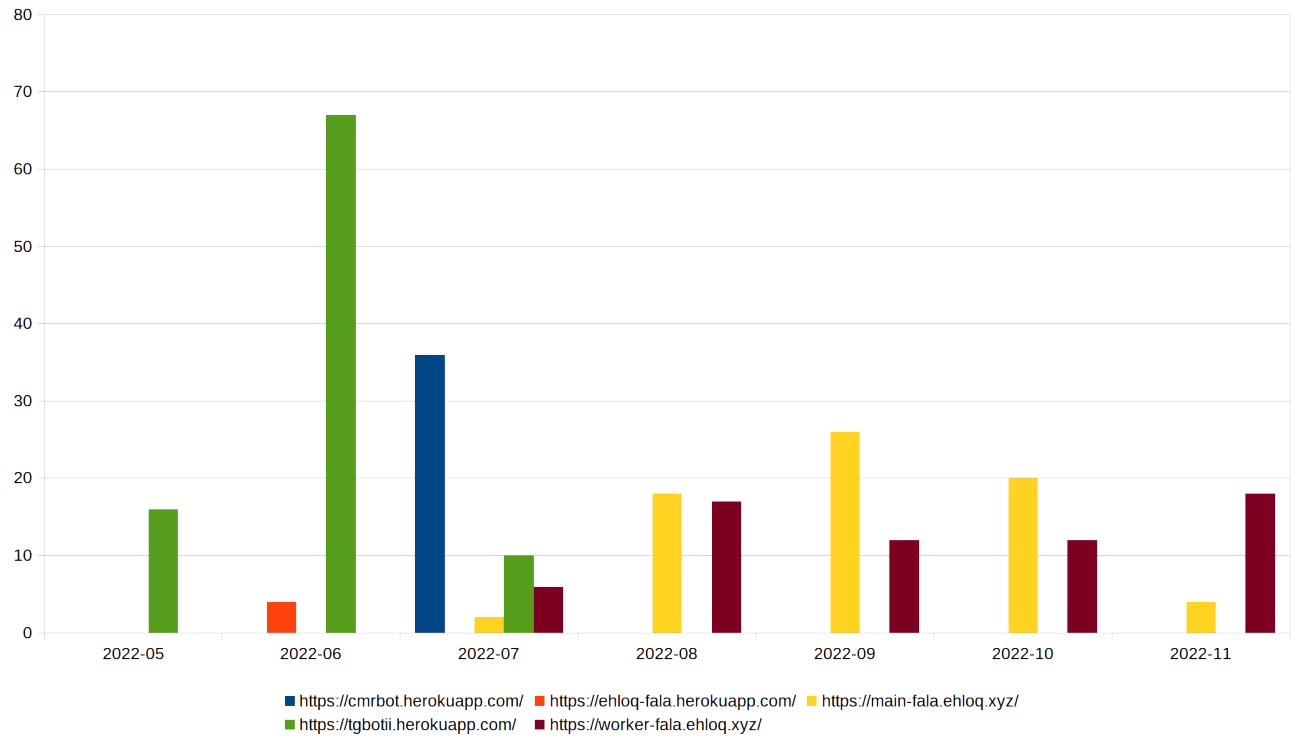
Revisando los dominios de C2 usados este mes de Noviembre tenemos la siguiente tabla:

Dominio BBDD	Cantidad
main-fala.ehloq.xyz	4
worker-fala.ehloq.xyz	18

Siguen usando los mismos 2 sub-dominios para C2 como lo habíamos visto en reportes anteriores. Estos sub-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].

Los FC-03 siguen activos y mantienen su infraestructura para nuevas campañas

Si vamos un poco más atrás, desde mayo, tenemos que los dominios de C2 son pocos, pero similares:



Como pueden ver en un inicio (hasta julio de este año) usaba mucho la plataforma de herokuapp.com para subir sus sistemas de Comando y Control, pero luego comenzó el cambio para usar el dominio “ehloq.xyz” y los 2 sub-dominios nombrados anteriormente.

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

Con esto queremos mostrar que los FC-03 siguen activos y mantienen su infraestructura para nuevas campañas, 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 lo contrario, lo más probable es que sigan levantando sitios, de campañas nuevas o existentes, y aunque se les haga la baja de algunos de estos de “forma rápida”, sigue siendo rentable.

Pack 0009-5

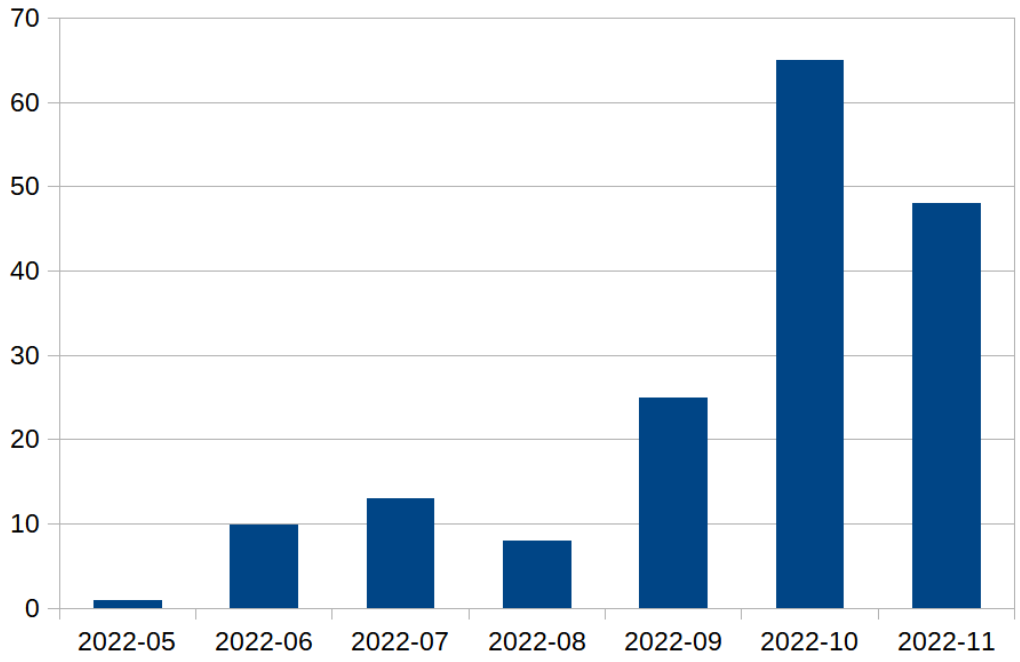
El grupo que está detrás del pack 0009-5 es un grupo que aún no tenemos definido, pero ha estado muy activo estos últimos meses.

De hecho, es uno de los que más nos genera detecciones dentro de la plataforma, gracias a que ataca solamente a 1 institucion bancaria en Chile, y uno de sus servicios de monitoreo y takedown usa nuestra plataforma para validaciones[8].

De este pack ya hemos hablado en reportes anteriores[9], y queremos actualizar un poco cuál es su status.

Siguen sacando muchos dominios de manera constante, pero ahora ya no usan siempre la misma IP como backend para sus redirecciones (204.11.58.233 como salía en el reporte anterior), sino que ahora usan Cloudflare para generar sus dominios.

Nuevamente vemos que de todas las detecciones que hemos tenido de este pack dede mayo, el resultado sigue siendo el mismo: el C2 que está almacenando los datos robados sigue siendo ***https://garyvideos.click***, para el 100% de las detecciones.



Todas las detecciones del gráfico tienen el mismo C2.

8 Muchas gracias a la gente de ese servicio de takedown.

9 Más información sobre el kit en el reporte de septiembre: https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/

Con respecto a las IPs "intermedias" que habíamos hablado anteriormente, que ayudan para la redirección del pack tenemos que usan solo 2, y no en todos los casos:

IP de redirección	Cantidad de detecciones
165.22.222.242	10
157.245.104.204	14

Para recordar el funcionamiento de estas IPs, podemos revisar un ejemplo real de detección de la plataforma[10]:

N° Redirección	URL Redirección	Dominio Redirección
0	http://bit.ly/3tCROKm	bit.ly
1	http://157.245.104.204/6a2b38ed5aae15f/2802c885cbf0df/900153547558ON/eded352493853f7fc	157.245.104.204
2	http://157.245.104.204/6a2b38ed5aae15f/2802c885cbf0df/900153547558ON/eded352493853f7fc/	157.245.104.204
3	https://asistencia-banestado.click/redlanga?&rpsnv=63843e04b0f7a32d94539cf328ed335d39085a56	asistencia-banestado.click

Gracias a ese ejemplo podemos ver que la URL de redirección intermedia comienza con una IP, y luego con una ruta fija (siempre la misma para todas las redirecciones) que parece aleatoria. De ahí salta al link final del sitio de estafa.

La única forma de parar este tipo de phishing, es dando de baja toda la arquitectura

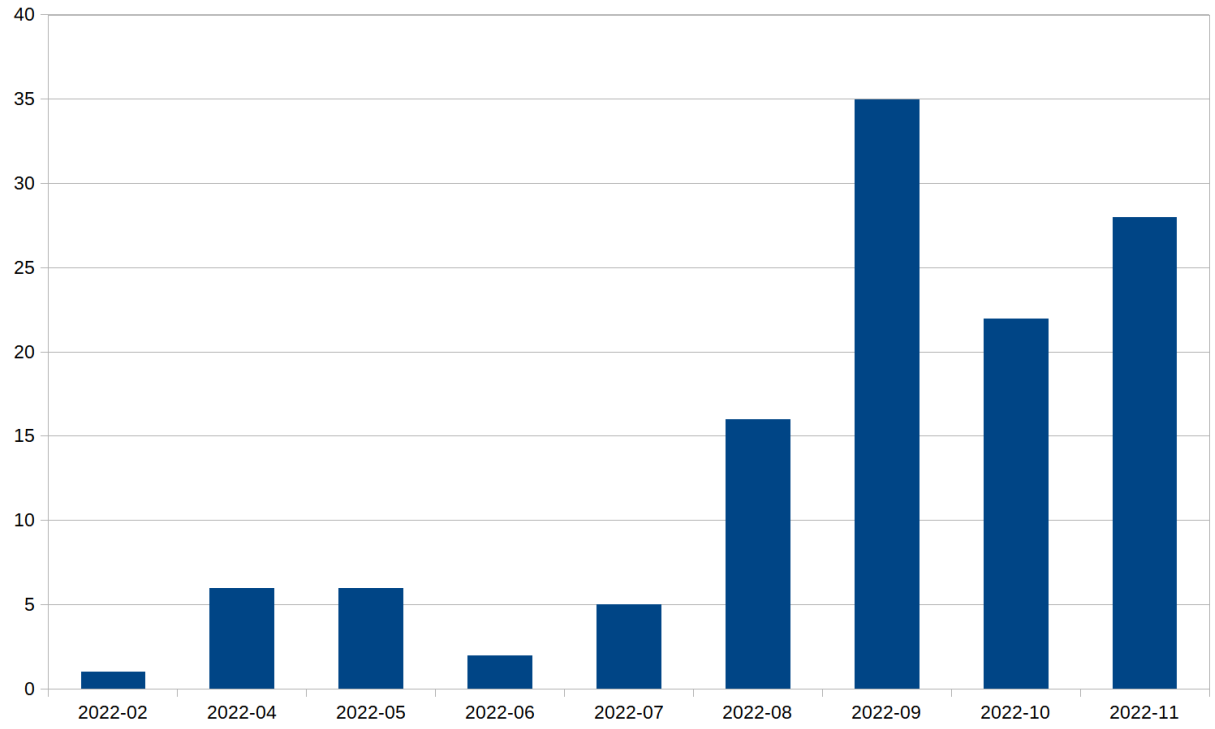
Insistimos que la única forma de parar este tipo de phishing, que usa plataformas de redirección, es dando de baja toda la arquitectura creada, no solamente el link inicial o el link final, porque mientras exista parte de la infraestructura, les conviene seguir infectando[11].

10 El link para la el ejemplo revisado es: https://phishing.finsin.cl/list.php?query=e5ea8cc8b4773da7eed9cf292da587e2674d5a418e0b5d628a1883a2f596eaed

11 Informamos que las IPs antes cubiertas fueron dadas de baja en diciembre, pero estuvieron activas todo el mes.

Actividad en Colombia

A través de los meses, hemos notado que otro de los países que tienen un problema bastante grande con el Phishing es Colombia. De hecho, nuestro gráfico de detección mensual para este país es el siguiente:



Hay un cambio sustancial luego de que participamos en la DragonJAR Security Conference de este año, en donde comenzamos a monitorear algunos kits relacionados con este país.

De hecho, si tomamos desde agosto, tenemos que podemos encontrar un patrón bastante interesante del comportamiento de algunos actores detrás de estos sitios de estafa:

IP	Detecciones
108.179.194.34	1
145.14.144.39	1
145.14.152.189	1
151.106.27.230	1
185.221.182.204	1
193.34.76.44	3
200.58.111.42	1
23.185.0.1	6
23.185.0.2	1
23.185.0.3	2
23.185.0.4	6
34.149.204.188	76
69.49.229.22	1

Como se puede ver, detrás de las detecciones, hay una IP que sobresale, y otras que vale la pena dar una segunda mirada:

replit	La IP 34.149.204.188 tiene la gran mayoría de las detecciones de este período, y está asociada al servicio de Replit[12] que habíamos hablado en un reporte anterior[13]. Siguen usando mucho este servicio para subir phishing, y todavía no tenemos un método eficiente para ir detectando todos los posibles sitios de estafa, por lo que nuestra detección es muy manual. Aun así logramos detectar un buen número
PANTHEON®	Las IP 23.185.0.1, 23.185.0.2, 23.185.0.3 y 23.185.0.4, son parte del servicio de Pantheon.io[14], que al igual que Replit, permite subir código de distintos tipos de lenguajes, pero con enfoque en PHP como backend. Es interesante como usan siempre las mismas IPs y también se puede monitorear la creación de dominios gracias a los DNS pasivos. Lo bueno que hemos visto en este servicio es que los phishing los dan de baja muy rápidamente, una muy buena práctica que otros servicios deberían copiar.

12 Sitio oficial: https://replit.com/
13 Este servicio fue revisado en el reporte de agosto: https://finsin.cl/2022/09/11/reporte-mensual-de-phishing-agosto-2022/
14 Sitio oficial: https://pantheon.io/

localtunnel	La IP 193.34.76.44 corresponde al servicio Localtunnel[15] que habíamos hablado en un reporte anterior[16], y desde ese reporte no hemos detectado más actividad relevante. Aun así, hay que seguir monitoreando el servicio.

Con esto tenemos que, de lo que hemos detectado, el mayor dolor de cabeza para las instituciones colombianas es el servicio de Replit, que permite subir mucho código y no tiene buen filtro anti phishing.

Se recomienda estas instituciones contactar con administradores de este servicio para llegar a un bloqueo de las cuentas que están subiendo este tipo de contenido, y/o lograr una detección temprana de este tipo de kits.

15 Sitio oficial: https://theboroer.github.io/localtunnel-www/

16 Este servicio fue revisado en el reporte de agosto: https://finsin.cl/2022/09/11/reporte-mensual-de-phishing-agosto-2022/

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 Replit, Pantheon, 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 Octubre:
  - https://finsin.cl/2022/11/14/reporte-mensual-de-phishing-octubre-2022/
- Reporte Septiembre
  - https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/
- 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
  - https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/