tra

FINSIN

Reporte de Phishing

Agosto 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 Agosto[1]:

Fuimos parte de DragonJAR Security Conference 2022

Solo el 70% de las detecciones del mes fueron de kits que afectan a personas en Chile

Al ver los números globales revisados tenemos una clara tendencia a la baja

Creemos que en el caso de Chile, ya no se están recibiendo tantos mensajes fraudulentos como antes

Los sitios de Phishing creados en repl.co son principalmente sitios dedicados a afectar a personas en Colombia

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

1 Cuando se habla de sitios detectados implica que fueron detectados por la plataforma, no corresponde al total real de Chile.

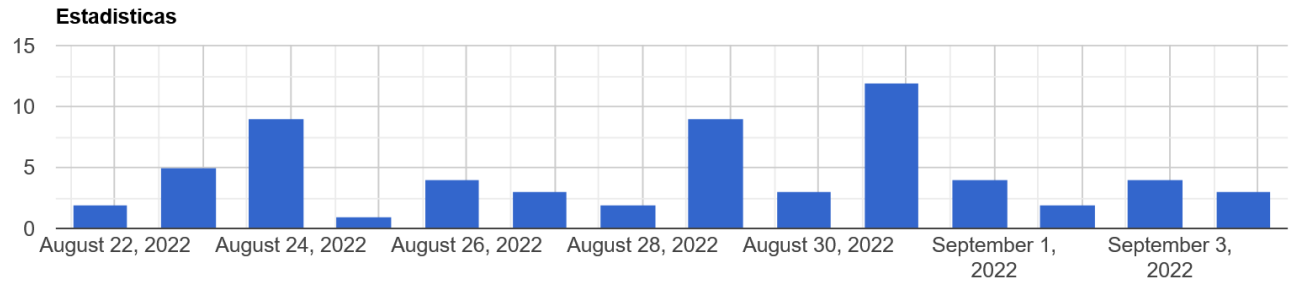
Phishing Checker

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

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

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

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



Recuerden, tenemos nuestro canal de Telegram dedicado a las alertas de los sitios detectados por la plataforma.

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

También, el día 08 de septiembre, fuimos parte de **DragonJAR Security Conference 2022**, donde mostramos un poco el problema del Phishing y qué hemos aprendido a través de estos meses con la plataforma.

La presentación en formato PDF y más información pueden encontrar aquí: https://finsin.cl/2022/09/08/participamos-en-dragonjarcon-2022/

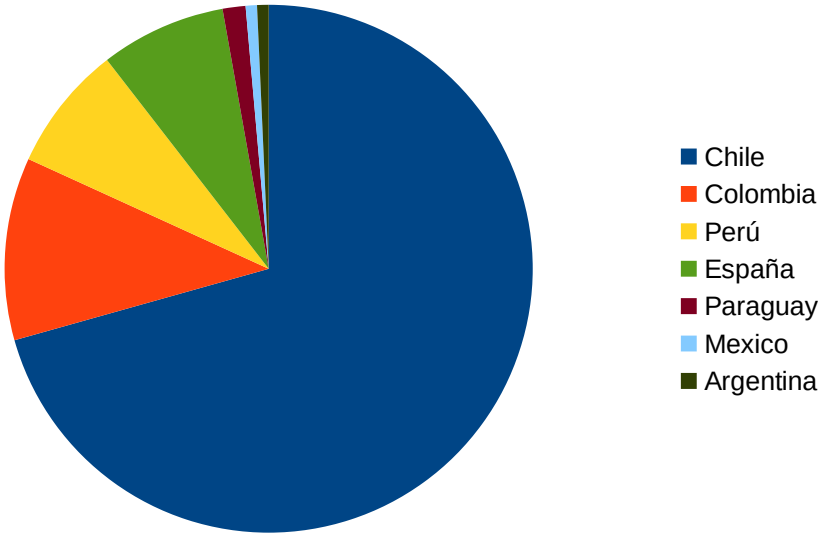
Agosto 2022

En agosto, hemos revisado que la cantidad total de sitios de phishing han ido a la baja, aún teniendo en cuenta que expandimos nuestras detecciones de estos sitios a distintos paises latinoamericanos.

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:

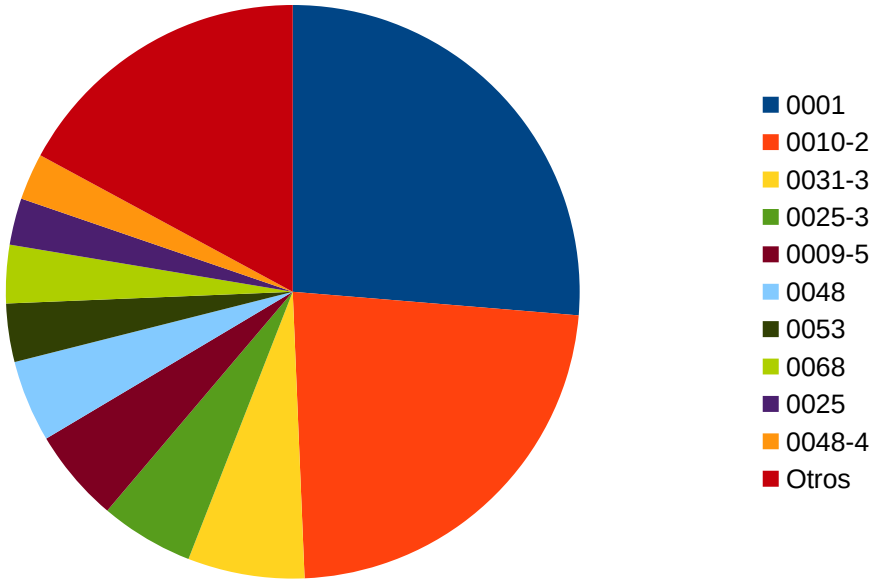


Pais	Porcentaje
Chile	70,63 %
Colombia	11,19 %
Perú	7,69 %
España	7,69 %
Paraguay	1,40 %
Mexico	0,70 %
Argentina	0,70 %

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 agosto logramos agregar 4 kits nuevos y 5 variantes nuevas de Phishing que ya conocíamos antes. Si graficamos estos datos queda un poco parecido a los meses anteriores:



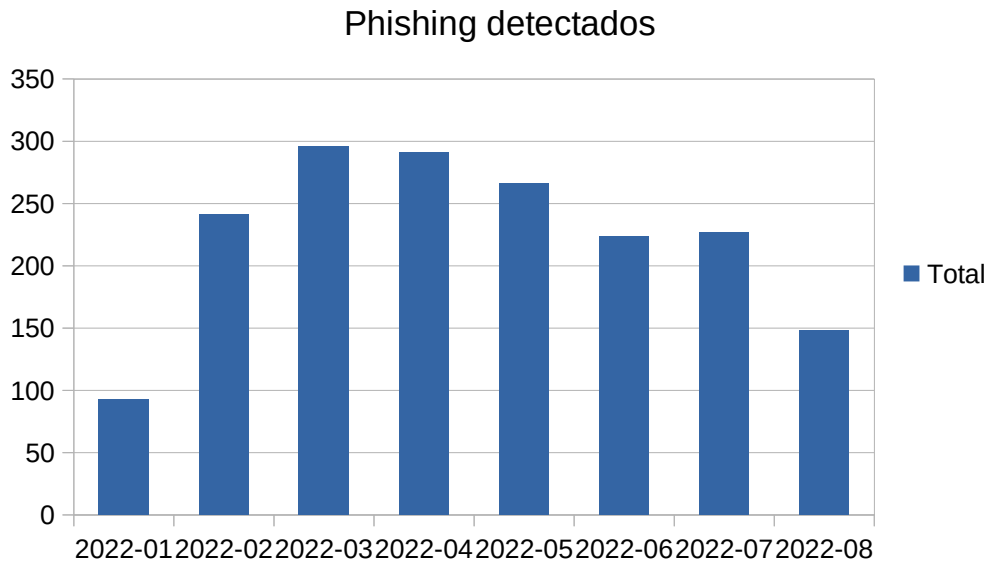
Ahora vemos que el predominio del pack “0001” es cada vez menos importante, de hecho están muy parecidos con el “0010-2”:

Pack	Porcentaje
0001	26,32 %
0010-2	23,03 %
0031-3	6,58 %
0025-3	5,26 %
0009-5	5,26 %
0048	4,61 %
0053	3,29 %
0068	3,29 %
0025	2,63 %
0048-4	2,63 %
Otros	17,11 %

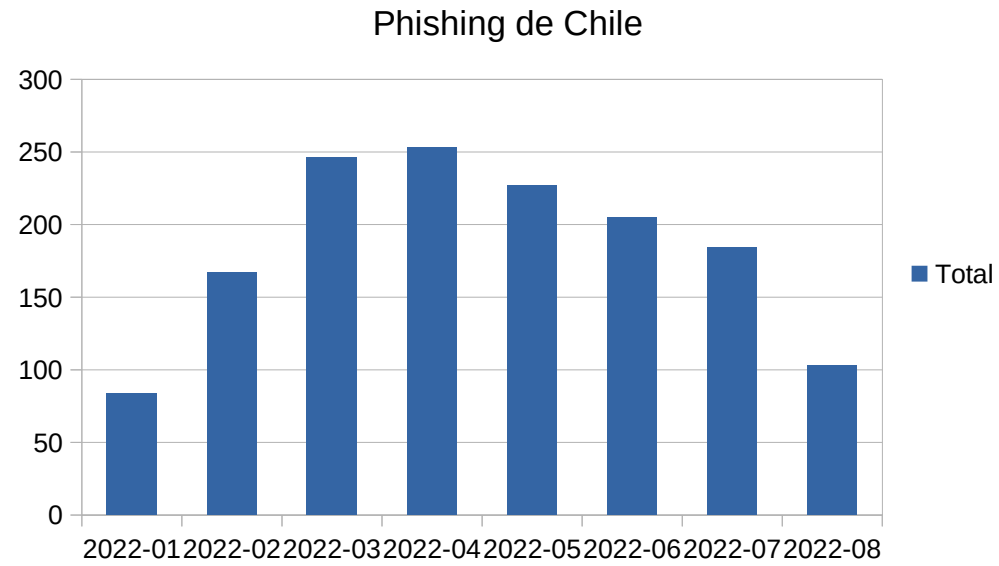
Podemos ver que los dos packs anteriores se escapan con las detecciones, y que los que siguen tienen muchas menos. De hecho, vuelve a aparecer en el tercer lugar el kit “0031-3” que afecta a las personas en España, aun cuando en número no hemos tenido muchas detecciones exitosas.

Baja de casos

Este mes tenemos que retomar un poco la revisión anual de los casos de phishing detectados durante el año. Al colocar los números globales revisados por la plataforma en un gráfico tenemos una clara tendencia a la baja:



Esta tendencia se ve bien marcado por la tendencia que tenemos en Chile, tenemos lo siguiente:



Con esto podemos validar un poco la disminución notoria que ha tenido en los últimos meses. Se nota en la cantidad de alertas que hemos podido observar en Twitter de la gente que recibe SMS o correos fraudulentos.

Creemos que en el caso de Chile, ya no se están recibiendo tantos mensajes fraudulentos como antes

Si hacemos la búsqueda "sms Chile" el año pasado[3] tenemos por lo menos 10 casos de Phishing que podemos investigar. Si luego hacemos la misma búsqueda para el mismo período de este año[4], tenemos que hay 0 casos relevantes.

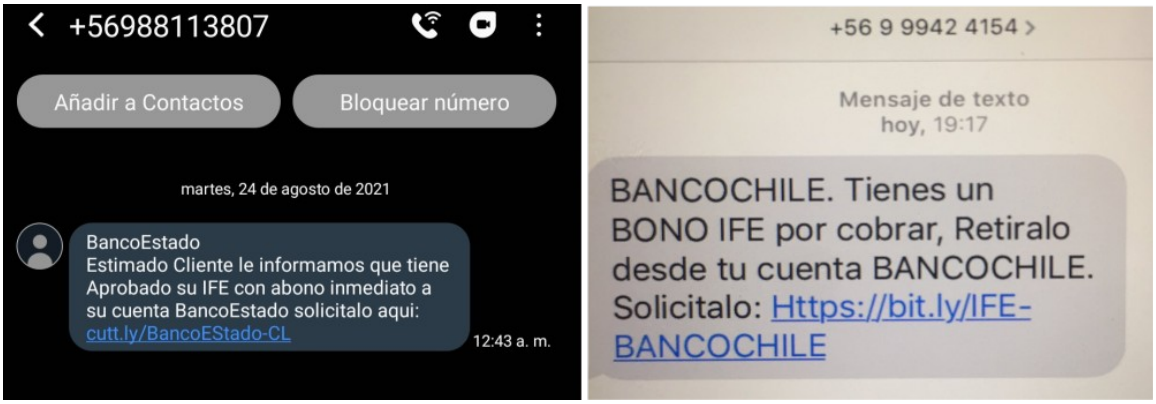


Figura 1: Casos del año 2021

Hoy en día no se reciben las mismas cantidades de alertas de los usuarios de Twitter, lo cual nos hace pensar 2 cosas:

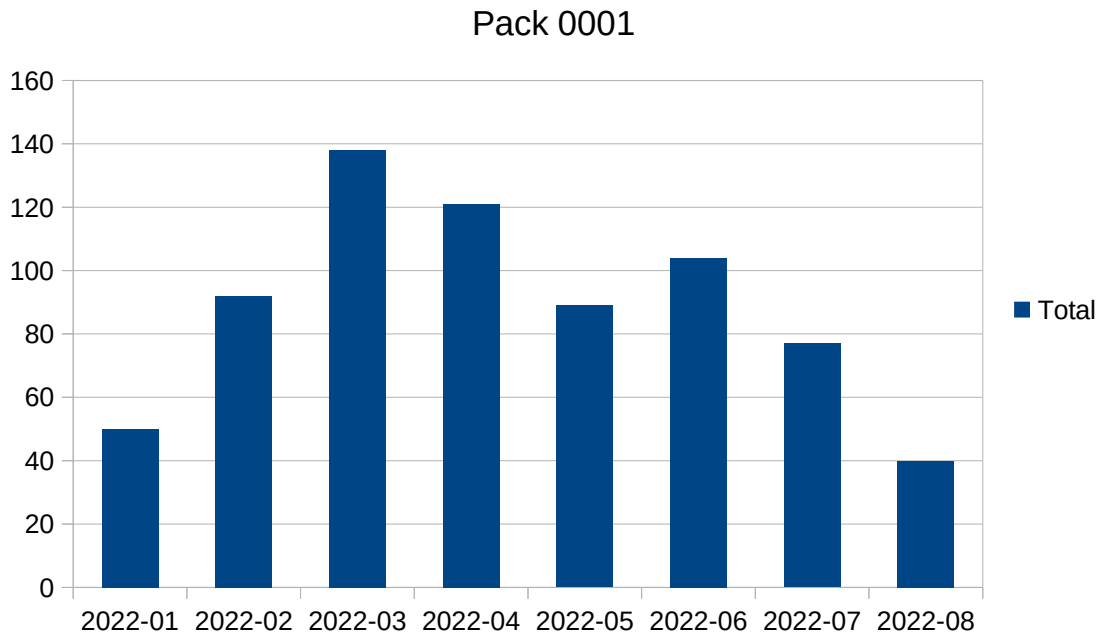
- No se están recibiendo muchos phishing por SMS (en este caso).
- Los usuarios de Twitter se cansaron de reclamar.

Creemos que por la naturaleza de la plataforma, este último no es el caso. Creemos también que en el caso de Chile, ya no se están recibiendo tantos mensajes fraudulentos como antes.

3 https://twitter.com/search?q=sms%20Chile%20since%3A2021-08-23%20until%3A2021-08-30&src=typed_query&f=top

4 https://twitter.com/search?q=sms%20Chile%20since%3A2022-08-23%20until%3A2022-08-30&src=typed_query&f=top

Este cambio de paradigma también lo vemos reflejado en el pack “0001”, que es el pack que más estamos “acostumbrados” a monitorear, y es el que se destaca en detecciones todos los meses.



Esto en general es una sorpresa, pero sí se alinea con las tendencias que hemos hablado en los últimos meses: los ataques de phishing se han ido profesionalizando, y en Chile se han detectado y dado de baja mucho más rápido.

Además, el excesivo spam que se generó con estos phishing generó que la gente se educara más sobre como reconocer y no caer en estos phishing más simples y notorios.

Con todo lo anterior, a los ciberdelincuentes se les está haciendo más complejo y costoso lograr nuevas víctimas.

¿Dónde están los sitios?

Los kits que hemos estado detectando últimamente nos sorprenden por el "dónde" estaban alojados. Hemos detectado un aumento de los phishing en servicios online dedicado al almacenamiento de código.

Estos servicios pueden ser considerados como "Platform as a Service" (PaaS), por el hecho de que permiten disponer de la plataforma en donde se va a ejecutar.

Este mes tenemos 2 plataformas de este tipo que para nosotros son interesantes: Firebase, Replit.

Además, queremos mostrar otra plataforma, en este caso de proxy reverso, que también nos llamó la atención: Localtunnel.

Firebase

Sitio web: https://firebase.google.com/
Prinicipal IP de phishing: 199.36.158.100

Servicio de Google en que se puede agregar código estático solo asociando una cuenta de Google.

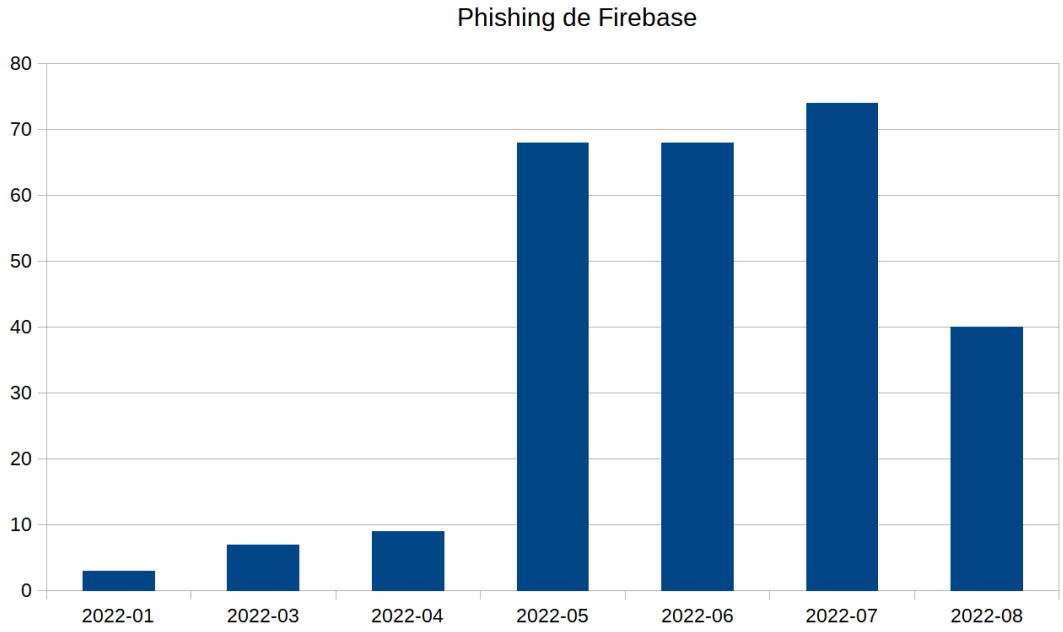
En Firebase hemos detectado los kits de la familia 0010 y 0053, que hemos hablado en reportes anteriores (Junio[5] y Julio[6] respectivamente) y es el servicio online que más genera sitios con los kits que tenemos.

Una de las principales características es que para el nivel de servicio gratuito el código almacenado siempre va a tener como dominio principal web.app y/o firebaseapp.com, y siempre va a estar asociado a la IP 199.36.158.100.

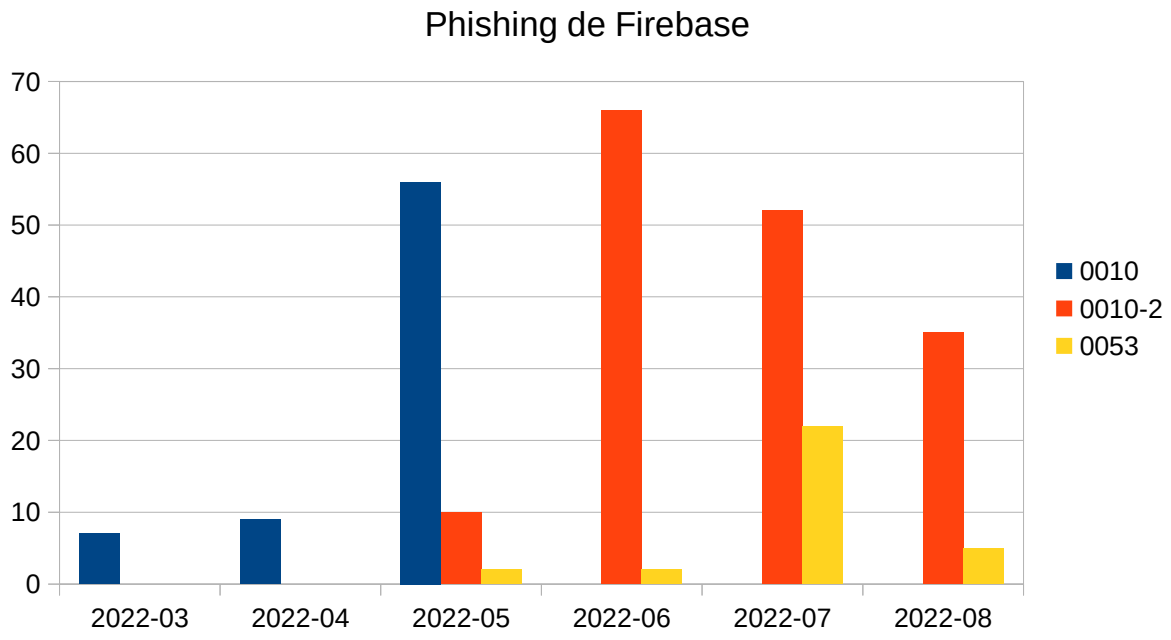
Basta estar atento tanto a los dominios como a la IP para poder ir detectando los nuevos sitios de phishing

5 https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/
6 https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/

Al monitorear la IP en cuestión tenemos que los sitios de phishing levantados en esta infraestructura venía en ascenso en los últimos meses, pero en agosto hubo una baja:



Además, al tomar la distribución de packs que están alojados en Firebase tenemos nuevamente algo similar a lo que estábamos diciendo anteriormente:



Vemos ahora que los packs de phishing que apuntan a Chile van en un constante descenso, porque las versiones del pack “0010” están en declive desde junio (por ahora coincidencia con nuestro reporte).

Además, el pack “0053” ha sido un poco inestable a través de los meses, solo en julio apareció fuerte en nuestro monitoreo, y luego en agosto bajó nuevamente.

Con toda esta información, basta estar atento tanto a los dominios como a la IP para poder ir detectando los nuevos sitios de phishing. Nosotros seguiremos monitoreando el servicio por si encontramos nuevas instancias de estos packs, u otros que podamos revisar.

Replit

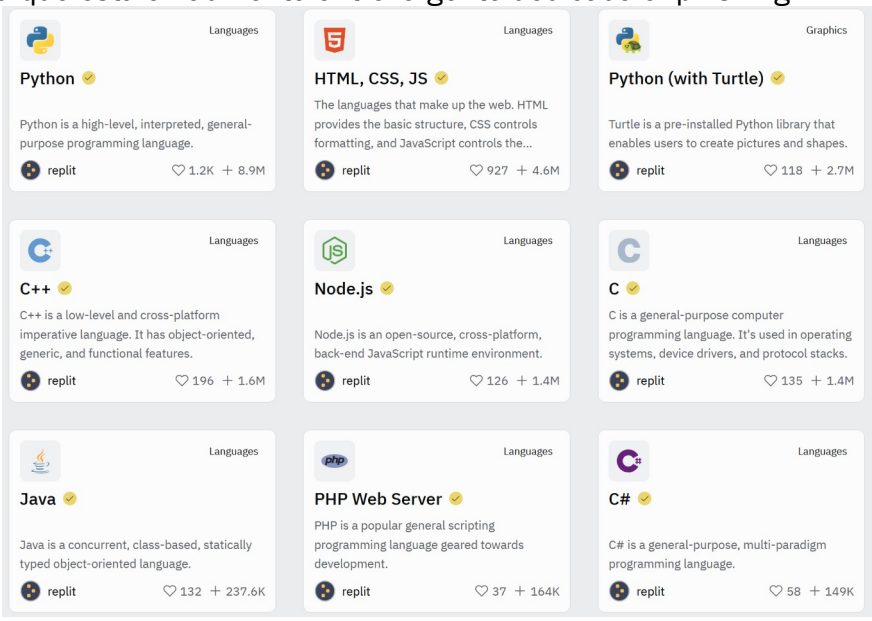
Sitio web: https://replit.com/
Prinicipales IP de sitios de phishing: 34.110.138.177, 34.149.204.188 y 35.186.245.55

Servicio en el que se puede subir cualquier tipo de código y luego éste es hosteado por el mismo Replit. De hecho el servicio en el nivel gratis te permite almacenar hasta 500 Mb de espacio en los servidores de Replit, y como los kit de phishing no requieren tanto espacio, es perfecto para ese objetivo.

Además, la lista de lenguajes disponibles es muy grande:

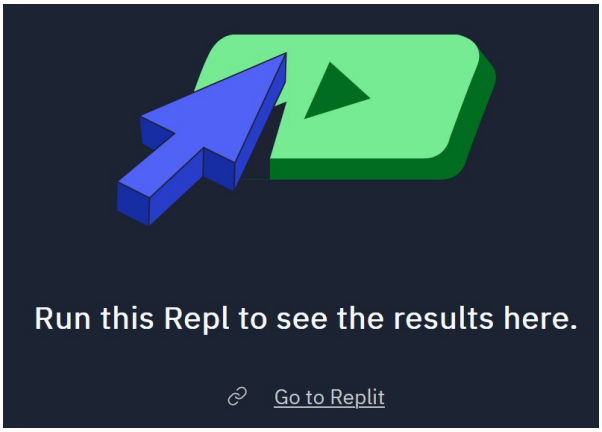
Clojure	Unlambda	JavaScript	Swift	Dart	SQLite
Haskell	CoffeeScript	Deno (beta)	Python (with Turtle)	Reason Node.js	Java
Kotlin	Scheme	Golang	Basic (beta)	Tcl	PHP CLI
QBasic	APL	C++	R	Erlang	Pyxel
Forth	Lua	C	Bash	TypeScript	Raku
LOLCODE	Ruby	C#	Crystal	Pygame	Scala (beta)
BrainF	Roy	F#	Julia	Love2D	Nix (beta)
Emoticon	Python	HTML, CSS, JS	Elixir	Emacs Lisp (Elisp)	Kaboom (beta)
Bloop	Node.js	Rust	Nim	PHP Web Server	

Lo anterior, sumado a que ya tiene varias plantillas para poder armar tu sitio “desde 0”, hace que sea una plataforma que está en aumento entre la gente dedicada al phishing.

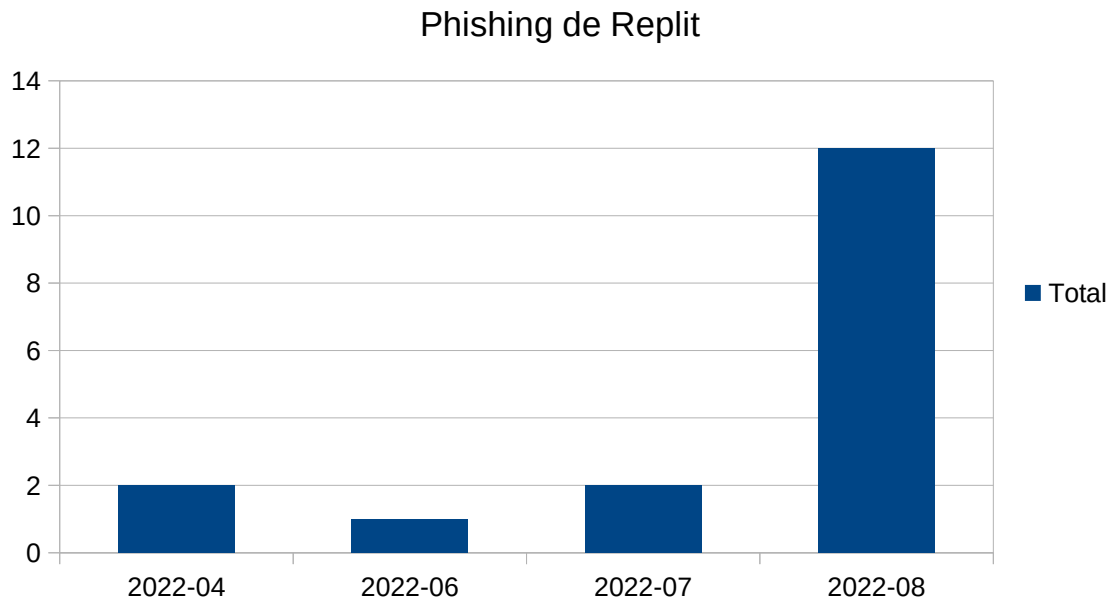


Esto se puede ver por el aumento de los casos que hemos detectado en la plataforma, y de hecho, en muchos de esos casos “llegamos tarde”, porque son sitios que ya se dieron de baja, y son kits que no tenemos completamente identificados.

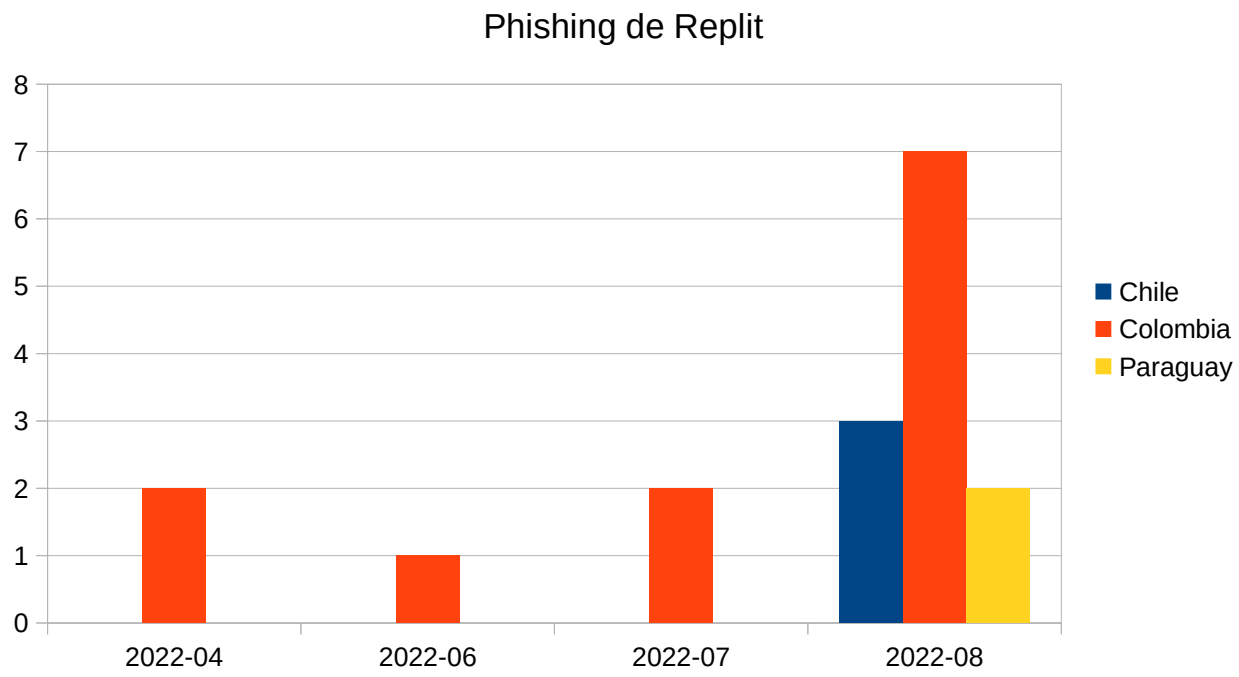
De hecho, las revisiones que hemos hecho de estos sitios nos generan sorpresa porque no sabemos exactamente si es que hay algún veto a las cuentas desde Replit, o la respuesta a los sistemas de abuso es muy rápida, porque existen casos de dominios generados en el mismo día que fueron dados de baja por la plataforma y vuelven al estado “vacío”:



Los números no son tan decidores si vemos los sitios de phishing que hemos detectado:



Se ve un aumento considerable en agosto, pero 2 a 12 sitios detectados. Lo interesante del caso son los países a los cuales está afectando:



Aun cuando tenemos pocos datos, se nota que principalmente son sitios dedicados a afectar a personas en Colombia.

Además, como decíamos antes, hemos estado aprendiendo y "llegando tarde" en algunas ocasiones, porque de los 40 sitios que hemos revisado históricamente, solo 17 hemos detectado como Phishing. Esto va a ir cambiando en Septiembre, con nuevos patrones y detecciones integradas a la plataforma.

Aun cuando tenemos pocos datos, se nota que principalmente son sitios dedicados a afectar a personas en Colombia

Otra característica de estos sitios de phishing en la plataforma Replit es que para el nivel de servicio gratuito el código almacenado siempre va a tener como dominio principal **repl.co.** Esto nos ayuda en el monitoreo, lo malo es que las IPs públicas en donde se va a dirigir estos sitios no siempre es la misma, puede ser: 34.110.138.177, 34.149.204.188 o 35.186.245.55.

Con esta información, basta estar atento a los subdominios de repl.co y también monitorear las IPs en cuestión para poder ir detectando los nuevos scams.

Localtunnel

Sitio web: https://github.com/localtunnel/localtunnel

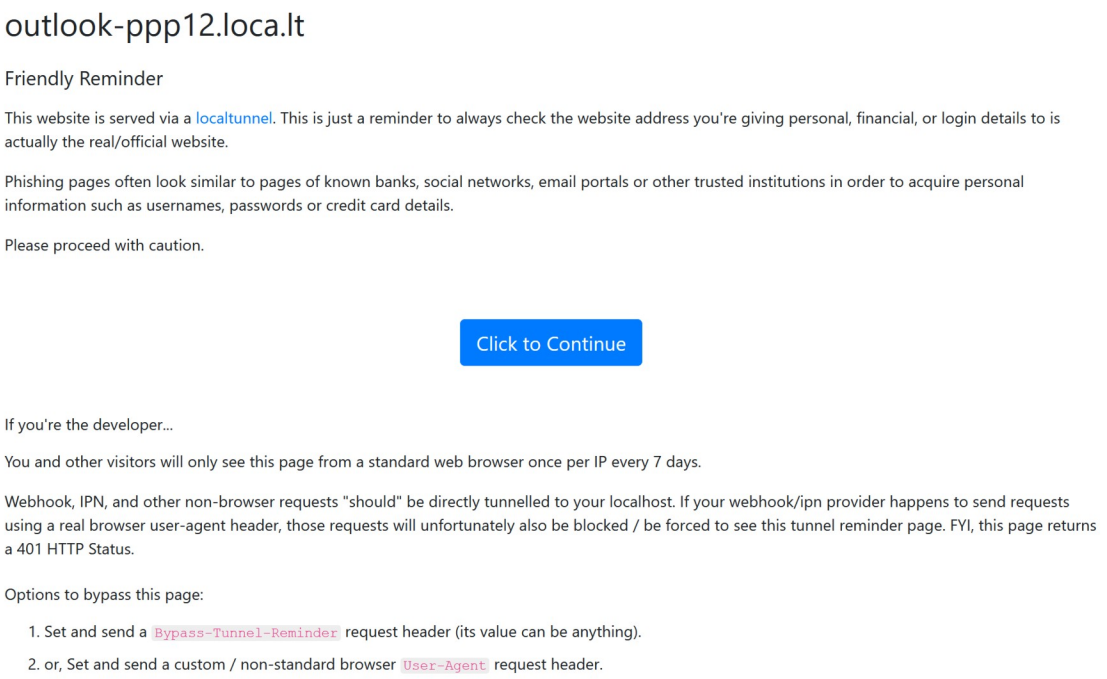
Prinicipal IP de phishing: 193.34.76.44

Localtunnel es un servicio que permite "mostrar" lo que tienes disponible en tu red privada interna (ej. red casera) a internet a través de un ruteo por internet. Esto hace posible que sitios web que están en pleno desarrollo y que no están listos para estar disponibles en internet puedan ser probados.

Esto además les permite a los ciberdelincuentes reducir los problemas de conseguir un hosting, porque todos los archivos quedan en tu red local y lo único que necesitas en ejecutar un comando como:

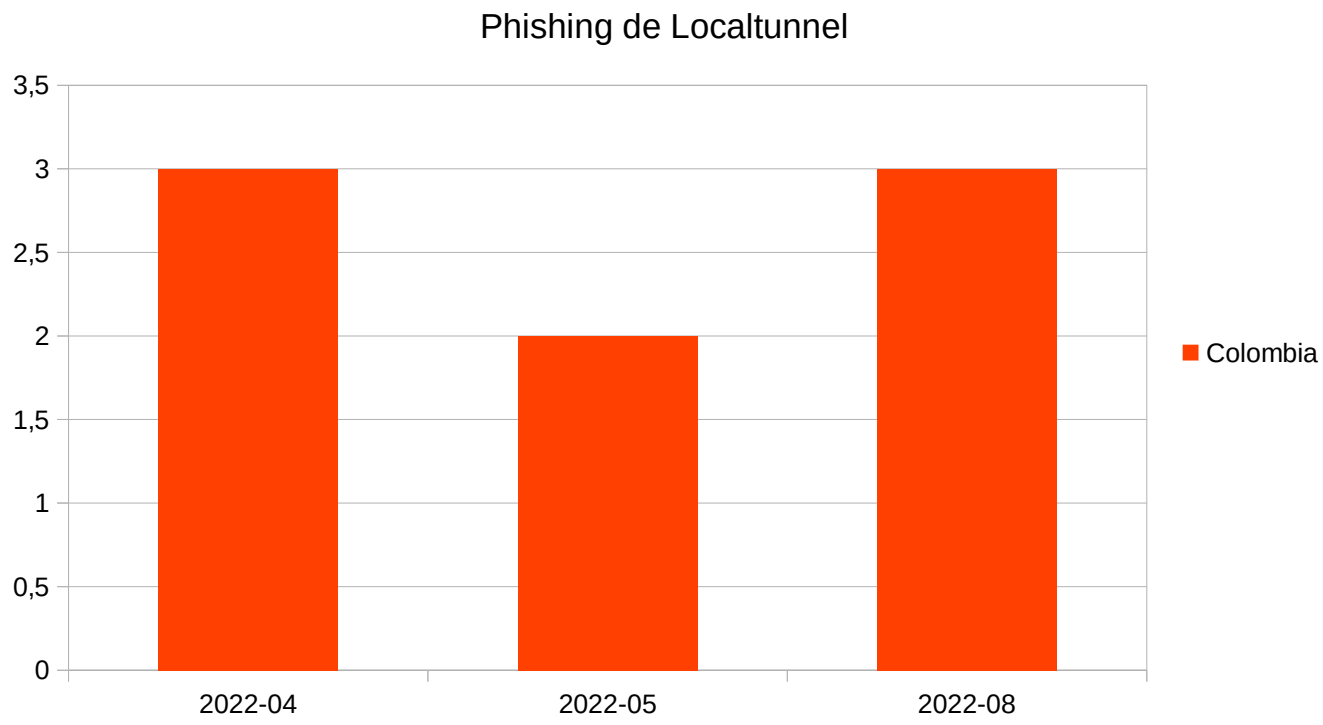
```
lt --port 8000 –subdomain [algo]
```

Con eso obtienes un subdominio de loca.lt o localtunnel.me, y ya tienes todo lo que se necesita para poder acceder al sitio de phshing. Lo malo es que te aparece una pantalla como la siguiente:



Lo que indica esta pantalla, es que justamente es un sitio hecho para desarrolladores que están probando sus servicios, y que se proceda con precaución porque pueden haber sitios de Phishing.

Aun con todo lo anterior, hemos detectado ciertos sitios de phishing, que han intentado montar su infraestructura de esta forma. Aunque son pocos, son decidores también de a qué público quieren atacar:



No lo podemos decir con certeza, pero creemos que son los mismos que están detrás del uso de Replit (visto en el punto anterior), los que están aprovechando ambas plataformas. Los kits que usan son muy similares, y probablemente están en la etapa de exploración de estas plataformas, para ver en cual se pueden quedar.

Creemos que en el futuro, van a dejar de usar Localtunnel y van a dirigir sus esfuerzos principalmente a Replit u otras plataformas similares en donde puedan subir cualquier código que quieran, sin tener esas pantallas de bloqueos.

Palabras finales

Al igual que en otros reportes, queremos agradecer a quienes nos han apoyado en la plataforma. A través de todos estos meses siempre es bonito y refrescante poder recibir las palabras de apoyo con el proyecto y que eso se traduzca tanto en la detección de nuevos kits como en el mejor entendimiento de éstos.

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

El "problema del Phishing" es algo que requiere una acción constante y hay que llegar un poco más allá para poder buscar el fondo del asunto. Cada institución afectada tiene el derecho de contactarse con empresas como Firebase, Replit 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 Julio
  - https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/
- Reporte Junio
  - https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/
- Reporte Mayo
  - https://finsin.cl/2022/06/05/reporte-mensual-de-phishing-mayo-2022/
- Reporte Abril
  - https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/
- Reporte Marzo
  - https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/
- Reporte Enero-Febrero 2022
  - https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/