FINSIN

Reporte de Phishing

Enero - Febrero 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 problema del "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 llegar a las personas al 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 que nos permitiera 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 Catcher 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.

Hoy en día me enorgullece presentarles algunos resultados de estas detecciones de los meses de enero (beta privada) y febrero (beta pública).

Ricardo Monreal Llop
Presidente FINSIN

TL;DR

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

El 80% de los sitios detectados afectan a las personas de Chile

Un 41% de los sitios usan la base de un mismo kit, el "0001"

El mismo kit "0001" es usado en múltiples países

Un grupo puede levantar hasta 9 sitios de phishing en un solo día

Existe un kit de phishing que permite descargar los datos de tarjeta robados directamente del sitio falso

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.

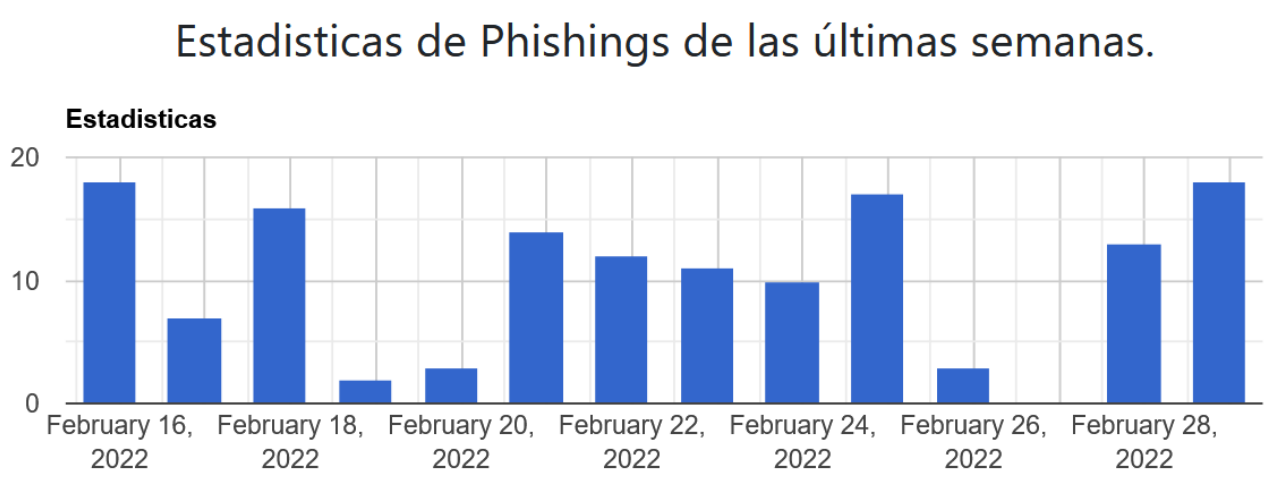
Phishing Checker

La plataforma “Phishing Checker” de FINSIN es un sitio web que ayuda tanto a usuarios normales 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 “porqué” 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/



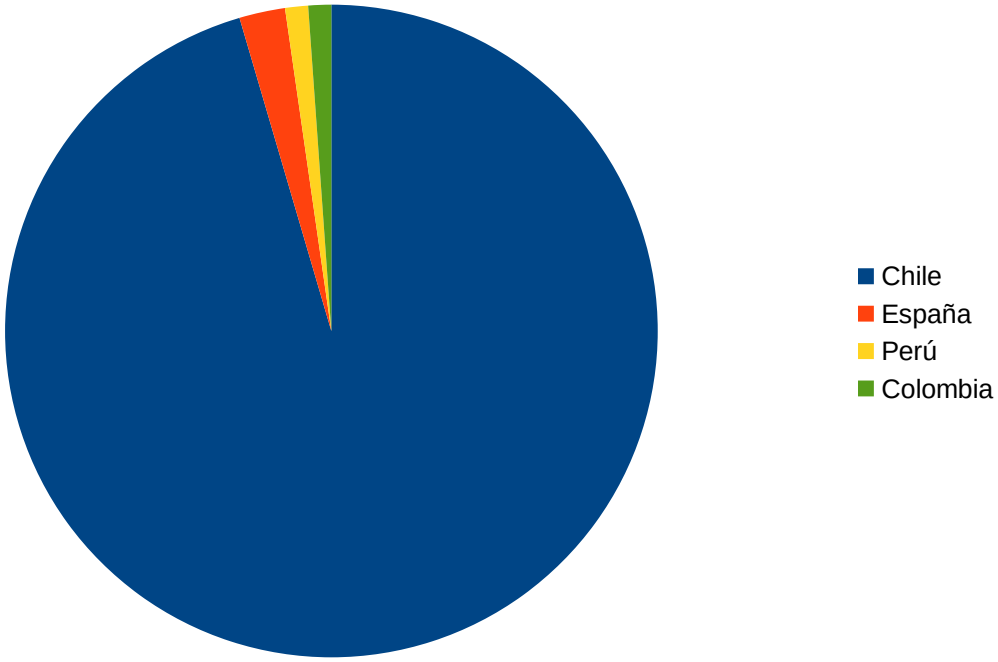
Enero 2022

Como se dijo anteriormente, en enero estuvimos en una beta privada en donde estábamos probando el sistema y podemos tener una base de lo que estamos revisando.

El esfuerzo en este mes fue apuntado principalmente a dar los toques finales a la detección de estos sitios y la respuesta de la plataforma en general, pero aún no podíamos "salir a la luz" para que cualquiera pueda ingresar, por lo que solamente ciertas personas seleccionadas nos ayudaban con estos reportes.

Datos de países[2]

En nuestra revisión detectamos a qué institución intentan afectar estos phishings y a qué país están dirigidos, y si lo miramos desde ese punto de vista tenemos el siguiente resumen:



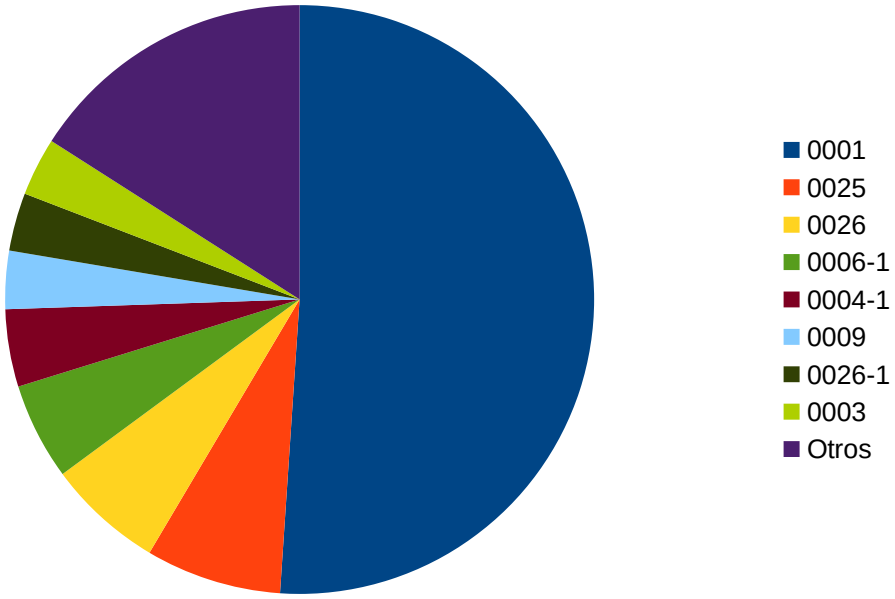
Pais	Porcentaje
Chile	95,45%
España	2,27%
Perú	1,14%
Colombia	1,14%

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

Dentro de los distintos tipos de kits que encontramos tenemos que predomina mucho el kit 0001, con el cual están atacando a distintas instituciones en toda latinoamética.

La distribución es la siguiente:



Pack	Porcentaje
0001	51,06%
0025	7,45%
0026	6,38%
0006-1	5,32%
0004-1	4,26%
0009	3,19%
0026-1	3,19%
0003	3,19%
Otros	15,96%

Aquí se ve que predomina claramente el 0001, con más del 50% de las detecciones, y es porque es el kit más distribuído en latinoamérica. Creemos fue desarrollado en Perú, desde donde comenzó su expansión.

Hoy en día afecta a empresas de Chile, Perú y Colombia, y puede ser mucho más expandido todavía pero nos faltan más detecciones.

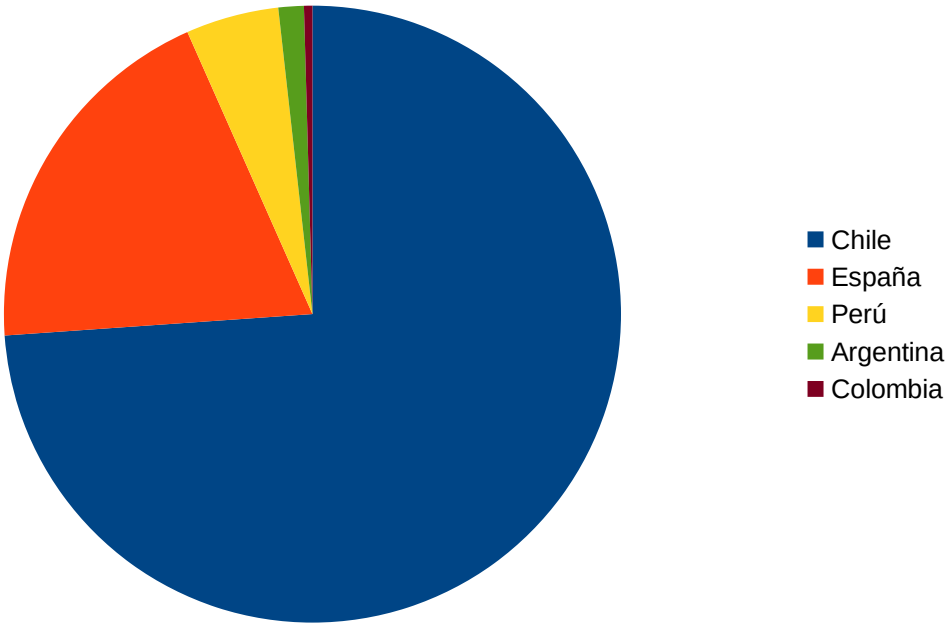
Febrero 2022

A fines de enero lanzamos la plataforma y logramos identificar muchos más sitios de phishing. Logramos un aumento del 256% en la cantidad de sitios detectados, lo cual en sí mismo ya es un gran logro.

Además logramos identificar 8 familias nuevas de Phishing, las cuales nos permitieron ampliar mucho los kits que podemos detectar.

Datos de países[3]

En nuestra revisión detectamos a qué institución intentan afectar estos phishings y a qué país están dirigidos, y si lo miramos desde ese punto de vista tenemos el siguiente resumen:



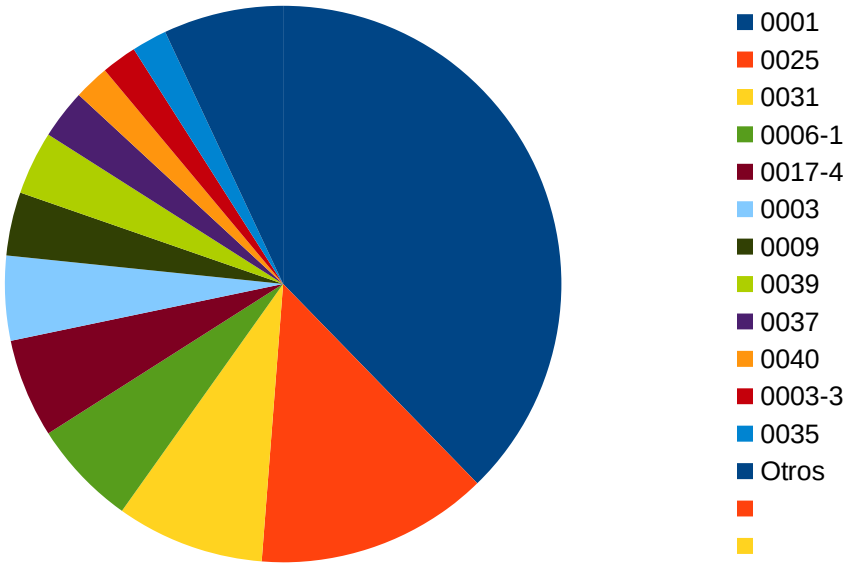
Pais	Porcentaje
Chile	73,89%
España	19,47%
Perú	4,87%
Argentina	1,33%
Colombia	0,44%

3 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.

Con esto se muestra claramente que empezamos a ver muchos más kits de otros países, principalmente España y Perú, que tienen tipos de phishing parecidos a los que afectan o afectaron a Chile.

Datos de kits

Si ponemos ahora los datos de los kits, tenemos lo siguiente:



Aquí se ve que predomina claramente el pack 0001, pero no tanto como el mes anterior porque el pack 0025 empieza a tomar mucho más protagonismo. Esto se verá cuando ahondemos en el grupo FC-01 más adelante.

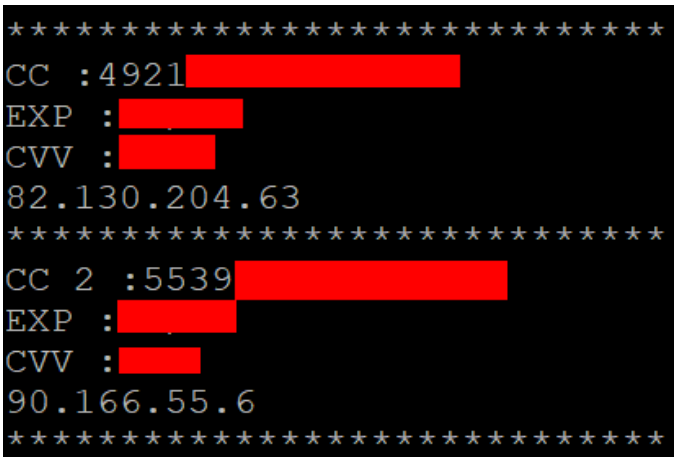
Pack	Porcentaje
0001	37,70%
0025	13,52%
0031	8,61%
0006-1	6,15%
0017-4	5,74%
0003	4,92%
0009	3,69%
0039	3,69%
0037	2,87%
0040	2,05%
0003-3	2,05%
0035	2,05%
Otros	6,97%

Caso de filtración de información

Este mes de Febrero tenemos un caso interesante a evaluar sobre la filtración de información que se produce al tener sitios de Phishing que ataquen a las personas.

Dentro de los kits de Phishing que detectamos hoy en día existe uno que clona la marca de una institución Española.

Este kit está dedicado a robar datos de tarjeta de crédito y de teléfonos de gente en España, y aunque mucha gente se da cuenta de que es una estafa e ignora el sitio o lo llenan con datos basura, hay casos de gente que se conectan y entregan información potencialmente verdadera.



Pudimos detectar que en este kit los datos robados están siendo almacenados directamente en el mismo sitio web en un archivo .txt, con lo que queda al alcance de los delincuentes que necesitan sacar esos datos rápidamente, pero también quedan al alcance de cualquier otro que sepa buscar.

Aunque nosotros no monitoreamos constantemente estos archivos para ver cuál es la actualización de estos datos en el tiempo, si tenemos algunas muestras de estos potenciales datos privados de las personas.

Con un poco más de 20 archivos distintos revisados tenemos un poco más de 1100 datos de tarjetas potencialmente válidas, lo cual no deja de ser interesante. Aún cuando de éstas el 50% sean falsas o virtuales, tenemos un importante número de datos de tarjetas para intentar hacer compras.

Lamentablemente en el reporte no podemos entregar más información acerca de las tarjetas, para cualquier consulta favor dirigirse directamente a los puntos de contacto de FINSIN.

Con un poco más de 20 archivos distintos revisados tenemos un poco más de 1100 datos de tarjetas potencialmente válidas

El grupo “Fishers Constantes 01”

En este reporte queremos ahondar en un grupo del cual no tenemos un nombre oficial, pero para poder agruparlo de alguna forma los queremos llamar “Fishers Constantes 01” (FC-01 en adelante).

El FC-01 está enfocado en levantar sitios de phishing contra algunas instituciones financieras en Chile, y está levantando sitios a una velocidad impresionante, hasta 9 sitios de phishing en un solo día.

Creemos que esta gran velocidad se debe principalmente que las instituciones afectadas tienen muy buena respuesta en la baja de los sitios, por lo que tienen que estar atentos y cambiar rápidamente en cuanto haya una sospecha de “takedown”.

Aprovechamos de agradecer a las instituciones por hacer rápido el takedown y por mantener la comunicación para cuando tenemos este tipo de información.

Si nos enfocamos en una de las instituciones afectadas, en todo el mes de febrero levantaron 33 sitios distintos de Phishing. Pero cuando empezamos a ver si en la misma infraestructura tenemos más sitios o dominios de otras instituciones tenemos resultados bien interesantes: levantaron 81[4] sitios de Phishing.

El FC-01 está levantando sitios a una velocidad impresionante, hasta 9 sitios de phishing en un solo día.

No podemos asegurar con certeza que todos los sitios de phishing sean del mismo grupo, pero estamos bastante confiados en que no es coincidencia lo que ellos están haciendo.

Les comento un poco como fue apareciendo esta evidencia:

4 Este número es solamente de los sitios/dominios que logramos identificar, pueden haber más

1) Un nuevo kit

Una de las primeras instancias en donde empezaron a aparecer cosas extrañas fue a fines de Enero, cuando comenzamos a detectar un kit totalmente nuevo, lo nombramos internamente el kit “0025”, y esto nos dió unas luces de un patrón nuevo que podría comenzar a repetirse.

Junto con ese nuevo kit, apareció un dominio sospechoso (que no pudimos clasificar inmediatamente como phishing) en la misma IP, con un patrón muy similar. Al tener ambos dominios en la misma IP, nos da una idea que pueden ser el mismo grupo que está controlando ambos dominios, pero la evidencia es muy pobre.

En este momento solamente teníamos los dominios finales del Phishing, y el patrón para clasificarlos como tal. Pero nos falta evidencia de cómo le llega esa URL a la persona que quieren engañar.

Links a los reportes

- Detección inicial: https://phishing.finsin.cl/list.php?query=e81863f2743d06da486a75848052ac87c114b8c86670649c227619a5a348bcf7
- Detección sospechosa: https://phishing.finsin.cl/list.php?query=60742160c5346ab97b8a2e2a8c1a681a7b892b0bb86b2a02a510e1ab2341a02c

2) Otro link de lo mismo

Luego de eso, el 30 de Enero encontramos el link inicial (o por lo menos eso creíamos en ese momento) que le enviaban a los clientes, con lo cual se empieza a observar la "arquitectura" detrás del phishing. Ahora vemos que el link que envía es solo parte de una cadena:

N° Redirección	URL Redirección
0	http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en-GB/enviar02.php
1	https://bit.ly/35xWPLu?l=www.bancofalabella.cl
2	http://www.endrich.jp/activacion/cuenta-ohzj/
3	https://www-falabella-cl.artech.gr/login

Tenemos que en este caso:

- La URL 0, es el link enviado a los clientes, con un archivo llamado "enviar02.php"
- La URL 1 es una redirección de bit.ly para ocultar algún patrón malicioso
- La URL 2 es un nuevo dominio de redirección, que solo se utiliza como filtro y gestión
- La URL 3 es finalmente el sitio de phishing

Lo interesante de este caso es que finalmente la arquitectura armada es mucho más compleja de lo que se creía en un principio, y nos dedicamos ahora a investigar estas redirecciones.

Además, igual que en el caso anterior, si verificamos la IP en donde está alojado, también nos aparece otro phishing, con un patrón similar, pero que afecta a otra institución en Chile.

Lo interesante es que si monitoreamos ese link solo, vemos que con los días va cambiando el destino final, pero la ruta se mantiene casi constante, si se busca por este dominio tenemos lo siguiente:

Result	Query
Phishing (Reporte)	Query: https://bit.ly/3JaXa55 Final: http://www-banc0falabella-cl.judithmartens.nl/login
Phishing (Reporte)	Query: https://bit.ly/3JaXa55 Final: https://www-banc0falabella.cl.visionhvac.in/login
Phishing (Reporte)	Query: https://bit.ly/3JaXa55 Final: https://wwwbanc0falabella-cl.visionhvac.in/login
Phishing (Reporte)	Query: https://bit.ly/3JaXa55 Final: https://www-banc0falabella-cl.corescappilates.co.za/login
Error en scan (Reporte)	Query: https://bit.ly/3JaXa55 Final: http://xn--1990-4eor2hg0cxbdc9jbd9c2c7b6kf5pvcg.co...
Phishing (Reporte)	Query: https://bit.ly/3JaXa55 Final: http://www-banc0falabella-cl.dstgroup.vn/login
Phishing (Reporte)	Query: https://bit.ly/3JaXa55 Final: https://www-banc0falabella-cl.apspayroll.com.au/login
Phishing (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-banc0falabella-cl.bzbestbuyer.com/login
Phishing (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-banc0falabella-cl.bzbestbuyer.com/login
Phishing (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-banc0falabella-cl.hoanmyquangninh.vn/login
Normal (Reporte)	Scam: https://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/e...
Phishing (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-banc0falabella.cl.pixel8k.com/login
Phishing (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-banc0falabella-cl.pixel8k.com/login
Phishing (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-banc0falabella.cl.maderasparada.cl/login
Phishing (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-banc0falabella-cl.maderasparada.cl/login
Sospechoso (Reporte)	Query: http://xn----8sbirdcwdj7bl2hk.xn--p1ai/language/en... Final: https://www-falabella-cl.artech.gr/login

¡El mismo dominio aparece dentro de las redirecciones de muchos de los sitios de phishing!

Con esto deducimos que el mismo grupo reutiliza la misma infraestructura, y solamente cambia la URL final.

Links a los reportes

- Detección inicial: https://phishing.finsin.cl/list.php?query=7e4c2b81c2e6b7d5ad6a90f890f3aabab9fa9a6447ecec59df1106bda8d1b7f5

- Detección del dominio solo: https://phishing.finsin.cl/list.php?query=3cee9866635a9178a81d48ed7269042f8760b3c5d7f02f592f09d98feea4f206
- Detección del otro dominio de la misma IP: https://phishing.finsin.cl/list.php?query=bc6098a47d4d8db1d86c181d85fbf12165eb01be1d94277c0fcc9abca5576711

3) Encontrando más evidencia

A través de los días, más sitios de phishing iban apareciendo con los mismos patrones de URL final y con la misma arquitectura, ya sea cambiando la URL final, o la URL intermedia de "redirección y gestión".

El patrón se va repitiendo, y de hecho se repite tanto que tenemos que ir generando reportes constantes de estos dominios nuevos que van apareciendo.

Luego de esto, el 18 de Febrero pudimos encontrar un "link original" que hacía el mismo trabajo que antes, pero con otra institución:

N° Redirección	URL Redirección
0	https://bit.ly/3gMw34i?l=w.bancoestado.cl
1	http://xn--119-hy7mx2m78r.kr/assets/bootstrap/css/enviar03.php?l=858384412
2	https://bit.ly/3LFsKtX?l=www.bancoripley.cl
3	https://sam-tech.jp/activacion/cuenta-ihgg/
4	http://www-bancoestado-cl.judithmartens.nl/
5	http://www-bancoestado-cl.judithmartens.nl/1645192514/Login

Acá vemos un patrón muy parecido al de antes, pero partiendo de un bit.ly:

- La URL 0 es el bit.ly que le llega a las personas afectadas
- La URL 1 es la redirección inicial con el script "enviar03.php"
- La URL 2 es el segundo bit.ly que actúa como redirector para ocutlar la amenaza
- La URL 3 es el dominio de redirección y gestión con el patrón "activación/cuenta-[random]"
- La URL 4 es el dominio de phishing final
- La URL 5 es la URL final de phishing que se le muestra a la persona afectada, que tiene un timestamp en la misma URL.

Un patrón demasiado parecido al anterior, pero que tiene como objetivo una segunda institución financiera.

Y si revisamos el mismo link 2 días después el 20 de Febrero tenemos que cambiaron nuevamente la institución afectada, pero repitiendo el mismo patrón:

N° Redirección	URL Redirección
0	https://bit.ly/3gMw34i
1	http://xn--119-hy7mx2m78r.kr/assets/bootstrap/css/enviar03.php?l=858384412
2	https://bit.ly/3oZTdbZ?l=www.bancoripley.cl
3	https://wardatalwadirealestates.com/activacion/cuenta-vqgw/
4	http://www-bancoripley-cl.judithmartens.nl/
5	http://www-bancoripley-cl.judithmartens.nl/1645387572/Login

Links a los reportes:

- Detección 07 de Febrero: https://phishing.finsin.cl/list.php?query=35c4eab920660150206670cb235d36d5e3e813d90a6410ce64773d2369feac8d
- Detección 14 de Febrero: https://phishing.finsin.cl/list.php?query=c6ce2c8a9f017aab5f1c564ec880c90d0d435dd37996a77b1b4bcccc07618532
- Detección 18 de Febrero: https://phishing.finsin.cl/list.php?query=ebdde41484c3cdb9d0952c59d13745e92c082ee8f7d7a267b6a757ee6832707c
- Detección de nuevo afectado: https://phishing.finsin.cl/list.php?query=419c375222eeb3456aa788d19ef83b8d4d8b94f5b6901ee4cc4aaf5abb04f862
- Detección de cambio de primera redirección: https://phishing.finsin.cl/list.php?query=cdb7dca31ec874904a623f801d099fa6abbd268bd7e51db4163ec17431058d2e

Finalmente...¿gracias FC-01?

Juntamos toda la evidencia de los kits que estas personas están usando, más las IP en las que montan esta infraestructura y tenemos los siguientes datos del mes de Febrero:

Dominios totales levantados: 81
IPs totales usadas: 15
Instituciones afectadas: 4 (por ahora)

Cantidad de sitios, por IP:

IP	Cantidad
42.112.30.39	13
185.69.233.105	12
192.185.75.180	10
43.224.137.92	7
135.181.225.5	6
89.252.190.36	5
101.0.123.146	4
138.117.149.178	4
147.124.223.173	4
5.77.50.29	4
196.12.12.102	3
213.136.93.169	3
69.16.230.59	3
185.94.230.132	2
137.74.76.89	1
Total	81

Si miramos con detención, logran usar muchas IPs distintas para sus sitios, y algunas se repiten bastante. Tenemos que tener ojo con las 3 principales, porque lo más probable es que tarde o temprano vuelvan a usarlas con otro dominio.

Cantidad de sitios, por fecha:

Fecha	Cantidad
2022-02-01	3
2022-02-02	1
2022-02-03	3
2022-02-04	1
2022-02-05	0
2022-02-06	1
2022-02-07	2
2022-02-08	3
2022-02-09	4
2022-02-10	0
2022-02-11	0
2022-02-12	0
2022-02-13	0
2022-02-14	4

Fecha	Cantidad
2022-02-15	4
2022-02-16	7
2022-02-17	0
2022-02-18	4
2022-02-19	1
2022-02-20	1
2022-02-21	6
2022-02-22	6
2022-02-23	9
2022-02-24	5
2022-02-25	8
2022-02-26	2
2022-02-27	0
2022-02-28	6

Estos datos nos muestran una tendencia al alza a fines de mes, y datos impresionantes como que el 23 de Febrero se llegó a un peak de 9 sitios, pero el 25 no se queda atrás con un total de 8 sitios levantados.

Como dato curioso de este caso, este grupo se nota que trabaja principalmente en la semana laboral, porque los fines de semana se nota demasiado la baja de actividad.

Por ejemplo, usando todos los datos anteriores tenemos estos números por día de semana:

Dia	%
Lu	22,22
Ma	19,75
Mie	25,93
Ju	9,88
Vi	16,05
Sa	3,7
Do	2,47

Y no sé si alguna vez lean esto, pero muchas gracias a FC-01 por darnos el fin de semana libre ;)

Palabras finales

Primero quieremos 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.

El “problema del Phishing” es algo que requiere una acción constante que sea más que solamente buscar si en el domino aparece el nombre de una marca, o se reconoce la imagen corporativa del sitio original. Hay que llegar un poco más allá para poder buscar el fondo del asunto.

Con FINSIN estamos buscando llegar más allá y creemos que con este tipo de plataformas podemos dar más información tanto para las empresas afectadas, como 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.