FINSIN

Reporte de Phishing

Abril 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 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.

Ricardo Monreal Llop
Presidente FINSIN

TL;DR

A modo de resumen, tenemos los siguientes resultados para el mes de Abril:

Les queremos presentar el grupo FC-02

Este mes tenemos el surgimiento de 2 packs que antes estaban muy abajo en las detecciones

Una IP tiene 24 de los 29 casos del kit 0037 en Abril

Sigue constante el robo de datos de tarjetas a personas en España

En una campaña de FC-02 tenemos 48 dominios para el mes de abril y 33 para el mes de marzo!

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

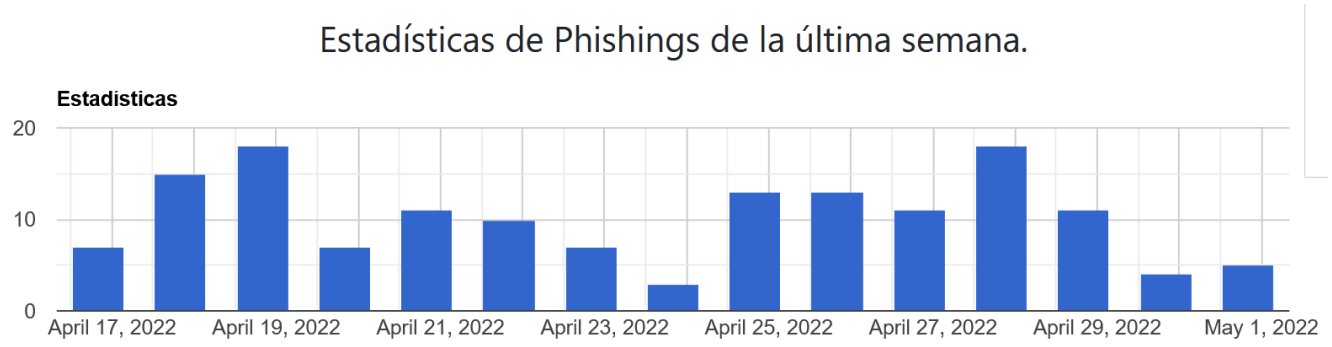
Phishing Checker

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/

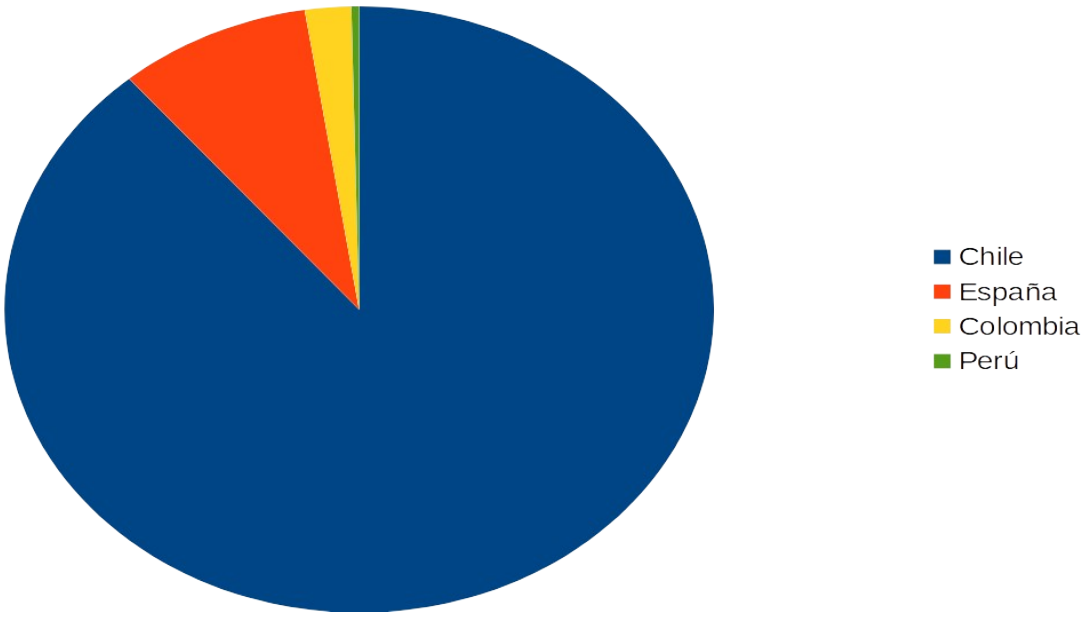


Abril 2022

En el mes de abril tuvimos bastante movimiento por la detección de phishings, tanto a nivel de tipos, como a nivel de cantidad de sitios por día.
Tenemos la detección de 4 nuevos kits, más la configuración de nuevas variantes para kits antiguos, logrando un total de 17 nuevas formas de phishing que el mes de marzo no teníamos.

Datos de países[1]

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:



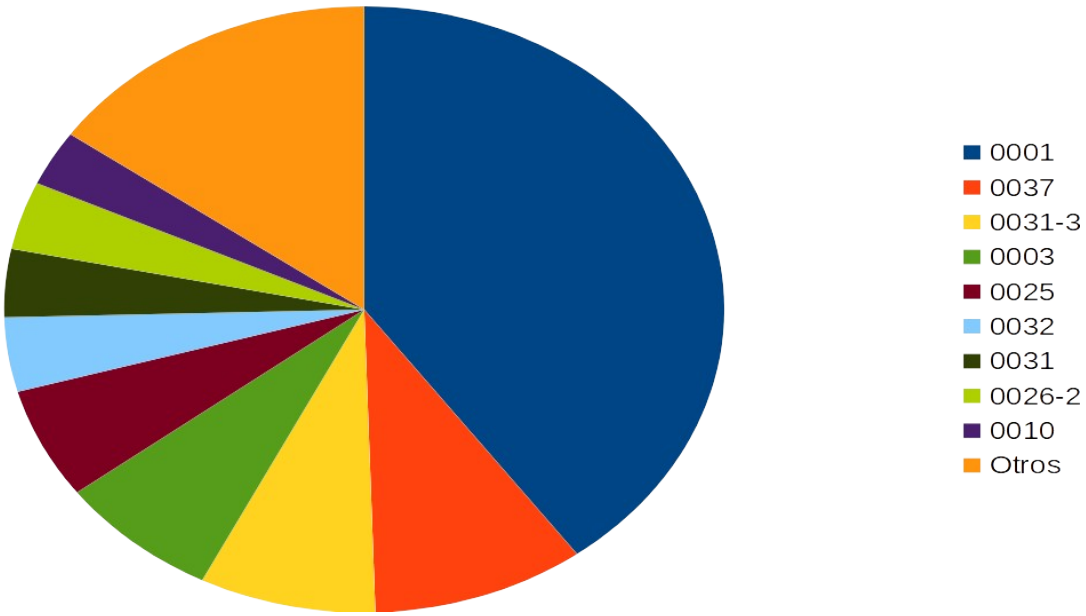
Pais	Porcentaje
Chile	88,77%
España	8,77%
Colombia	2,11%
Perú	0,35%

1 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 seguimos teniendo como tendencia que predomina mucho el kit 0001, pero ahora bajó del 40% de las detecciones. Además, este mes tenemos el surgimiento de 2 packs que antes estaban muy abajo en las detecciones.

La distribución es la siguiente:



Pack	Porcentaje
0001	39,93%
0037	9,57%
0031-3	7,92%
0003	7,26%
0025	5,94%
0032	3,96%
0031	3,63%
0026-2	3,63%
Otros	18,15%

El ingreso del kit “0037” en el top 3 nos muestra una campaña que está siendo utilizada contra una institución bancaria en Chile. Este pack no es nuevo, pero sí hubo una fuerte crecida de este pack con 29 dominios en el mes, casi uno diario.

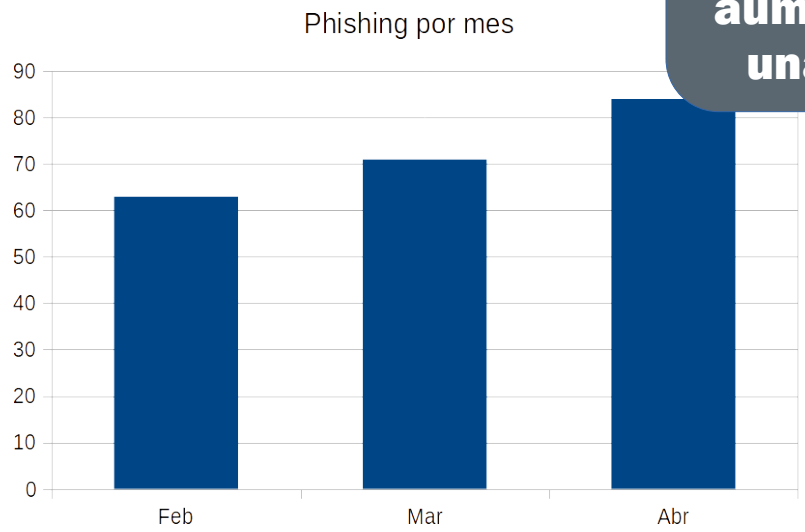
El pack “0031-3” es la tercera variante de un pack de detección que tenemos para los sitios usado con la institución española que venimos siguiendo desde enero. Su actividad ha sido bastante agresiva este mes, y lo revisaremos un poco más adelante.

Caso de filtración de información

Como veíamos en el resumen de los kits detectados por la plataforma, sigue constante el robo de datos de tarjetas a personas en España. Este mes sigue fuerte la campaña que busca clonar a una institución española:

A través de los meses hemos visto que, al contrario de lo que se podría pensar luego de varias publicaciones[2][3] intentando concientizar al respecto este tipo de estafa, sigue siendo muy utilizada y que incluso ha aumentado. Como se ve en el siguiente gráfico:

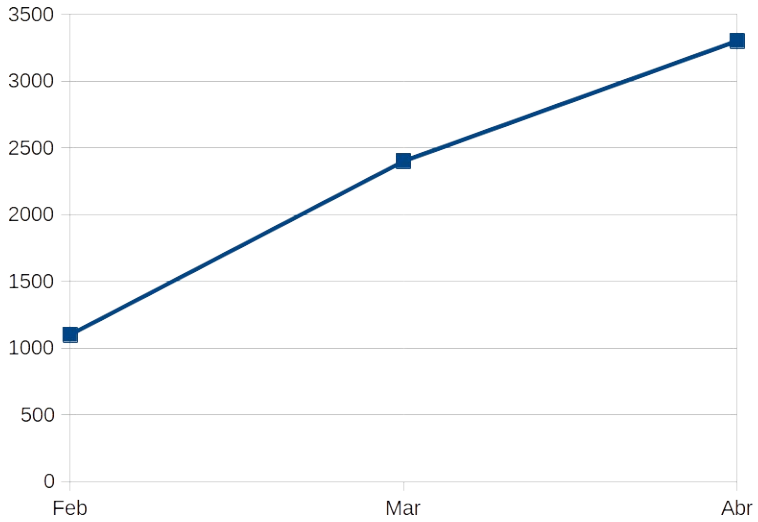
A través de los meses hemos detectado un aumento, en vez de una disminución



2 https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-phishing-suplantando-correos-robar-informacion

3 https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-phishing-suplantando-correos-0

Ahora, al revisar cuan lucrativa sigue siendo esta campaña tenemos que revisar qué tan efectivos son en recibir datos de tarjeta de crédito/debito. Con lo revisado este mes logramos acumular más de 3300 datos de tarjeta, manteniendo la trayectoria en ascenso de los datos obtenidos por estos cibercriminales.



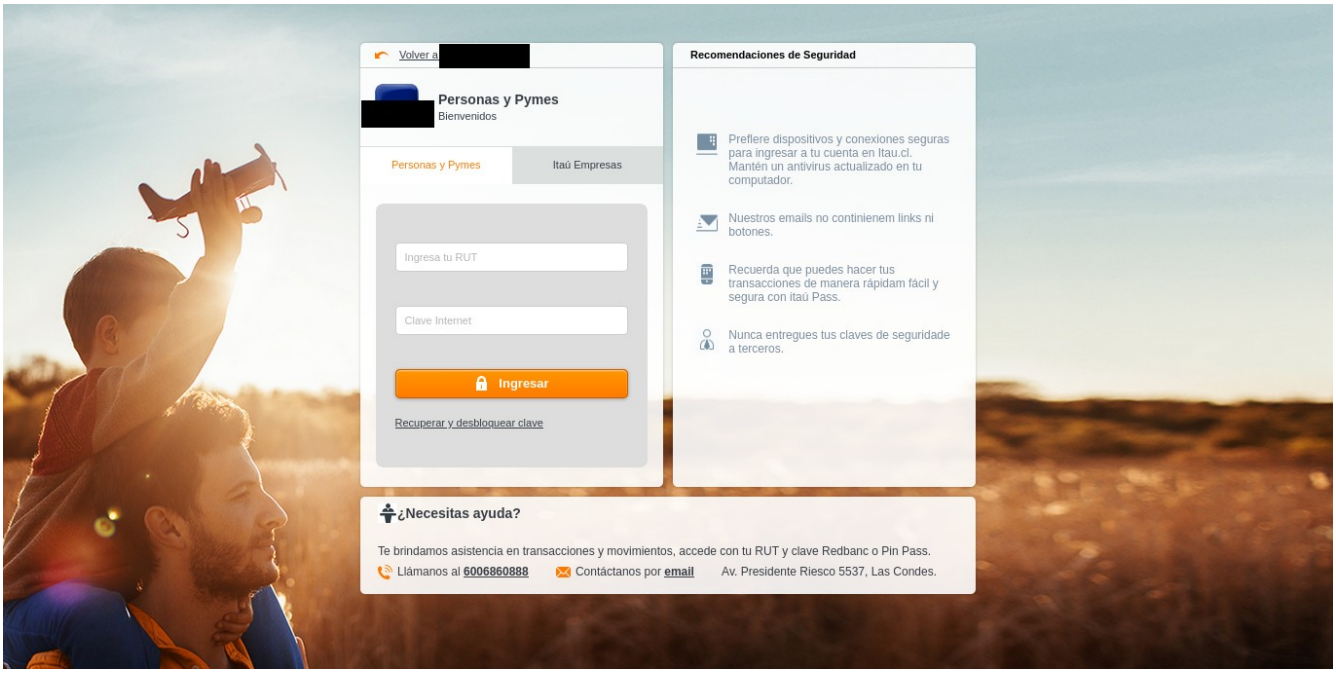
Lamentablemente en el reporte no podemos entregar más información acerca de las tarjetas, para cualquier consulta favor dirigirse directamente a los puntos de contacto de FINSIN.

A pesar de todo lo malo, a fin de mes (el 30 de abril) los "Mossos d'Esquadra" (policía de Cataluña) lograron atrapar[4] a dos personas de 19 y 20 años que están directamente implicados con este tipo de engaños. Ojalá que con ésta y otras investigaciones futuras se puedan disminuir este tipo de phishing y ayudar a las víctimas.

4 https://www.elperiodico.com/es/delitos-informaticos/20220430/mossos-estafa-sms-phishing-smishing-13591088

Pack 0037

Este nuevo pack, que afecta a una institución bancaria chilena, lo comenzamos a detectar por primera vez a inicios de febrero[5], y es bastante bullicioso por el tipo de URL que genera:



`https://[Dominio]/App91bf4ee/access.php?verify=IAHIVXUOIAHI-6QE4-IAHI6QE46QE4-5TG76QE4&sessionUser=dqil8gatnmkcg2ln8c78j36r6e&userLogin=c51ce410c124a10e0db5e4b97fc2af39&queryString=`

Este tipo de sitio (al igual que otros como el 0001) lo único que quiere es que las detecciones por URL completa sean ineficientes, por lo que usa una parte aleatoria dentro de ella.

En la URL de ejemplo anterior tenemos que luego del dominio principal, hay una ruta que comienza con App y luego le sigue con 7 caracteres raros (en el caso del ejemplo es "App91bf4ee"). De hecho, si ingreso nuevamente al sitio raíz me genera otra ruta aleatoria dentro de la url, en esta caso "App7378009"[6].

5 https://phishing.finsin.cl/list.php?query=518fdfd81240c33fbf386eb63c44a52c467e00dae6b1fa89edb92478f0c25a70

6 https://[Dominio]/App7378009/access.php?verify=G99QDKVPG99Q-EV6S-G99QEV6SEV6S-N7GEEV6S&sessionUser=dqil8gatnmkcg2ln8c78j36r6e&userLogin=c51ce410c124a10e0db5e4b97fc2af39&queryString=

Además, para cargar los archivos JS del kit usa una ruta relativa que apunta a la “raiz” del sitio:

```
<script src="../public/javascripts/jquery.min.js"></script>
<script src="../public/javascripts/jrut.js"></script>
<script src="../public/javascripts/jquery.mask.js"></script>
<script src="../public/javascripts/all.js"></script>
```

Con esto podemos asumir que la programación del sitio de phishing es en la ruta base del dominio, de hecho tenemos el archivo api.php como parte del proceso de autenticación y monitoreo.

La información que tenemos de este kit es solamente circunstancial, no contamos con el kit completo para poder analizarlo como en ocasiones anteriores, pero tenemos algo de evidencia. En ciertos sitios de phishing existe un log con información de los afectados, por ejemplo, en el archivo “xreg.txt” tenemos la lista de las víctimas que ingresaron al sitio, pero solamente con la IP, el tipo de navegador y la ubicación geográfica:

```
04-May-2022**22:58:04**Mobile (iPhone)****/?SEDRFG7H8JD6H3FLS323D4F5G6H7JHGTFRCE
XCRVTYBUNHYGTFRDERFTGYHUJH7654E34R56Y78UJ7HGTFREDRFTGYHUJHYGTFRDCECRVTBYNUYBTVRC
EXUYG6F5D43SDECRVTBYNUIMNUBYVTRCXES4ER56GYNBYVTCR**186.106.108.138 (186.106.108.
138)**Safari**Chile - Santiago Santiago Metropolitan
04-May-2022**23:09:46**Mobile (iPhone)****/?SEDRFG7H8JD6H3FLS323D4F5G6H7JHGTFRCE
XCRVTYBUNHYGTFRDERFTGYHUJH7654E34R56Y78UJ7HGTFREDRFTGYHUJHYGTFRDCECRVTBYNUYBTVRC
EXUYG6F5D43SDECRVTBYNUIMNUBYVTRCXES4ER56GYNBYVTCR**191.125.176.203 (191-125-176-
203.bam.movistar.cl)**Safari**Chile - Santiago Santiago Metropolitan
04-May-2022**23:23:56**Desktop (Mac OS)****/?SEDRFG7H8JD6H3FL323D4F5G6H7JHGTFRCE
XCRVTYBUNHYGTFRDERFTGYHUJH7654E34R56Y78UJ7HGTFREDRFTGYHUJHYGTFRDCECRVTBYNUYBTVRC
EXUYG6F5D43SDECRVTBYNUIMNUBYVTRCXES4ER56GYNBYVTCR**191.112.91.213 (191-112-91-21
3.baf.movistar.cl)**Chrome**Chile - Santiago Santiago Metropolitan
04-May-2022**23:26:46**Desktop (Windows)****/?SEDRFG7H8JD6H3FL323D4F5G6H7JHGTFRC
EXCRVTYBUNHYGTFRDERFTGYHUJH7654E34R56Y78UJ7HGTFREDRFTGYHUJHYGTFRDCECRVTBYNUYBTVR
CEXUYG6F5D43SDECRVTBYNUIMNUBYVTRCXES4ER56GYNBYVTCR**190.208.14.73 (cache.google.
com)**Chrome**Chile - Santiago Santiago Metropolitan
04-May-2022**23:36:21**Mobile (Android)****/?SEDRFG7H8JD6H3FLS323D4F5G6H7JHGTFRC
EXCRVTYBUNHYGTFRDERFTGYHUJH7654E34R56Y78UJ7HGTFREDRFTGYHUJHYGTFRDCECRVTBYNUYBTVR
CEXUYG6F5D43SDECRVTBYNUIMNUBYVTRCXES4ER56GYNBYVTCR**191.112.164.71 (191-112-164-
71.baf.movistar.cl)**Chrome**Chile - La Florida Santiago Metropolitan
```

Cuando revisamos los sitios que han sido generados con este kit vemos que hay una tendencia que se repite. Son casi todos de la misma IP: 20.226.60.161

Esta IP tiene 24 de los 29 casos de este kit en Abril, lo cual la hace un foco para nuestros monitoreos. Lo ideal sería que para dar baja de este tipo de ataque se genere un reclamo de abuso contra el hosting, más aún si es una IP administrada por Microsoft.

Dentro de las detecciones de este tipo de pack tenemos el apoyo de Germán Fernández en Twitter[7], mostrando que al igual que en otros casos, la administración de estos sitios se encuentra directamente en el sitio (con credenciales simples). Pudiendo acceder a la información de los afectados directamente.

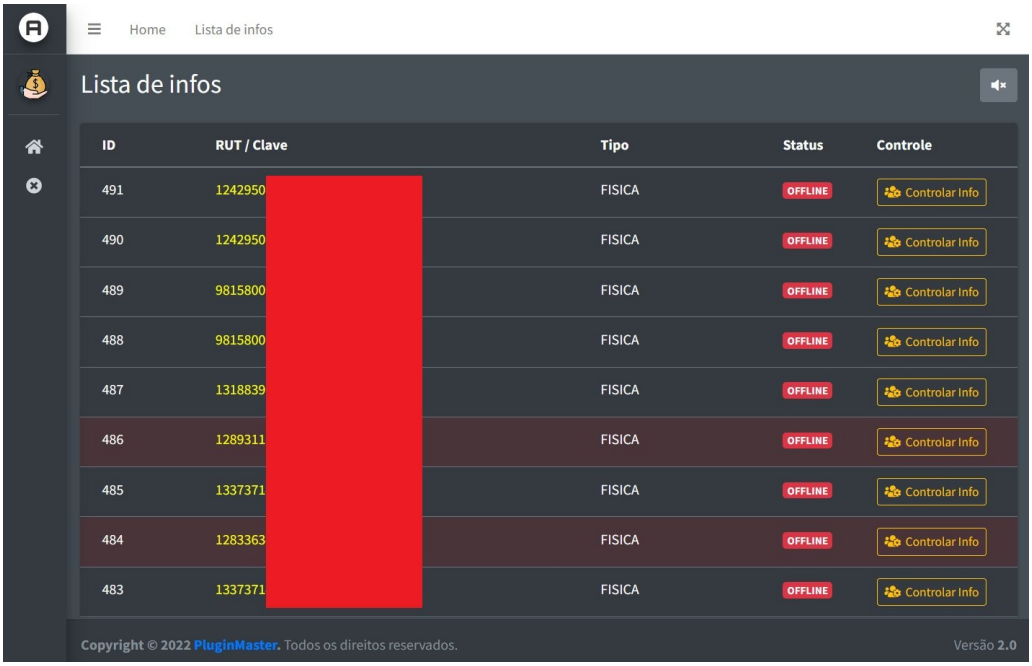


Foto obtenida por @1ZRR4H en Twitter

Lamentablemente no es siempre igual, depende de la "variante" de este kit donde se encuentra el sitio de administración. No hemos podido encontrar el panel de administración de todas estas variantes, pero esperamos que con la ayuda de la comunidad, podamos poder seguir aprendiendo de este y otro tipo de Phishing.

7 https://twitter.com/1ZRR4H/status/1513598645656072197

El grupo “Fishers Constantes 02”

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 02” (FC-02 en adelante).

El FC-02 está enfocado en levantar sitios de phishing contra una institución bancaria específica en Chile, y lo hace a través de una metodología muy precisa.

Al revisar cuál es el pack que utilizan, no es tan novedoso, es el mismo pack 0001. Como hemos dicho anteriormente este pack es muy robusto, y ha sido utilizado desde hace mucho tiempo para campañas tanto en Chile como en otros países de Latinoamérica.

Lo interesante de este caso es la cantidad de dominios nuevos que van generando para esta campaña y la forma en que mantienen cierta infraestructura para ello. Dentro de nuestras detecciones **tenemos 48 dominios para el mes de abril y 33 para el mes de marzo**.

Creemos que esta gran velocidad se debe principalmente a 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”.

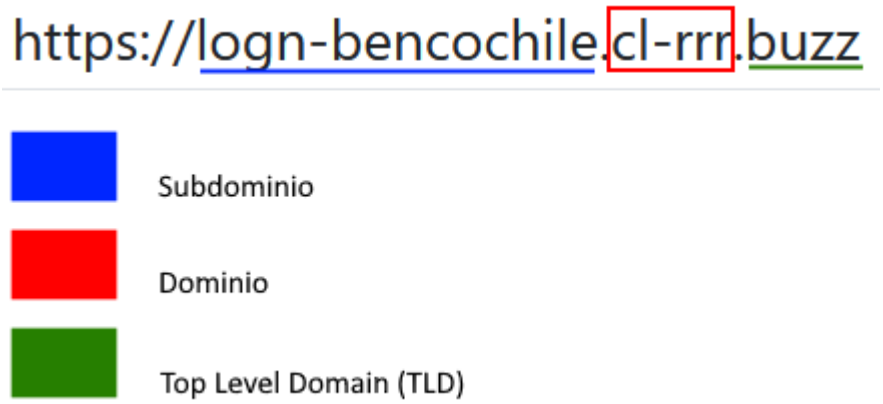
Tenemos 48 dominios para el mes de abril y 33 para el mes de marzo

Caso inicial

El primer caso que encontramos de un sitio subido por FCO2 fue en febrero de este año[8], pero por el desconocimiento de como operaban, no hicimos un correcto seguimiento de este caso, sino que fue solamente una detección de una vez. Lo interesante es ver la estructura que tenía este caso:

N° Redirección	URL Redirección
0	https://bit.ly/portal-banchile
1	https://diarioedomex.com/banchile.php
2	https://logn-bencochile.cl-rrr.buzz
3	https://logn-bencochile.cl-rrr.buzz/1644977705/bcochile-web/persona/login/index.html/login

Podemos ver que parte con link del acortador Bitly, y luego pasa por un dominio que tiene un script .php que finalmente redirige al sitio final del Phishing. Lo llamativo del sitio final de phishing es el patrón que tiene:



Este patrón es interesante, porque colocan como subdominio un string que sea similar al sitio de la institución afectada, luego en la parte del dominio principal es “cl-[algo]”, en este caso es un string aleatorio de 3 letras, y finalmente termina con el top level domain .buzz.

Al contar los caracteres desde el inicio del subdominio hasta las primeras 2 letras del dominio tenemos 18 caracteres. Esto lo hacen para que en los dispositivos celulares no se lea el TLD, y que todo lo demás parezca del sitio original.

8 https://phishing.finsin.cl/list.php?query=cd173f3be9c96e4e912382e8d6a8efc17af98e71ab3a622aeea7d1ad38a71f42

Luego de ese caso, volvemos a encontrar un caso parecido el 03 de marzo[9], solo que con otro link inicial:

N° Redirección	URL Redirección
0	https://bit.ly/aumento-marzo
1	https://melissagilfillian.com/chile1.php
2	https://logn-bnnchochile.cl-ijb.buzz/
3	https://logn-bnnchochile.cl-ijb.buzz/1646340365/bcochile-web/persona/login/index.html/login

Podemos ver que a nivel de redirecciones es la misma idea, parte con un Bitly, luego viene un dominio que en la raíz tiene un script .php que finalmente redirige al sitio de phishing.

Si vemos el subdominio final, tenemos que sigue teniendo un patrón similar: un subdominio largo que parezca al sitio original, un dominio principal que sea "cl-[algo]", y termina con el TLD .buzz.

Todo es muy similar para dejarlo de lado como coincidencia, pero todavía no nos percatabamos que era algo más. Llegó el tercer caso[10] de este patrón el 07 de marzo y volvía a ser lo mismo que antes:

N° Redirección	URL Redirección
0	https://bit.ly/cuposs_marzo
1	https://heidikrieghauser.com/chile.php
2	https://logim-bnnchochile.cl-gdd.buzz/
3	https://logim-bnnchochile.cl-gdd.buzz/1646656565/bcochile-web/persona/login/index.html/login

Dos veces es coincidencia, pero una tercera habla de un patrón de comportamiento. Sigue comenzando con un link Bitly, luego un dominio que en la raíz tiene un script .php que finalmente redirige al sitio final que en su dominio principal es un "cl-[algo]" y luego el TLD es .buzz.

9 https://phishing.finsin.cl/list.php?query=f3cc25d34241e5148d620e47fd742189bb9dd3d6c0508a39b669284d247079c8

10 https://phishing.finsin.cl/list.php?query=2bdfb5806529bfb3491b488eef4b3c08dbcba5838781117b3e5b443266258610

Pero además, ese mismo día apareció otro caso curioso[11]:

N° Redirección	URL Redirección
0	https://bit.ly/disponible_cupo
1	https://jeffiekaysanders.com/chile1.php
2	https://logim-bnnchochile.cl-gdd.buzz/
3	https://logim-bnnchochile.cl-gdd.buzz/1646656625/bcochile-web/persona/login/index.html/login

Comienza con un Bitly, sigue con un dominio que en la raíz tiene un script .php que finalmente redirige, ¡al mismo sitio que el caso anterior!

Tenemos 2 links distintos, que pasan por infraestructura distinta que llegan al mismo lado. Esto nos pareció sumamente extraño e interesante a la vez. Esto habla de infraestructura repartida para una misma campaña.

Otra cosa interesante también es la reutilización de estos links iniciales, porque el 08 de marzo[12] tenemos la reutilización de un link anterior:

N° Redirección	URL Redirección
0	https://bit.ly/aumento-marzo
1	https://bitly.com/a/warning?hash=3IF1vxE&url=https%3A%2F%2Fmelissagilfillian.com%2Fchile1.php
2	https://melissagilfillian.com/chile1.php
3	https://logn-bnnchochile.cl-fcc.buzz
4	https://logn-bnnchochile.cl-fcc.buzz/1646743806/bcochile-web/persona/login/index.html/login

Aunque el link de bit.ly sea marcado con warning por phishing, igual podemos detectar que el sitio intermedio (melissagilfillian[.]com en este caso) redirige a un sitio completamente nuevo del mismo estilo: con un nombre largo al inicio, con el dominio principal es un "cl-[algo]" con el TLD .buzz.

11 https://phishing.finsin.cl/list.php?query=3a41b4e7d2f16b4f11c4450912b0a5babf01c88c9005d0de0c6a6f3ed6fd15fd

12 https://phishing.finsin.cl/list.php?query=1d06bb3098009803c596c3fe037724298259f1c7c1f4eb06d18e523cdaf1f520

Otro de los patrones que tienen estas campañas es que todas están "protegidas" por Cloudflare, de hecho todos los dominios anteriores tienen resoluciones a IP de Cloudflare. Con esto los delincuentes generalmente pueden ganar 2 protecciones

- **geofencing**: la habilidad de restringir el paso solamente a las IP que correspondan a las víctimas, o sea, en este caso solo a IP de Chile.
- **antibot**: el poder restringir y bloquear a las revisiones automáticas de varios sitios, para que solamente caigan "víctimas reales" a los sitios de Phishing.

Como se "escudan" en Cloudflare, estamos un poco ciegos porque no podemos ver la IP y/o hosting que están realmente utilizando los ciberdelincuentes, y además tenemos que extremar las precauciones para que no seamos detectados como bots en la infraestructura de Cloudflare.

Acumulando datos

A través de los días, pudimos ir visualizando esta campaña un poco mejor, algunos días aparecían nuevos links bitly y otras veces podíamos usar los mismos.

Nos dimos cuenta que ya no era solamente 1 o 2 links, sino que todo un set, tanto de links originales, como de sitios intermedios, que todos apoyan a una misma campaña. En total hemos encontrado estos 11 links de Bitly.

Redirector bit.ly	Cantidad
https://bit.ly/portal_consumo	28
https://bit.ly/aumento_digital	12
https://bit.ly/Abril_Aumento	11
https://bit.ly/disponible_cupo	10
https://bit.ly/aumentos_cupo	9
https://bit.ly/Cupo_Disponible	6
https://bit.ly/Aumento_digitales	5
https://bit.ly/cuposs_marzo	4
https://bit.ly/aumento-marzo	2
https://bit.ly/portal-banchile	1
https://bit.ly/ActivaConsumo	1
Total	**89**

También podemos ver que de repente se repiten también los sitios intermedios que son parte de estas campañas, teniendo a veces 1 sitio intermedio o de repente 2 o 3. Y aunque no es una revisión exhaustiva, podemos ver que reutilizan ciertos dominios constantemente para redirigir el tráfico al nuevo sitio final del momento. Por ejemplo, tenemos la siguiente lista de "URL intermedias":

URL
https://acceszonet.com/
https://diarioedomex.com/banchile.php
https://heidikrieghauser.com/chile.php
https://heidikrieghauser.com/chile3.php
https://jeffiekaysanders.com/chile.php
https://jeffiekaysanders.com/chile1.php
https://jeffiekaysanders.com/chile3.php
https://jeffiekaysanders.com/chile4.php
https://maritau.com/
https://melissagilfillian.com/chile1.php
https://offcuerks.com
https://parasolbook.com/chile.php
https://parasolbook.com/chile2.php
https://teckling.com/
https://trululu.xyz
https://xcl-persona.nl/
https://xperosnas-cl.ml/

Si revisamos todos los casos que hemos ido viendo casi todos ellos son de campañas muy similares. Por ejemplo, en el sitio final del phishing casi siempre comienzan con un dominio largo, y luego el dominio principal que comienza con "cl-[algo]" y luego el TLD es .buzz. De hecho es tan común que dejo la tabla de todos los sitios finales que encontramos:

Subdominio	Main Domain	TLD
logrin-brancrochile.cl-bbub.buzz	cl-bbub.buzz	.buzz
logjn-barncochrile.cl-bclr.buzz	cl-bclr.buzz	.buzz
logjn-barncochrile.cl-brbr.buzz	cl-brbr.buzz	.buzz
logjn-bnncochrile.cl-bvu.buzz	cl-bvu.buzz	.buzz
logrn-barncochrile.cl-czlb.buzz	cl-czlb.buzz	.buzz
logih-brhancochile.cl-eang.buzz	cl-eang.buzz	.buzz
logjn-barncochrile.cl-ewq.buzz	cl-ewq.buzz	.buzz
logn-bnnchochile.cl-fcc.buzz	cl-fcc.buzz	.buzz
logrn-lbarncochile.cl-foxz.buzz	cl-foxz.buzz	.buzz
logrn-bnncochrile.cl-fvxr.buzz	cl-fvxr.buzz	.buzz
logim-bnnchochile.cl-gdd.buzz	cl-gdd.buzz	.buzz
logn-bnnchochile.cl-greh.buzz	cl-greh.buzz	.buzz
logjn-barncochrile.cl-gxvx.buzz	cl-gxvx.buzz	.buzz
logrin-brancochile.cl-hbm.buzz	cl-hbm.buzz	.buzz
logjn-barncochrile.cl-hbmr.buzz	cl-hbmr.buzz	.buzz
logrin-brancochrile.cl-hngn.buzz	cl-hngn.buzz	.buzz
logrin-brancochrile.cl-hvbs.buzz	cl-hvbs.buzz	.buzz
loqin-hancochile.cl-hyds.buzz	cl-hyds.buzz	.buzz
logn-bnnchochile.cl-ih.buzz	cl-ih.buzz	.buzz
logn-bnnchochile.cl-ijb.buzz	cl-ijb.buzz	.buzz
login-hancochile.cl-ilp.buzz	cl-ilp.buzz	.buzz
logrin-barncochrile.cl-ivx.xyz	cl-ivx.xyz	.xyz
logirn-barncochirle.cl-jjgh.buzz	cl-jjgh.buzz	.buzz
lggin-hnncochile.cl-lgnin.buzz	cl-lgnin.buzz	.buzz
logrn-brancochrle.cl-niad.buzz	cl-niad.buzz	.buzz
logirn-barncochrile.cl-nnrr.buzz	cl-nnrr.buzz	.buzz
logrn-bnncochrile.cl-nvmm.buzz	cl-nvmm.buzz	.buzz
logrn-brancochrile.cl-ocno.buzz	cl-ocno.buzz	.buzz
lgogin-hancochile.cl-oud.buzz	cl-oud.buzz	.buzz
logrin-barncochrile.cl-pwu.buzz	cl-pwu.buzz	.buzz
login-bancrochrile.cl-pxxq.buzz	cl-pxxq.buzz	.buzz
logrin-barncochirle.cl-qqpz.buzz	cl-qqpz.buzz	.buzz
logrn-brancochirle.cl-rbzr.buzz	cl-rbzr.buzz	.buzz
lohjn-hancochile.cl-rpi.buzz	cl-rpi.buzz	.buzz
logrn-barncochrile.cl-sddq.buzz	cl-sddq.buzz	.buzz
logrn-brancochrile.cl-sxxs.buzz	cl-sxxs.buzz	.buzz
logn-bnnchochile.cl-taa.buzz	cl-taa.buzz	.buzz
loqin-barncochrile.cl-tffa.buzz	cl-tffa.buzz	.buzz
logjn-barncochrile.cl-tfrd.buzz	cl-tfrd.buzz	.buzz
logrn-barncochrle.cl-trde.buzz	cl-trde.buzz	.buzz
loqin-brancochrile.cl-twxz.buzz	cl-twxz.buzz	.buzz
logrin-barncochrile.cl-ubnn.buzz	cl-ubnn.buzz	.buzz
logrin-barncochrile.cl-ubvc.buzz	cl-ubvc.buzz	.buzz
logn-bnnchochile.cl-ud.buzz	cl-ud.buzz	.buzz

logunbrancochrile.cl-undrt.buzz	cl-undrt.buzz	.buzz
logrnbrancochrile.cl-unts.buzz	cl-unts.buzz	.buzz
logrn-barnocrile.cl-utdb.buzz	cl-utdb.buzz	.buzz
logn-bnnchochile.cl-utq.buzz	cl-utq.buzz	.buzz
consumos.nl	consumos.nl	.nl
l0gin-brancoclhile.buzz	l0gin-brancoclhile.buzz	.buzz
l0gin-p0rtal-personasl-cl.cf	l0gin-p0rtal-personasl-cl.cf	.cf
login-benco-chrile.buzz	login-benco-chrile.buzz	.buzz
portal-bancochile.login-cl.cf	login-cl.cf	.cf
portalpersonas.lorgin-bancochile.tk	lorgin-bancochile.tk	.tk
personas.lorgin-bancorchile.gq	lorgin-bancorchile.gq	.gq
personas-bancochile.lorgin.cf	lorgin.cf	.cf
portal-bancochile-personas.lorgin.gq	lorgin.gq	.gq
offcuerks.com	offcuerks.com	.com
logins-personas-bancrcochile.perosnas-cl.cf	perosnas-cl.cf	.cf
personas-chile.cf	personas-chile.cf	.cf
portal-consumo-edwards-chile.cf	portal-consumo-edwards-chile.cf	.cf
portal-consumo-edwards-chile.tk	portal-consumo-edwards-chile.tk	.tk
portales-bancochile-web-mibancochile-cl.portaleslogin-cl.gq	portaleslogin-cl.gq	.gq
portales-personas-bancochirle-cl.portalogin.cf	portalogin.cf	.cf
banochiel-pernsonas-cl.protales-cl.cf	protales-cl.cf	.cf
portales-bancorchile-cl.xlogin.cf	xlogin.cf	.cf
logins-portales-bancorchile.xperosnas-cl.cf	xperosnas-cl.cf	.cf
xperosnas-cl.ml	xperosnas-cl.ml	.ml
bchile-portal.tk	bchile-portal.tk	.tk

Se puede apreciar que la cantidad de sitios generados es bastante grande, además de que aunque la gran mayoría cumplen con el patrón anterior, no todos lo cumplen. De hecho varios de los que no cumplen nos dan un poco más de indicios de su real infraestructura.

Si revisamos las IP que resuelven los dominios anteriores que no son de Cloudflare nos quedan solamente 2:

- 91.209.70.109
  - ASN: 43317
  - ISP: FNK LLC
  - País: Rusia
- 91.234.99.84
  - ASN: 213058
  - ISP: Private Internet Hosting LTD
  - País: Rusia

Lo cual nos llena de curiosidad, de hecho si resolvemos varios de los dominios (casi todos) apuntando directamente a alguna de esas IP, vamos a encontrar que sí son las IP que están detrás de estos sitios de Phishing.

Además, si vemos en el histórico de DNS (Passive DNS) de ambas IP[13][14], se ven que están dedicadas a generar este mismo tipo de Phishing a la misma institución chilena.

¿Qué hay que hacer al respecto?

Mucho monitoreo, tanto de infraestructura incial (redirecciones bit.ly) como de infraestructura intermedia (servidores con script.php) para poder dar de baja la cadena completa, no solo el sitio final (cl-[algo].buzz).

Comunicarse con todos en la cadena, principalmente bit.ly y Cloudflare, para que ante estos patrones puedan generar alertas o alguna revisión un poco más exhaustiva y que no se creen más de estos sitios/link/protecciones que solo ayudan a estos cibercriminales.

Contactar a los dueños (hostings) que usan esas IP, pero al ser rusos hay poca posibilidad de que hagan algo, por una estafa de tan poco valor para ellos.

13 Para IP 91.209.70.109: https://www.virustotal.com/gui/ip-address/91.209.70.109/relations
14 Para IP 91.234.99.84: https://www.virustotal.com/gui/ip-address/91.234.99.84/relations

Palabras finales

Al igual que en meses anteriores, primero quieremos agradecer a los que nos han apoyado en la plataforma, sin el apoyo de amigos y colegas varios no podríamos tener los datos que hoy en día tenemos y esto solo nos motiva a seguir avanzando en el descubrimiento de nuevos sitios y nuevas formas de defenderse de ellos.

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 Cloudflare o Bitly para identificar y denunciar este tipo de abusos, cosa de que no solo sea el takedown 1 vez, sino que una investigación más a profundidad en conjunto.

Podemos ver que hay ciertos tipos de phishing, que muy al contrario de lo que uno esperaría, no están a la baja sino que tienen un despliegue constante o a veces van al alza en cantidad de sitios generados. Esto nos impulsa a mejorar nuestrar redes de contactos para poder detectar más rápido estas nuevas estafas.

Con FINSIN estamos buscando llegar más allá y creemos que al entregar este tipo de información a la comunidad estamos aportando nuestro granito de arena para poder en algún futuro disminuir los ataques generales de phishing, haciéndolos cada vez más caros de realizar por las constantes denuncias de spam o abuso.

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