FINSIN

Reporte de Phishing

Mayo 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 tópicos para el mes de mayo[1]:

El 88% de los sitios detectados afectan a personas en Chile

Estamos detectando kits que afectan a 6 países Iberoamericanos

Con un máximo de 50 tarjetas por sitio y un valor aproximado de USD$10 cada una tenemos "asegurado" unos USD$500 por sitio levantado.

FC-01 y FC-02 tuvieron un máximo de 82 sitios detectados mensualmente

Tenemos un nuevo canal de Telgram para seguir los phishing detectados

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.

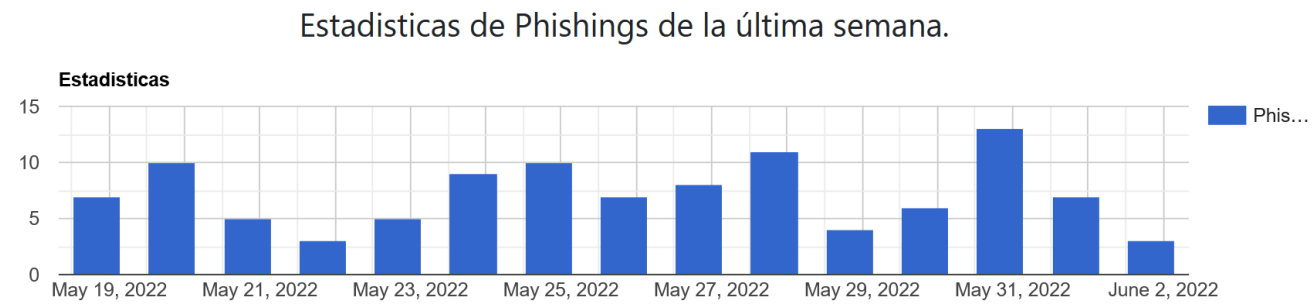
Phishing Checker

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/



¡Novedad!

Este mes queremos lanzar el canal de Telegram dedicado a las alertas de los sitios detectados por la plataforma.

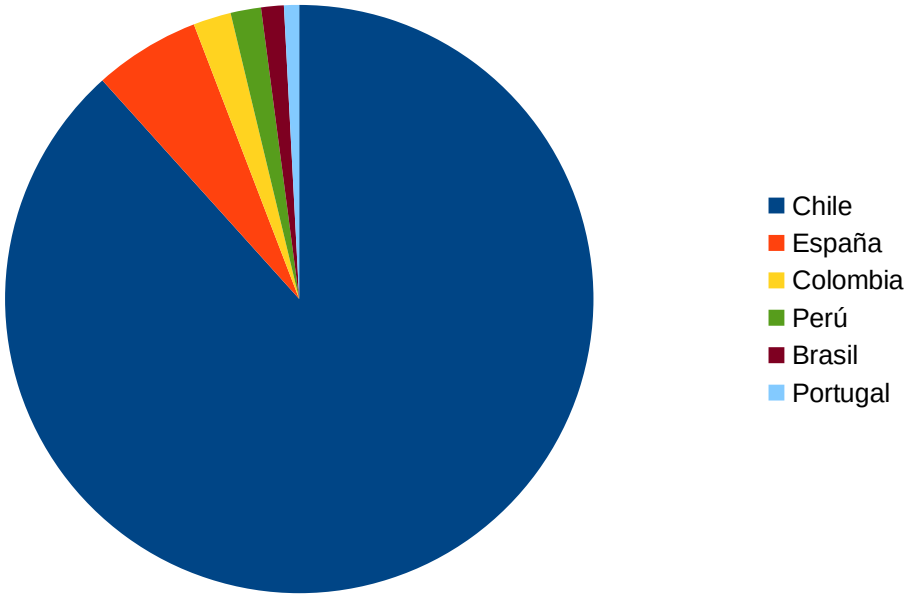
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Mayo 2022

En este ajetreado mes de mayo, logramos identificar 6 nuevas familias, 11 variantes de familias detectadas anteriormente y ajustamos los patrones de 5 familias antiguas de Phishing. Todo esto nos permitió ampliar mucho los kits que podemos detectar en este mes.

Datos de países[2]

En nuestra revisión mensual queremos detectar a qué institución intentan afectar estos phishings y a qué país están dirigidos, y si lo miramos desde ese punto de vista tenemos la siguiente distribución:



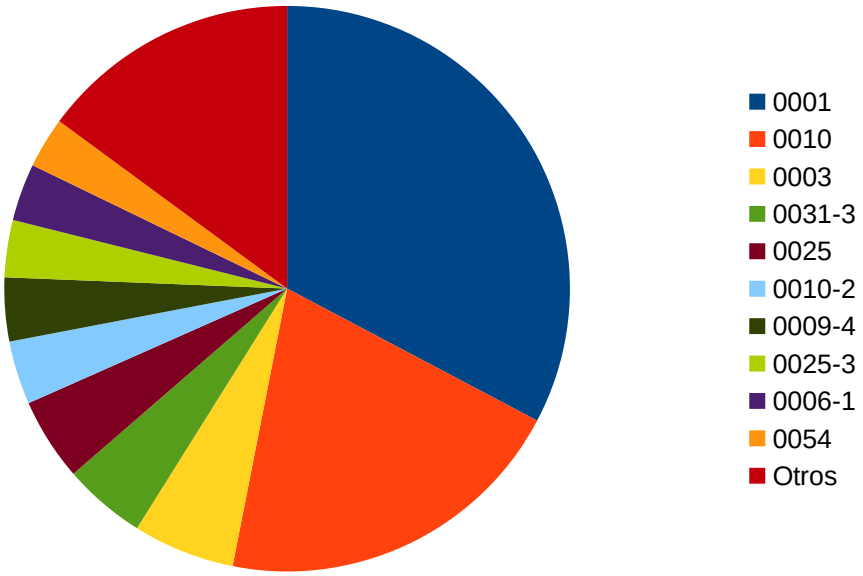
Pais	Porcentaje
Chile	88,33 %
España	5,84 %
Colombia	2,33 %
Perú	1,56 %
Brasil	1,17 %
Portugal	0,78 %

Ahora podemos detectar de más países iberoamericanos, incluyendo a una institución de Portugal y una de Brasil dentro de nuestro patrones. Esperamos apoyarlos con nuestra plataforma.

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

Como veíamos anteriormente, tenemos muchos kits nuevos, variantes nuevas y arreglos a los patrones anteriores, con lo que tenemos muchas novedades. Si graficamos ahora la distribución de los datos de los kits, tenemos lo siguiente:



Aquí se ve que, al igual que los meses anteriores, predomina claramente el pack 0001, pero en mayo empieza un cambio porque el pack 0010 tiene el segundo lugar con un alto porcentaje.

Pack	Porcentaje
0001	32,73 %
0010	20,36 %
0003	5,82 %
0031-3	4,73 %
0025	4,73 %
0010-2	3,64 %
0009-4	3,64 %
0025-3	3,27 %
0006-1	3,27 %
0054	2,91 %
Otros	14,91 %

Tanto el pack 0010 como su segunda variante 0010-2, son packs asociados a una campaña dirigida a una institución bancaria en Chile que queremos presentar (si se mantienen relevantes) en el siguiente informe de Junio.

Caso de filtración de información

Este mes de Mayo volvemos a hablar sobre el robo de información que realiza el kit de Phishing que clona la marca de una institución Española.

Recordemos que 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 conecta y entrega información potencialmente verdadera.

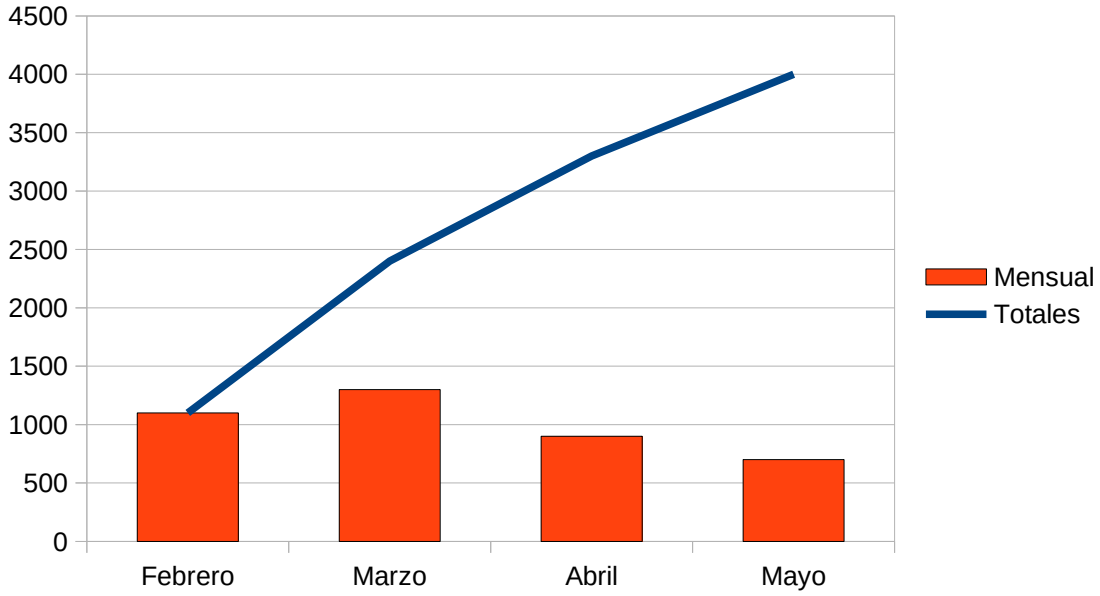
A través de los meses hemos podido detectar varias instancias de estos kit, pero el mes de mayo han bajado las detecciones. Tenemos los siguientes datos:

Tenemos una baja de más de la mitad de sitios que hemos detectado

Tenemos una baja de más de la mitad, con relación al mes de abril, en cantidad de sitios que hemos detectado.

Como lo hemos visto en los meses anteriores podemos conseguir los datos de tarjetas robados por este kit descargando un archivo desde el mismo sitio, que almacena los datos puestos por sus víctimas.

Como en mayo hubo una baja en sitios detectados esto también se traduce directamente en la cantidad de tarjetas que hemos logrado detectar. En estos 4 meses que hemos ido monitoreando tenemos al rededor de 4000 tarjetas, y podemos ver que la curva ha ido en disminución



Un último dato interesante que sale al revisar estos meses de phishing, es que dentro del "retorno a la inversión" que un delincuente puede tener con estos sitios, las potenciales utilidades son buenas. Teniendo en cuenta un número "promedio" de tarjetas por sitio en los últimos meses tenemos que:

Mes	0,00
Febrero	50,00
Marzo	50,00
Abril	25,71
Mayo	46,67

Con un máximo de 50 tarjetas por sitio y un valor aproximado de USD$10[3] cada una tenemos "asegurado" unos USD$500 por sitio levantado. No es malo para "solo un ataque de phishing".

3 Según investigación de NordVPN https://nordvpn.com/es/research-lab/payment-card-details-theft/

Como habíamos dicho el mes anterior, en el caso de esta campaña se ha generado bastante ruido en el lado de la concientización de las personas. Se han generado múltiples campañas para avisar que existe este tipo de engaño existe y que la gente en España tenga cuidado.

También existen múltipes esfuerzos para parar este tipo de ataques. A fines de abril, los Mossos d'Esquadra lograron tomar detenidos[4] a unos jóvenes de 19 y 20 años que realizaban este tipo de ataques de "phishing" y "smishing". Además de otros esfuerzos realizados por la polítcía en España[5][6], a fines de este mes también se juntaron muchas policías a través de la Europol para botar una de las mayores botnets de teléfonos móviles "Flubot"[7].

Con todo esto se espera que los grupos delictivos dedicados a este tipo de estafa bajen un poco su actividad, y ojalá que este tipo de engaño por SMS vaya en disminución, pero al parecer es muy lucrativo para dejarlo de lado.

4 https://www.metropoliabierta.com/informacion-municipal/sucesos/detenidos-dos-jovenes-por-estafas-con-mensajes-moviles-tarjetas-bancarias_53990_102.html
5 https://www.lasprovincias.es/sucesos/detenidos-estafas-metodo-smishing-sms-fraudulentos-20220515102137-nt.html
6 https://www.genbeta.com/actualidad/policia-nacional-descubre-grupo-que-phishing-imitaba-a-banco-espana-para-robar-mucho-dinero-asi
7 https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

Los grupos FC-01 y FC-02

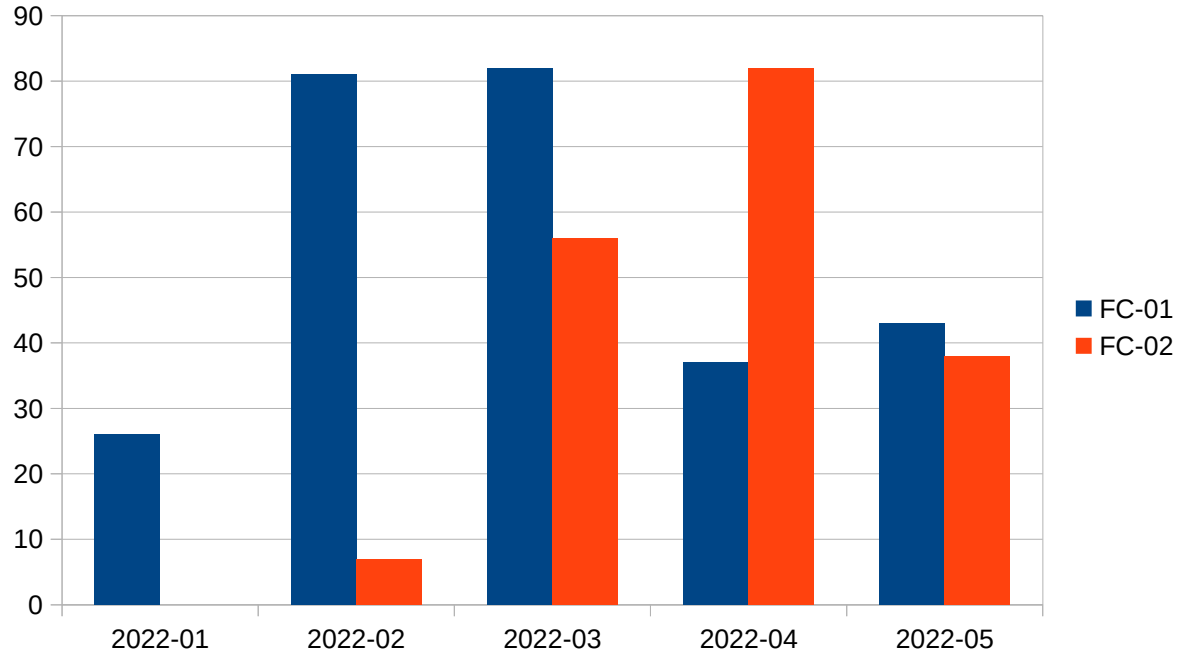
En este reporte queremos volver a revisar a los grupos que nosotros como FINSIN hemos llamado "Fishers Constantes 01" y "Fishers Constantes 02" (FC-01 y FC-02 en adelante).

Estos son grupos que se especializan en enviar campañas de Phishing para empresas e instituciones en Chile. El comportamiento de estos grupos los describimos en boletines anteriores (para FC-01 el boletín de febrero[8] y para FC-02 el boletín de abril[9])

Queremos revisitar un poco estos grupos para observar un poco cuanto es el impacto que han tenido y si es que siguen siendo relevantes el día de hoy. Para ello revisamos los comportamientos históricos de esta banda y hemos encontrado sitios antiguos que a primera instancia no parecían parte, pero con un nuevo análisis si.

Ambos grupos tuvieron un máximo de 82 sitios detectados mensualmente

Los totales en estos 4 meses son los siguientes:



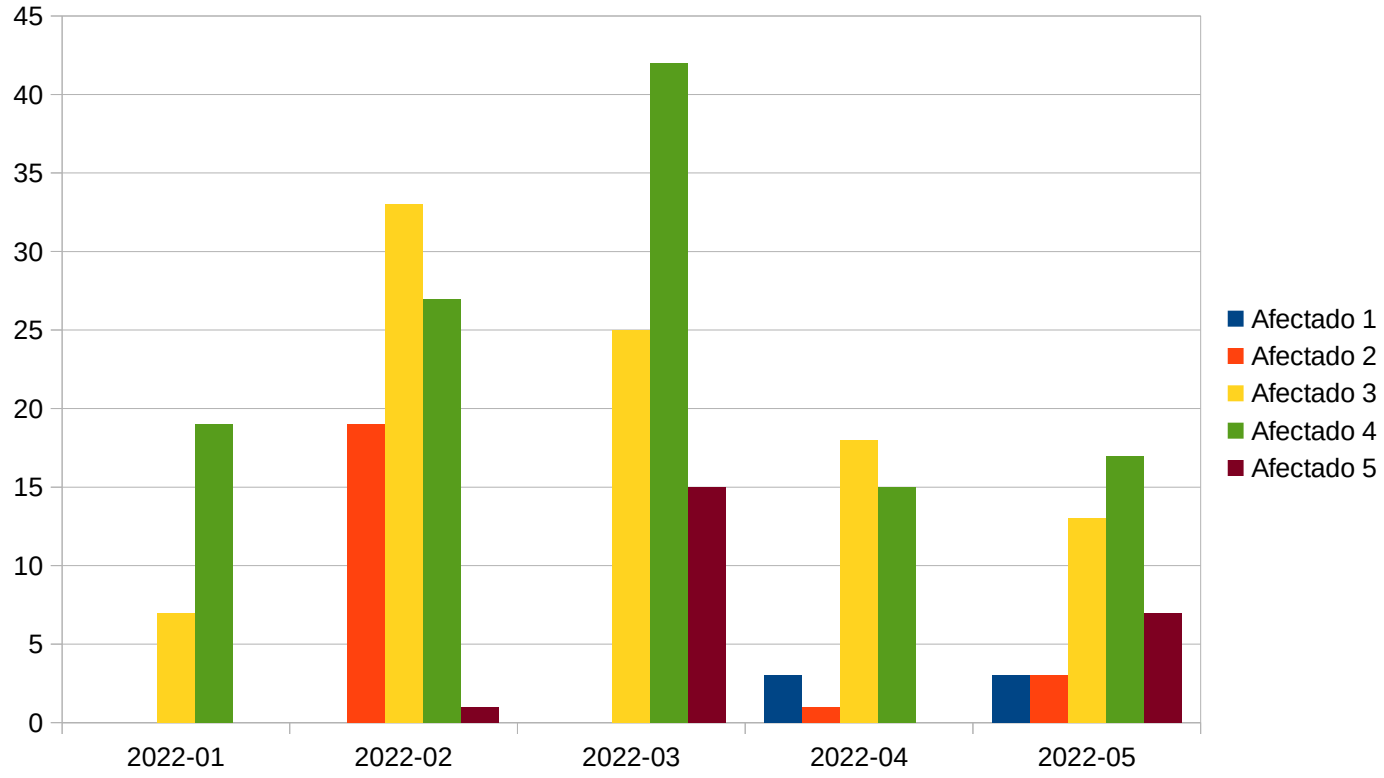
Podemos observar que ambos grupos han sido bastante eficientes en la cantidad de sitios por mes que pueden sacar, ambos grupos tuvieron un máximo de 82 sitios detectados mensualmente.

8 https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/
9 https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/

Lo que sí es interesante, es que lo que ambos grupos han ido bajando mucho su actividad, llegando en mayo a casi la mitad de su máximo. Si nos metemos un poco dentro de cada uno de los grupos podemos ver que hay otros comportamientos interesantes.

Analizando el mes para FC-01

Es un grupo que se dedica a atacar a múltiples entidades de Chile, hasta el momento ha atacado a 5 empresas distintas con la siguiente distribución mensual[10]:



Mes	Afectado 1	Afectado 2	Afectado 3	Afectado 4	Afectado 5	Total mes
2022-01			7	19		**26**
2022-02		19	33	27	1	**80**
2022-03			25	42	15	**82**
2022-04	3	1	18	15		**37**
2022-05	3	3	13	17	7	**43**
Total	**6**	**23**	**96**	**120**	**23**	**268**

10 Los afectados de FC-01 no corresponden a los mismos afectados de FC-02. Para anonimizar a las empresas afectadas las llamamos “Afectado X”, pero solo con el efecto de ejemplificar comportamiento. El “Afectado 1” de FC-01 no es el mismo que el “Afectado 1” de FC-02

Tenemos que el principal afectado es el “Afectado 4” con una presencia importante en todos los meses que hemos revisado. El “Afectado 3” no se queda tan atrás dentro de los totales, y aunque es son un poco más de 20 sitios menos en total, sigue siendo un número alto comparadocon los demás.

Lo interesante de revisar un poco más los datos en detalle tenemos que ha ido mutando un poco la aparición de los afectados. Las campañas han sido cada vez menos masivas, y los sitios encontrados son cada vez más de “prueba” que con clientes afectados reales.

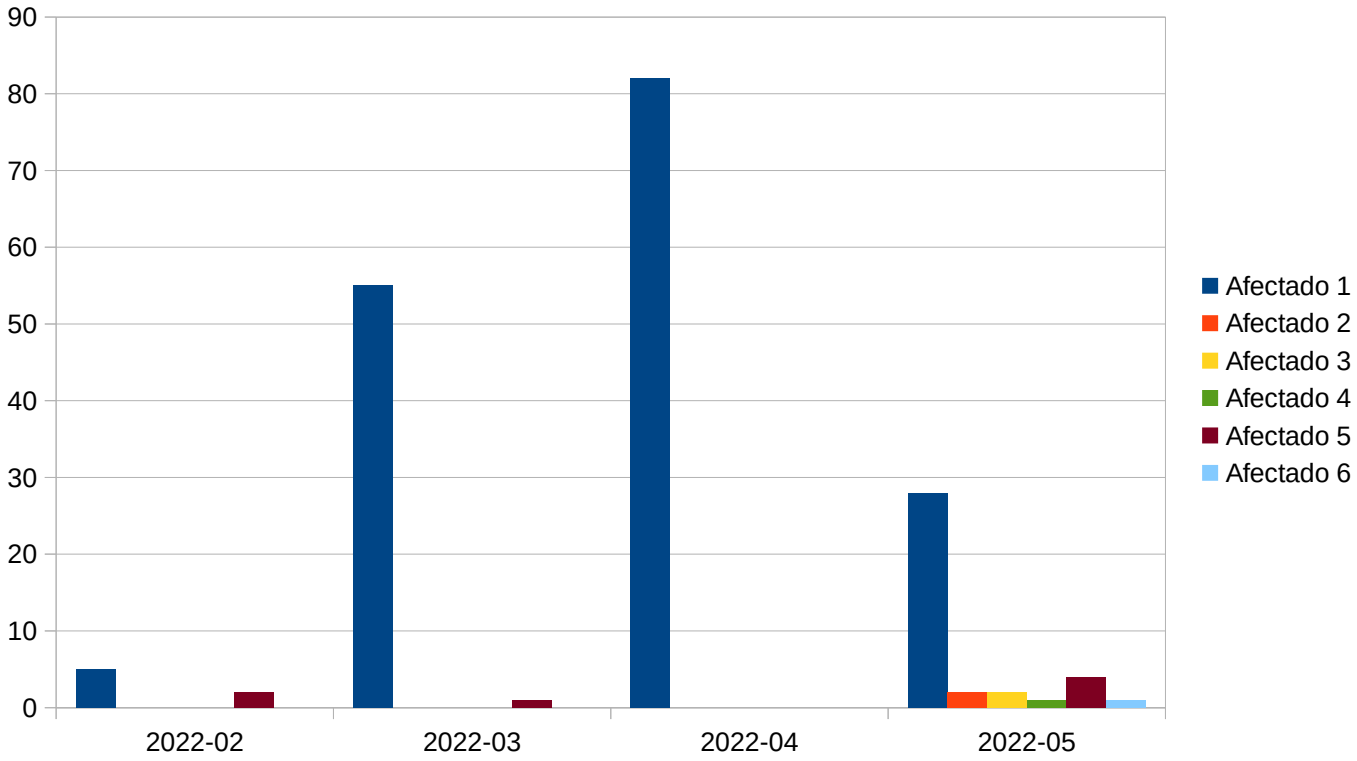
Por ejemplo, el “Afectado 3” tiene 13 sitios levantados en mayo, pero esos son solamente en los primeros 9 días del mes, luego de eso no se le han levantado más campañas.

Los 17 del “Afectado 4” era en general porque se mantenía parte de la infraestructura de pivote, pero gracias al equipo de takedown, se pudo dar de baja tanto los sitios finales como el sitio intermedio de redirección. Luego de ello, solo se han visto sitios sueltos que no representan el mismo poder de generación de dominios que se veía en los primeros meses.

En general estimamos que por la disminución de la capacidad de generación de dominios y la rapidez en el takedown de estos sitios cada vez está siendo más “caro” para FC-01 atacar a las empresas acá en Chile. Deberíamos ver una disminución en general de este tipo de sitios, o un cambio en el tipo de kits en las semanas y meses que vienen.

Analizando el mes para FC-02

Este grupo es un poco menos general en las empresas que abarca. Como vimos en el reporte del mes de abril, en general se dedica a una sola empresa, aunque en el mes de mayo hemos visto que se ha diversificado un poco. Tenemos la siguiente distribución[11]:



Con esto vemos que en los primeros meses casi no exisía un segundo afectado, con muy pocas detecciones por mes, pero luego en mayo aparecieron muchas más empresas asociadas.

Esto se debe principalmente al análisis de las IP que pudimos encontrar detrás de la infraestructura de este grupo. Si revisamos nuestro reporte del mes de abril, teníamos 2 IPs rusas que estaban siendo usadas como hosting para almacenar estos sitios, ahora tenemos 4 asociadas a este grupo, porque en el mes de mayo comenzaron a compartir infraestructura con los redirectores de campañas anteriores.

11 Los afectados de FC-02 no corresponden a los mismos afectados de FC-01. Para anonimizar a las empresas afectadas las llamamos “Afectado X”, pero solo con el efecto de ejemplificar comportamiento. El “Afectado 1” de FC-01 no es el mismo que el “Afectado 1” de FC-02

Como vimos en el caso anterior, las IPs usadas por este grupo son de los mismos segmentos, asumimos que se las da el mismo hosting que tienen contratado. En este caso son las siguientes:

- 91.209.70.109:
  - ASN: 43317
  - ISP: FNK LLC
  - País: Rusia
- 91.209.70.166
  - ASN: 43317
  - ISP: FNK LLC
  - País: Rusia
- 91.234.99.84
  - ASN: 213058
  - ISP: Private Internet Hosting LTD
  - País: Rusia
- 91.234.99.198
  - ASN: 213058
  - ISP: Private Internet Hosting LTD
  - País: Rusia

Lo extraño es que al revisar en el historial de los sitios de mayo, hubo un cambio a mediados de mes, días después de que hayamos lanzado el reporte de abril comenzaron a caer varios de los sitios de redirección intermedia que hablábamos en el reporte anterior[12].

Al rededor del 12 de mayo las campañas que circulaban con los links de bit.ly ya no les funcionaba, y además dejaron de usar Cloudflare como herramienta de protección de sus sitios. Con esto tuvieron que comenzar a levantar dominios directamente en la IP del hosting, lo cual hace mucho más fácil seguir (¡Gracias Virustotal[13]!).

Lo único que queda del patrón de comportamiento anterior es una URL de bit.ly que afecta a otra institución (no es para el "Afectado 1").

La campaña que tenemos en mira es la siguiente:

N° Redirección	URL Redirección
0	https://bit.ly/Bestado
1	https://acceszonet.com/estado.php
2	https://brancoestado-cl.nbjjjh.cf/
3	https://brancoestado-cl.nbjjjh.cf/1654293526/i

12 Es totalmente coincidencia, pero me gustaría pensar que fue por la información que sacamos en el reporte.
13 https://www.virustotal.com/gui/ip-address/91.234.99.198/relations

Como vimos antes, es el mismo patrón anterior, parte con un link de bit.ly, luego viene un dominio con un script .php al final y termina en el dominio con el nombre largo, solo que en este caso no necesariamente termina en .buzz como antes.

Lo que sí podemos encontrar, buscando este dominio intermedio en la plataforma, es que ha sido usado solo para múltiples campañas, por ejemplo en las siguientes:

Phishing (Reporte)	Query: https://bit.ly/Bestado Final: https://bamco-estad0.cl-ssdt.xyz/1653926884/imagen...
Phishing (Reporte)	Query: https://bit.ly/Bestado Final: https://bamco-estado.cl-jccv.buzz/1653686643/image...
Phishing (Reporte)	Query: http://djdjjr.gq Final: https://logrin-bancorchile-personas.djdjjr.gq/banc...
Phishing (Reporte)	Query: https://bit.ly/Abril_Aumento Final: https://logins-portales-bancorchile.xperosnas-cl.c...
Phishing (Reporte)	Query: https://bit.ly/aumentos_cupo Final: https://l0gin-brancoclhile.buzz/1651679646/bchile-...

Con esto podemos hacer el link entre ambos grupos y la infraestructura que están usando. Porque separan las campañas, para un afectado usan un script .php y para el otro ocupan un segundo script o directamente el index.php de la raíz.

Podemos asumir con alta confianza que estas campañas son del mismo grupo, y que últimamente se les ha complicado mucho la monetización de los sitios de phishing para el “Afectado 1” con lo que tienen que comenzar a diversificar y atacar a otras instituciones.

¿Seguirán activos estos grupos?

La tendencia del comportamiento de estos grupos indica que ambos van en disminución, tanto FC-01 como FC-02 están bajando su nivel de actividad y en el caso de FC-02 está siendo cada vez menos cuidadoso con su infraestructura, pudiendo así ser detectado fácilmente.

Creemos que el costo por sitio ha ido subiendo mucho para estos grupos, por lo que se espera que baje la cantidad de phishing producido por ellos en las siguientes semanas y/o meses.

Palabras finales

Primero queremos 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.

Pudimos ver que cuando un actor delictual quiere levantar un sitio, puede tener un ingreso de hasta USD$500 por sitio, con eso podemos entender el porqué se levantan tantos sitios al mes y lo incansables que pueden llegar a ser, generando hasta 82 un solo grupo.

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.

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.

Reportes anteriores

- Reporte Enero-Febrero 2022
  - https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/
- Reporte Marzo
  - https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/
- Reporte Abril
  - https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/