FINSIN

Reporte de Phishing
Abril y Mayo 2023

Índice

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 es un ataque muy barato, porque los ciberdelincuentes pueden generar muchos sitios de estafas diariamente, y al hacer que las personas visiten el sitio pueden engañarlas y robarles sus claves u otro tipo de información.

Analizando algunos de estos sitios encontramos que tienen 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.

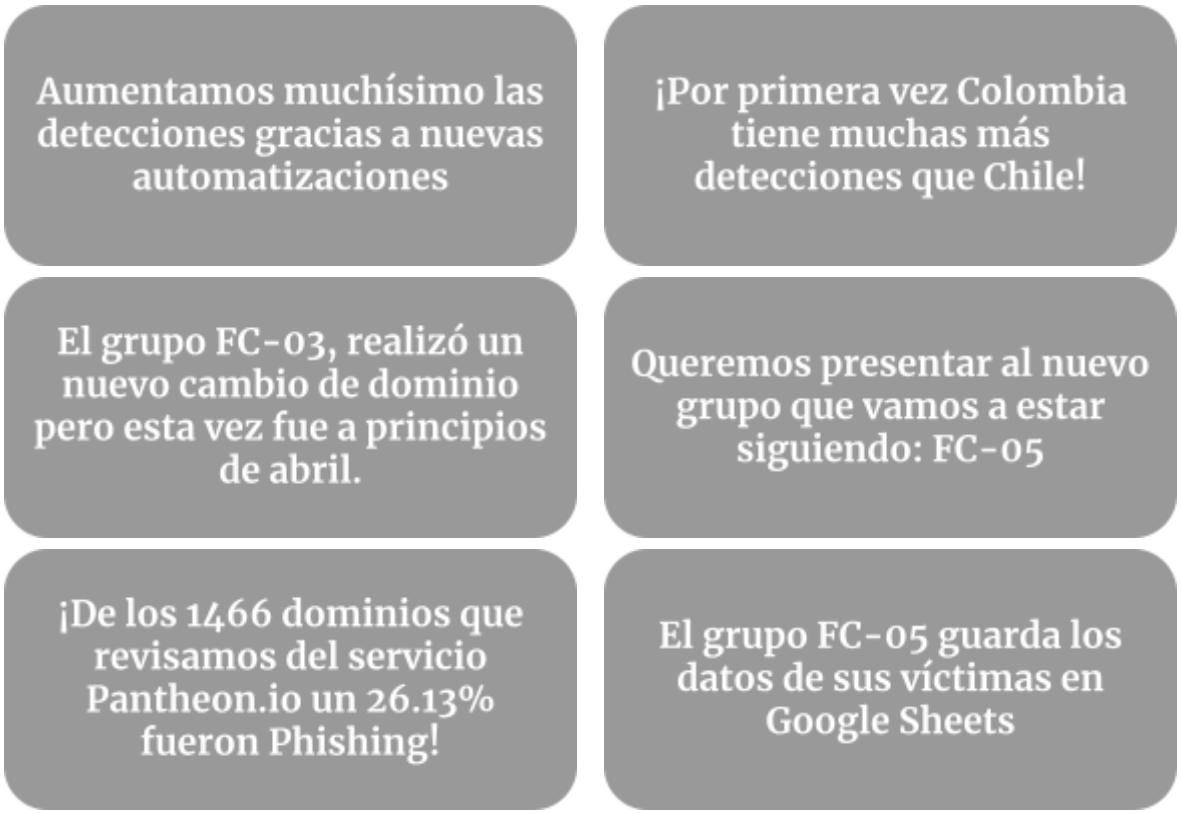
Para ello, decidimos generar un sistema automático con la capacidad de detectar, clasificar y agrupar los sitios de phishing que aparecen, logrando identificar patrones que nos permitan definir si un sitio es o no un Phishing y además a qué tipo de kit está asociado.

Con lo anterior, a principios de Febrero del 2022 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.

Ricardo Monreal Llop
Presidente FINSIN

TL;DR

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



Esperamos que con estos datos sigan leyendo el documento.

[1] Cuando se habla de sitios (o kits) detectados implica que fueron detectados por la plataforma, no corresponde al total real de Chile ni del país nombrado

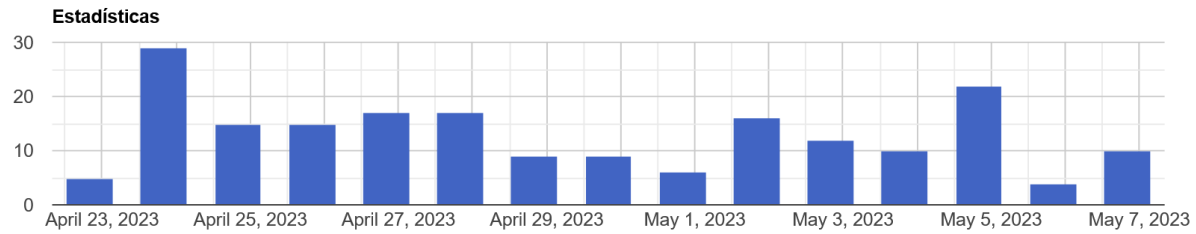
Phishing Checker

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, donde basta con tener una URL para 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.

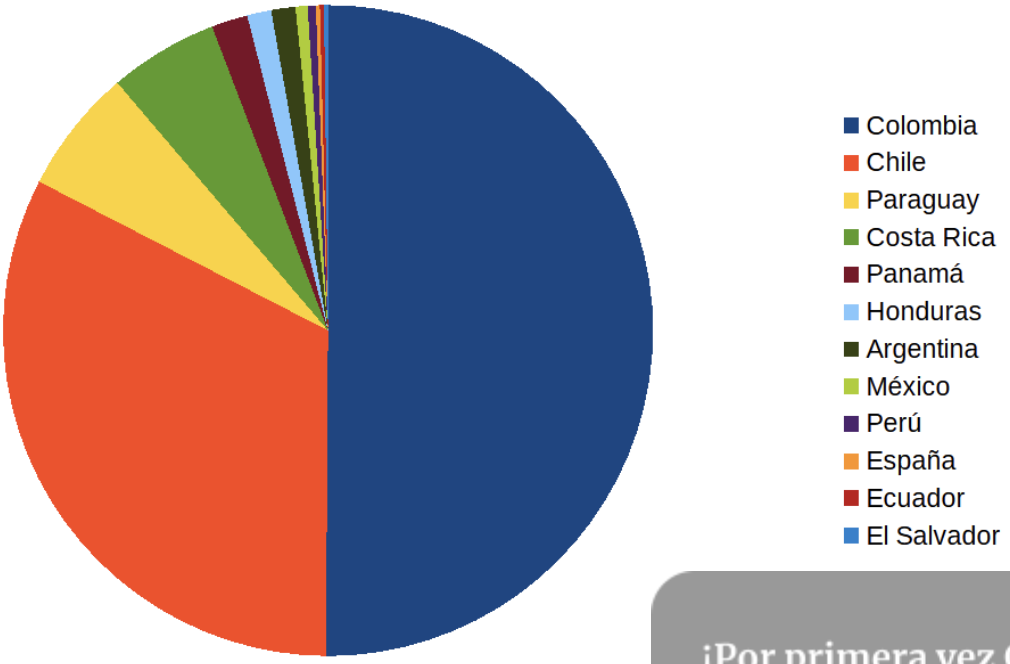
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Abril 2023

Como hemos visto en los meses anteriores, queremos dividir el análisis en países y en packs. La idea es agrupar el top de packs detectados y en vez de revisar las instituciones afectadas, queremos analizar los países a los que pertenecen esas instituciones y así ver a qué público están dirigidos.

Datos de países

Si miramos los países de las marcas afectadas tenemos un gran cambio en las detecciones:



¡Por primera vez Colombia tiene muchas más detecciones que Chile!

País	Porcentaje
Colombia	50,10 %
Chile	32,46 %
Paraguay	6,21 %
Costa Rica	5,41 %
Panamá	1,80 %
Honduras	1,20 %
Argentina	1,20 %
México	0,60 %
Perú	0,40 %
España	0,20 %
Ecuador	0,20 %
El Salvador	0,20 %

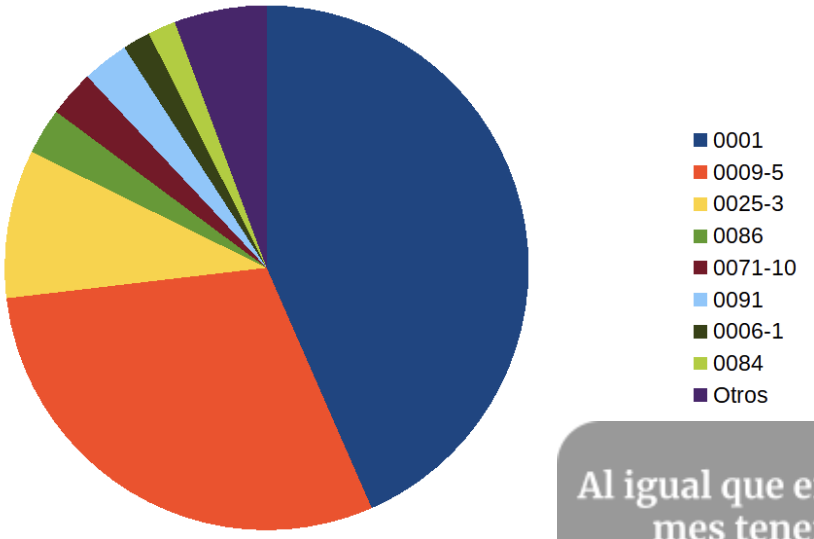
¡Por primera vez Colombia tiene muchas más detecciones que Chile!

Este mes aumentamos mucho las revisiones de Phishing gracias a que comenzamos a realizar detecciones automáticas relacionadas con Colombia. Vamos a ampliar este punto más adelante.

En Chile, hemos detectado este mes algunos de los que "se repiten siempre", pero no hemos podido detectar campañas nuevas que estén afectando a los clientes nacionales, estamos cada vez más seguros que los Phishing en Chile están en retirada.

Datos de kits

Si graficamos los datos del mes asociados a los kits de phishing, podemos ver que con los cambios de automatización, también cambian los pack más detectados:



Al igual que en los países, este mes tenemos un gran cambio, ¡el pack 0001 sale del primer lugar!

Pack	Porcentaje
0071-3	26,82 %
0001	13,21 %
0086	10,26 %
0009-5	8,68 %
0070-12	4,93 %
0091	4,93 %
0096	4,34 %
0010-5	3,16 %
Otros	23,67 %

Este mes podemos ver que la distribución de las detecciones está siendo mucho más homogénea que el mes anterior.

Seguimos con muchas detecciones del pack 0001, 0010-2, 0025-3 y 0009-5, pero, además, tenemos una gran lista de otros con más del 20% de las detecciones del mes.

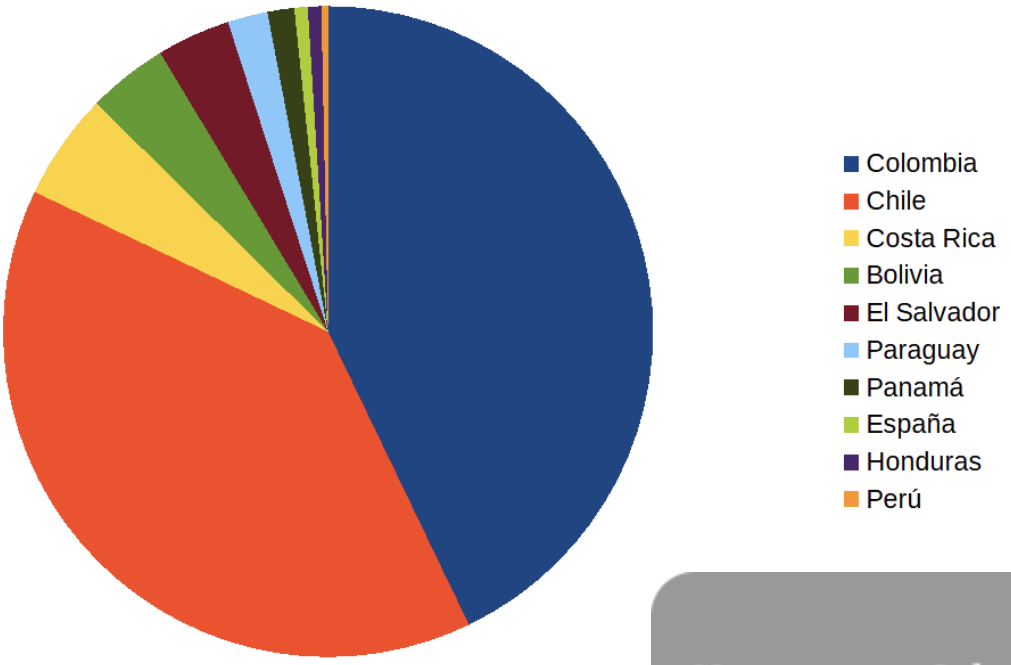
Al igual que en los países, este mes tenemos un gran cambio, ¡el pack 0001 sale del primer lugar!

Mayo 2023

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

Si miramos los países de las marcas afectadas tenemos un gran cambio en las detecciones:



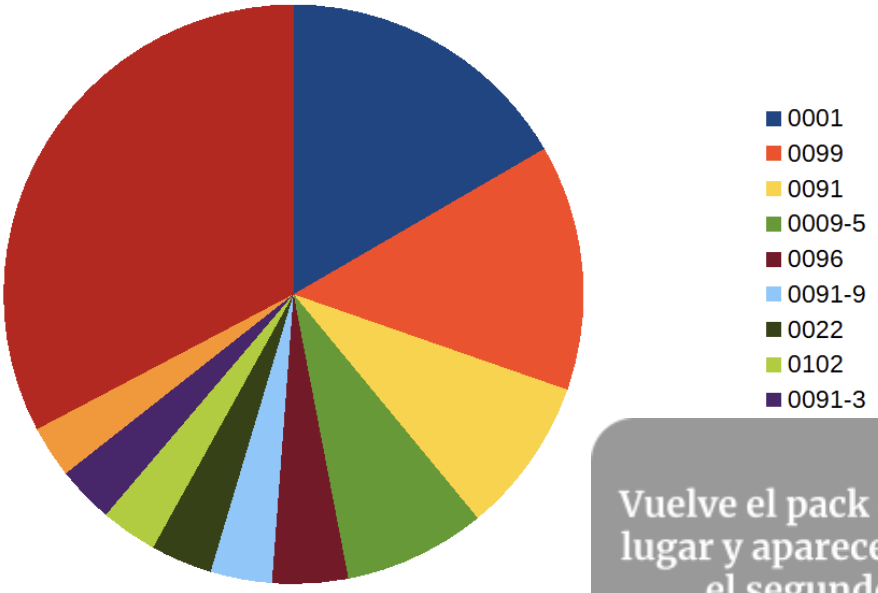
País	Porcentaje
Colombia	42,86 %
Chile	39,20 %
Costa Rica	5,32 %
Bolivia	3,99 %
El Salvador	3,65 %
Paraguay	1,99 %
Panamá	1,33 %
España	0,66 %
Honduras	0,66 %
Perú	0,33 %

¡Nuevamente Colombia tiene más detecciones que Chile!

¡Nuevamente Colombia tiene más detecciones que Chile!

Datos de kits

Si graficamos los datos del mes asociados a los kits de phishing, podemos ver que con los cambios de automatización, también cambian los pack más detectados:



Vuelve el pack 0001 al primer lugar y aparece uno nuevo en el segundo, el 0099

Pack	Porcentaje
0001	16,62 %
0099	13,72 %
0091	8,71 %
0009-5	7,92 %
0096	4,22 %
0091-9	3,43 %
0022	3,43 %
0102	3,17 %
0091-3	3,17 %
0070-17	2,90 %
Otros	32,72 %

Vuelve el pack 0001 al primer lugar y aparece uno nuevo (que veremos un poco más adelante) en el segundo, el 0099 . Este mes podemos ver que comienza a aumentar las detecciones de packs nuevos (0099, 0091, 0096, etc.).

Esto habla de dos cambios: un cambio de los packs usados por los delincuentes y una mejor detección de nuestra parte de ellos porque son packs que no conocíamos antes.

Aumento de detecciones

Estos meses hemos logrado aumentar significativamente las detecciones de la plataforma porque comenzamos a monitorear uno de los dominios de SaaS que habíamos hablado en el pasado: **Pantheon.io**.

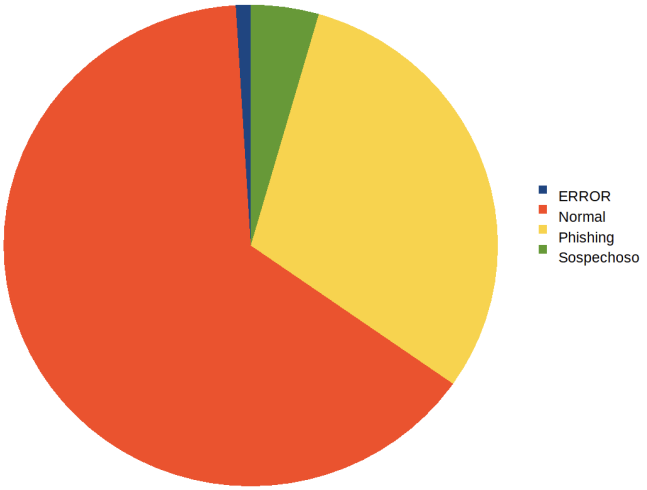
Este servicio tiene 4 IPs en donde publica los dominios asociados a su servicio de SaaS, estas IPs las habíamos nombrado en el pasado, pero son: 23.185.0.1, 23.185.0.2, 23.185.0.3 y 23.185.0.4.

Comenzamos a revisar automáticamente los dominios que van saliendo desde ese servicio, buscando los dominios que aparecen en esas IP. Una salvedad, de los dominios que se suben a esas IP solamente revisamos los dominios que son con el siguiente formato[2]:

dev-[nombre definido].pantheonsite.io

En estos 2 meses (abril y mayo) en total logramos 1466 dominios y encontramos resultados muy interesantes:

Resultado Scan	Porcentaje de Detección
Phishing	26.13%
Sospechoso	3.41%
Normal	69.71%
ERROR	0.75%



Tenemos un 26.13% de sitios catalogados como Phishing por nuestra plataforma. Los catalogados como "Sospechosos" en general son porque en el momento no teníamos la información completa para declararlos como "Phishing".

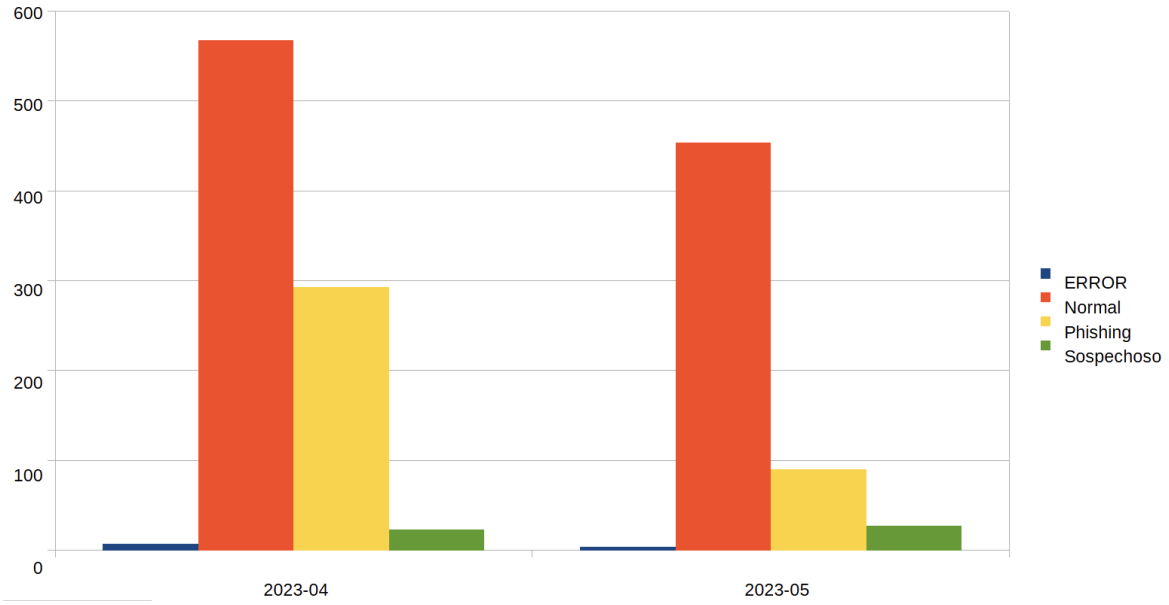
¡De los 1466 dominios que revisamos de Pantheon.io un 26.13% fueron Phishing!

[2] Tenemos pendiente empezar a monitorear los otros dominios de la documentación (https://docs.pantheon.io/guides/domains/platform-domains)

Si hacemos una simplificación, y decimos que los sospechosos son todos phishing y los ERROR son todos no-Phishing, tenemos que **¡3 de cada 10 sitios que se suben a la plataforma son Phishing!**

> ¡3 de cada 10 sitios que se suben a la plataforma son Phishing!

Al hacer una revisión por mes, tenemos algo muy interesante:



Resultado Scan	% Abril	% Mayo
Phishing	32,88 %	15,65 %
Sospechoso	2,58 %	4,70 %
Normal	63,75 %	78,96 %
ERROR	0,79 %	0,70 %

Tenemos que abril fue un mes excesivamente alto en números de phishing subidos en la plataforma. **¡1 de cada 3 sitios era Phishing!**

Son números muy altos, que creemos que fueron detectados por los administradores de la plataforma, ya que en mayo estos sitios de estafa se redujeron a la mitad.

Aclaración

Cabe destacar que los dominios de Phishing que suben en **Pantheon.io** son dados de baja muy rápidamente, lo cual habla muy bien de los sistemas de respuesta que tienen implementados.

No basta solo con medir “cuántos” sitios se generan, sino que un dato importante (que por ahora no tenemos) es cuántas víctimas caen en esos sitios, y para reducir esto el tiempo de vida de los sitios tiene que ser el menos posible.

No tenemos exactamente el promedio de tiempo en que estos sitios están arriba pero tenemos tiempos desde 15 minutos arriba hasta máximo 48 horas, cuando son de instituciones menos conocidas o cuando los nombres de los dominios no son “tan evidentes”.

La respuesta rápida a este tipo de estafas debe ser parte de la responsabilidad de cada uno de los hosting, SaaS o cualquier servicio que pueda ser abusado por ciberdelincuentes. Sabemos que no son responsables de la estafa, pero da gusto cuando se toman en serio la baja de los sitios de estafa como en este caso.

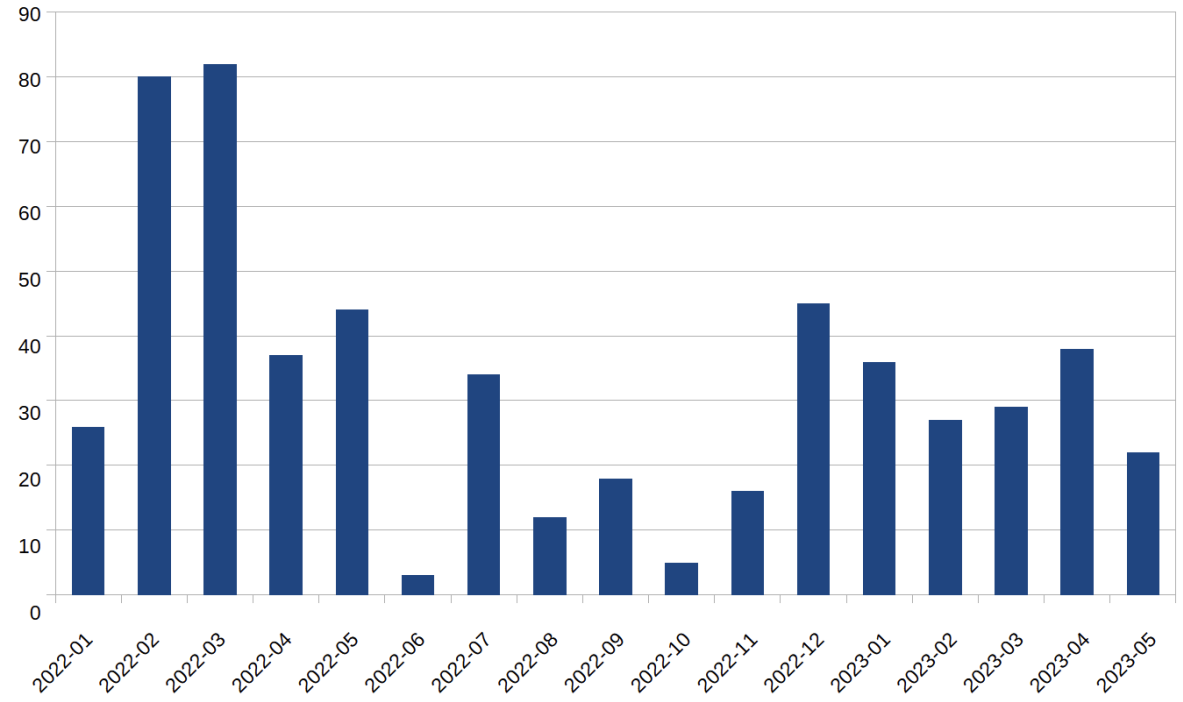
Actualización de Fishers Constantes (FC)

Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos que nosotros llamamos "Fishers Constantes" (o FC), que aunque tienen nombres parecidos tienen características muy distintas.

FC-01

Como hemos visto anteriormente[3], FC-01 tiene una actividad muy característica, usa varias capas y varias redirecciones para montar su infraestructura. Su "modus-operandi" no ha cambiado mucho, pero tampoco hemos podido asignarle más datos al comportamiento que hemos observado de ellos.

El comportamiento de este grupo a través de los meses ha sido un poco errático, como lo vemos en el siguiente gráfico:



Como vemos, estos últimos meses han estado un poco estancados levantando alrededor de 30 sitios "solamente" por mes este 2023, con 38 en abril y 22 en mayo.

[3] Este grupo fue definido en el reporte de febrero del 2022: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/

En estos meses pudimos seguir a este grupo por los patrones de los dominios, pero además por los dominios intermedios que usan, en este caso fueron los siguientes:

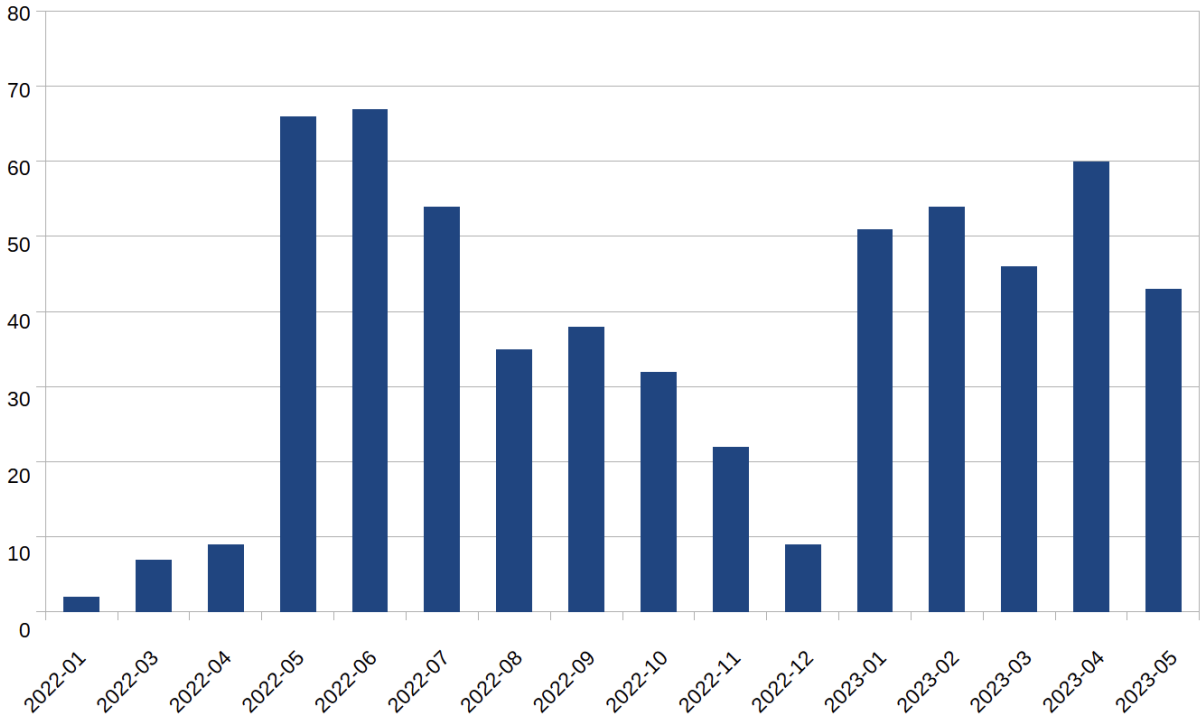
- https://sam-tech.jp/
- http://wordpress.zuliatec.com.ve/
- https://concierge.casasre.com/
- https://eilders.nl//

Al mantener un monitoreo constante sobre estos dominios, revisando la configuración del pack de redirección que tienen encima, podemos ir detectando cada cambio que los controladores realizan.

Al igual que en meses anteriores, se recomienda que dentro de la cadena de "takedown" de los sitios, no solo den de baja el inicio o el fin, sino que los puntos intermedios también.

FC-03

Como ya vimos en un reporte anterior[4], este grupo está usando 2 packs: el 0009 y el 0010 (con sus respectivas variantes), si vemos sus acciones este mes, podemos ver que las detecciones de este grupo están siendo muy parejas.



En estos últimos meses se están "estancando", y según lo que hemos podido detectar es por el comportamiento errático de las detecciones.

El pack 0009, solo mantiene 1 variante activa, la 0009-5. Si investigamos los centros de comando y control (C2) que usaron durante el mes, tenemos los siguientes:

Día inicio	C2
2023-04-01	https://edohello.info
2023-04-04	https://r4gn4r0kr4.dinamics.info
2023-04-13	https://r4gn4r0kr4.pescanet.info
2023-06-06	https://current-estado.info

[4] Reporte en el siguiente link:
https://finsin.cl/2023/01/13/reporte-mensual-de-phishing-diciembre-2022/

Como habíamos visto en el reporte anterior, se hizo un cambio de dominio de C2 durante los primeros días de abril a “r4gn4r0kr4.dinamics.info”, pero luego a mediados de mes hubo otro cambio a “r4gn4r0kr4.pescanet.info”, el cual se mantuvo todo el resto de abril y todo mayo.

El grupo FC-03 realizó dos nuevos cambios de dominio, el último a principios de junio.

Dejamos los datos de junio, porque a principios de mes se vio un nuevo cambio, ahora están usando otro dominio distinto, que no es un subdominio como los anteriores, sino que su dominio propio de scam.

Siguiendo los mismos comportamientos anteriores, tanto “pescanet.info” como “current-estado.info” son dominios comprados en Namecheap asociados a la misma IP: 66.29.146.71.

Ahora, si buscamos los dominios de C2, pero en las variantes del pack 0010 tenemos que siguen un camino distinto, pero similar:

Día inicio	C2
2023-04-01	https://new-falav2.edoblog.info
2023-04-02	https://new-falav3.edoblog.info
2023-04-04	https://falav2.dinamics.info
2023-05-02	https://falav3.pescanet.info
2023-05-12	https://new-main.ehloqservices.info
2023-05-18	https://fala.current-pro.info

Ahora, al analizar los dominios del pack “0010-5” vemos que tienen cierta relación con los anteriores. A principios del mes de abril, mantenían el dominio principal “edoblog.info”, pero luego se actualizaron, y en abril mayormente usaron el dominio principal “dinamics.info”.

En mayo ocurrió algo esperado, pero también algo inesperado. A principios de mes comenzó a aparecer el dominio principal “pescanet.info”. Luego reapareció, por un breve momento, un dominio utilizado a principios de año “ehloqservices.info”, pero finalmente siguió con la definición de un dominio nuevo “fala.current-pro.info” (que no tiene relación con el pack 0009-5 anterior).

Al igual que todos los dominios anteriores, este último, también fue registrado con Namecheap, y también apunta a la IP: 66.29.146.71.

Vamos a mantener un monitoreo de esta IP para ver si es que aparecen más dominios que podrían estar asociados a campañas similares, pero se recomienda validar con el hosting para ver quién podría estar detrás de estos dominios.

Presentamos FC-05

En este reporte queremos presentar los patrones que definen a un nuevo grupo, que estamos llamando internamente Fishers Constantes 05 (FC-05). La gracia de este grupo es el uso de un pack muy distintivo, el que internamente lo nombramos como “0099”.

En este punto queremos detallar un poco este pack, que afecta únicamente (según lo que hemos podido detectar nosotros) a un banco en Colombia.

Todos los sitios los hemos ido recolectando desde Replit, y todos con un patrón similar:

bancolombia.*[mua|app|360].*.repl.co

Siempre parte con bancolombia, luego viene algo de texto (puede ser “.com”), luego viene una de estas 3 palabras: “mua”, “app” o “360”, y luego termina con algo extra más, antes de usar el dominio de repl.co.

Con este patrón reconocible pudimos dar con la mayoría de los dominios maliciosos asociados a esta campaña.

Si analizamos lo que hemos encontrado, todos los packs de este tipo aparecen desde una misma IP: 34.149.204.188. Si recuerdan algún reporte anterior, tenemos que esta IP es la asociada al servicio de Replit.

Este es un servicio de PaaS bastante completo, en donde se puede subir código de distintos lenguajes:

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

En este caso volvemos a tener suerte, porque a pesar de poder usar muchos de los distintos tipos de lenguaje con código en el backend, en este caso toda la lógica de negocio está en el archivo main.dart.js, con lo cual podemos analizar el código.

Es un archivo bastante largo, con más de 5 MB de código Javascript, y muchas ofuscaciones y optimizaciones en el código que hacen bastante enredado leerlo, pero se pueden extraer cosas interesantes.

En el trasfondo puede que no sea tan interesante la lógica, sigue siendo un pack que usa el navegador para guardar información de las víctimas en un repositorio externo al sitio web actual, pero lo interesante en este caso es "qué repositorio" es el que están usando.

¡Están usando Google Sheets como almacenamiento de los datos!

POST	oauth2.googleapis.com	token
OPTIONS	sheets.googleapis.com	1-ggHujA9RGqNbayYkgCNIexKF0mxdA8VyEeYfoZeXTg
GET	sheets.googleapis.com	1-ggHujA9RGqNbayYkgCNIexKF0mxdA8VyEeYfoZeXTg
OPTIONS	sheets.googleapis.com	'NEJOPANELBEST'!A1:N1?valueInputOption=USER_ENTERED
PUT	sheets.googleapis.com	'NEJOPANELBEST'!A1:N1?valueInputOption=USER_ENTERED
GET	api64.ipify.org	/?format=
OPTIONS	sheets.googleapis.com	'NEJOPANELBEST'!A1:5000000?majorDimension=ROWS&valueRenderOption=UNFORMATTED_VALUE
GET	sheets.googleapis.com	'NEJOPANELBEST'!A1:5000000?majorDimension=ROWS&valueRenderOption=UNFORMATTED_VALUE
OPTIONS	sheets.googleapis.com	'NEJOPANELBEST'!A3:3?valueInputOption=USER_ENTERED
PUT	sheets.googleapis.com	'NEJOPANELBEST'!A3:3?valueInputOption=USER_ENTERED

Son comunicaciones que incluyen todo, desde la autenticación por OAuth a la API de Google y luego la inyección de los datos.

Nuevamente al igual que otros packs que ya hemos visto, como este pack está basando su lógica en archivos Javascript uno puede descargar esos archivos y obtener esos datos. Por ejemplo, podemos saber qué "scope" de la API están usando para la conexión:

```
B.IU=A.d(s([B.hK,B.z_,B.af,B.cN,B.aq,B.fg]),A.ac("v<lm>"))
B.IW=A.d(s(["https://www.googleapis.com/auth/spreadsheets","https://www.googleapis.com/auth/drive"]),t.s)
```

Podemos tener acceso al nombre usuario dueño de la planilla, además de la llave de API y el certificado usado (los datos están ofuscados, pero los tenemos).


```
{
  "type": "service_account",
  "project_id": "testri
  "private_key_id": "d1
  "private_key": "-----
  KEY-----\nMIIEvAIBADA
  T\nL1dr3jSDRC3cXjFQ9H
  3MtrAgMBAAECggEACi18y
  pUSCSdhKgrEzCSQutgzmg
  GvFhTWySq2syLOovjxagt
  kp+w6J2p5fDNb2vVwiny/
  D699YCMOauvCMgcRg8Dcg
  QOysqp7jsYYaIF88RdE45
  uL4/nBONFYNfiDbJDX\n1
  "client_email": "shet
  "client_id": "1169184
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/c
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/
}
```


Con estos datos podemos replicar esas llamadas, no solo para inyectar datos como si fuéramos del grupo, sino que también para descargar lo que ellos tienen o van subiendo.

Revisando información recopilada

Con la plataforma, nosotros tenemos detectados 52 de estos sitios, comenzando desde el 03 de mayo[5] hasta finales del mes[6].

En el transcurso de estos análisis nos hemos dado cuenta que han usado 2 sheets de Google distintas:

SheetID	Fecha Inicio	Fecha Fin
1zT0f84obFmPmlzP0Z-adlxzLBjDLNguIPpnS88bsIGY_1684340477 v1	2023-03-23	2023-05-26
1zT0f84obFmPmlzP0Z-adlxzLBjDLNguIPpnS88bsIGY_1684340477 v2	2023-05-27	2023-05-30
1-ggHujA9RGqNbayYkgCNlexKF0mxdA8VyEeYfoZeXTg_1685390239	2023-05-29	actualidad

El grupo "FC-05" parece que ha sido muy metódico en la forma que han organizado su planilla de datos, según lo que podemos obtener tienen los siguientes campos:

- **Id**: identificador único del usuario que está cayendo en la estafa
- **Fecha**: Fecha en que cayó en la estafa (ingreso de datos)
- **Usuario**: nombre de usuario del banco
- **Contraseña**: contraseña del usuario del banco
- **Dinamica**: Clave dinámica pedida por el banco (2FA)
- **Tarjeta**: Número de tarjeta de crédito/débito ingresada
- **Mes**: Mes de vencimiento de la tarjeta anterior
- **Año**: Año de vencimiento de la tarjeta anterior
- **Cvv**: Número de seguridad de la tarjeta anterior
- **Email**: Correo electrónico de la víctima
- **Clave email**: Clave del correo electrónico de la víctima
- **Celular**: Número de celular de la víctima
- **Ip**: IP de origen de la víctima
- **User**: Alias del que creó el sitio y está detrás de la campaña actual

[5] Reporte original en la siguiente URL: https://phishing.finsin.cl/list.php?query=0fa10781c8f271d31a66775d3359ec5ed681ae44b7c42a3de282bbdf0c8396e2

[6] Siguen las detecciones en junio, pero no cuentan para este informe

En general, los datos ingresados en la planilla no tienen todos los campos, son muchos los datos que faltan, porque se guarda cada interacción con el sitio, por lo que un mismo usuario, en distintas etapas del phishing (user, password, celular, tarjeta) tiene distintas filas en la planilla final.

A pesar de lo anterior, como números globales tenemos que:

Fecha inicio de recolección	2023-03-23
Fecha fin de recolección	2023-05-31
Número total de datos extraídos	20.352
Cantidad de números de celular (aprox)	3147
Cantidad de emails	3119
Cantidad de emails con clave	1930
Cantidad de tarjetas (aprox)	680

De ese listado habría que ir eliminando los datos basura que siempre existen en este tipo de estafas, pero no dejan de ser números bastante buenos para una estafa de este tipo.

Tenemos el listado completo de esta información, pero no podemos publicarla libremente, si alguien la requiere favor contactarnos.

Revisando información del grupo

Otro punto también interesante de revisar es la última columna, el de los usuarios controladores de este scam, para ello tenemos 2 fuentes de información:

Fuente 1: Nuestra plataforma

La primera forma es a través de los phishings que nosotros hemos ido identificando. Con los datos extraídos de los archivos del mismo sitio hemos ido identificando cuáles son los nombres de los "encargados", y tenemos lo siguiente:

User	Cantidad
newalejo	7
newalejobest	4
panelchente	3
ALEMAN	3
BURROQWE	2
ALEJOPANELQWE	2
NEJOQWERT	2
MARCUTOQWERT	2
nosotros	2
cangrejo	1
puebloflaco	1
budaa	1
alemanbest	1
calamar	1
panelnejodos	1

User	Cantidad
marcuto	1
suizodos	1
ESLOVACO	1
CHENTEUNO	1
NEWALEJOBESTUNO	1
alejoaaqwe	1
ALEMANQWE	1
CHENTEQWE	1
CALAMARDOQWE	1
MARCUTOQWE	1
PAKISTANQWE	1
CALAMARASD	1
ALEJOUJIUHYTGRFDEWSDH	1
Russo	1

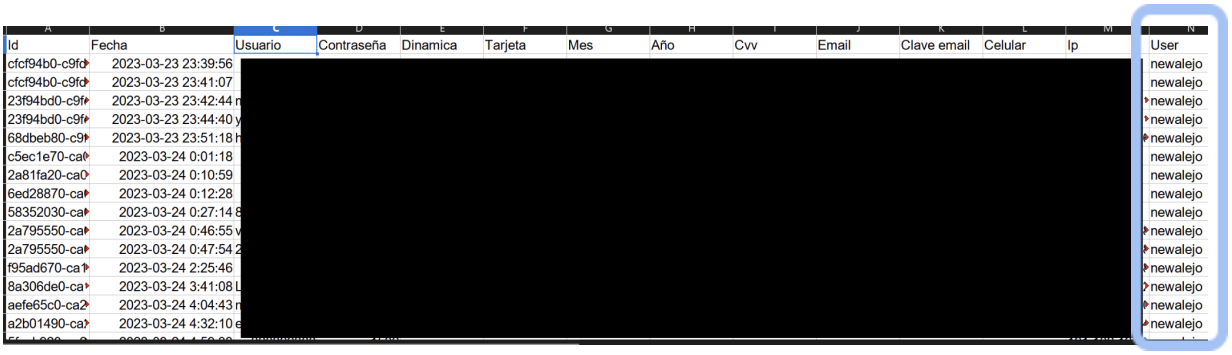
Tenemos 29 alias que hemos encontrado directamente asociados a esta campaña.

Estos alias son los que podemos asociar alguno de los sitios de phishing que encontramos, pero ahora viene lo interesante, asociar los datos guardados a los alias.

Tenemos 29 aliases que hemos encontrado directamente asociados a esta campaña.

Fuente 2: Datos almacenados

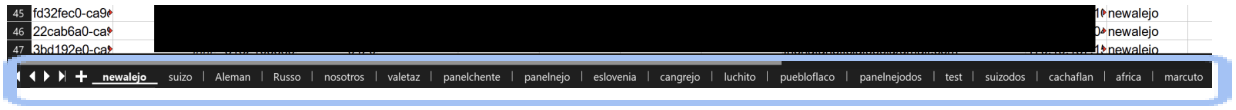
La segunda es extraerlos directamente de la planilla que ellos guardan online, como por ejemplo, lo que mostramos en el screenshot anterior:



Id	Fecha	Usuario	Contraseña	Dinamica	Tarjeta	Mes	Año	Cvv	Email	Clave email	Celular	Ip	User
cfcf94b0-c9fd	2023-03-23 23:39:56	[redacted]											newalejo
cfcf94b0-c9fd	2023-03-23 23:41:07												newalejo
23f94bd0-c9f	2023-03-23 23:42:44												newalejo
23f94bd0-c9f	2023-03-23 23:44:40												newalejo
68dbeb80-c9	2023-03-23 23:51:18												newalejo
c5ec1e70-ca	2023-03-24 0:01:18												newalejo
2a81fa20-ca0	2023-03-24 0:10:59												newalejo
6ed28870-ca	2023-03-24 0:12:28												newalejo
58352030-ca	2023-03-24 0:27:14												newalejo
2a795550-ca	2023-03-24 0:46:55												newalejo
2a795550-ca	2023-03-24 0:47:54												newalejo
f95ad670-ca1	2023-03-24 2:25:46												newalejo
8a306de0-ca	2023-03-24 3:41:08												newalejo
aefe65c0-ca2	2023-03-24 4:04:43												newalejo
a2b01490-ca	2023-03-24 4:32:10												newalejo

Como podemos ver en el extracto de esa planilla, en el campo de más a la derecha tenemos una columna llamada “User”, en este caso el campo dice “newalejo”, que es uno de los que habíamos identificado anteriormente.

Además, si vemos las hojas de la planilla, vemos que también están ordenados, tienen cada hoja identificada por uno de los alias utilizados:



Con esto, nos hacen el trabajo mucho más fácil, basta con juntar todos los datos, o extraer todos los alias de la plantilla, con esto tenemos:

User	User	User	User
africa	CALAMARASD	MARCUTOQWE	panelnejodos
alejoaaqwe	CALAMARASDX	MARCUTOQWERT	puebloflaco
ALEJOPANELQWE	CALAMARASDXZXCVB	MARCUTOUNO	Russo
ALEJOPANELQWERT	CALAMARDOQWE	NEJOPANEL	RUSSOQWE
ALEJOUJIUHYTGRFDEWSDH	cangrejo	NEJOPANELUNO	RUSSOQWEsdalkdj
Aleman	CHENTE	NEJOQWERT	suizo
ALEMANASD	CHENTEQWE	NEJOZXCV	suizodos
alemanbest	CHENTEUNO	NEJOZXCVkoijkiuhyu	SUIZOQWE

ALEMANQWE	ESLOVACO	newalejo	test
budaa	ESLOVACOUNO	newalejobest	valetaz
Burrodos	eslovenia	NEWALEJOBESTUNO	
Burrooaspdoaksopd	guillopyme	nosotros	
BURROQWE	luchito	PAKISTANQWE	
cachaflan	LUCHO	panelchente	
calamar	marcuto	panelnejo	

¡Tenemos 56 alias asociados a estas campañas!

Es una campaña mucho más masiva de lo que estábamos asumiendo, pero si miramos los alias, vemos que hay patrones que se repiten.

Por ejemplo, todos los siguientes tienen una raíz común:

- NEJOPANEL
- NEJOPANELUNO
- NEJOQWERT
- NEJOZXCV
- NEJOZXCVkoijkiuhyu
- panelnejo
- panelnejodos

De hecho, la raíz “NEJO” es muy parecida a “newalejo”, tiene el mismo inicio y el mismo final, lo cual lo hace muy sospechoso. Además, si hacemos esa asociación, tenemos que los “Alejo” deberían ser de la misma familia de los “newalejo”, y los asociamos al mismo actor por detrás.

Algo parecido podemos hacer con los siguientes:

- CHENTE
- CHENTEQWE
- CHENTEUNO
- panelchente

Todos tienen la palabra clave “chente” dentro del alias, por lo tanto los podemos asumir como el mismo actor.

Realizando esta asociación para todos los alias antes mencionados tenemos la siguiente lista corta de alias de ciberdelincuentes:

- africa
- Alejo
- Aleman
- budaa
- Burro
- Cachjaflan
- Calamar
- Cangrejo
- Chente
- Eslovaco
- Guillopyme
- Lucho
- Marcuto
- Nosotros
- Pakistan
- PuebloFlaco
- Russo
- suizo
- Test
- Valetaz

¡Son solo 20 alias los que nos interesan![7]

Y si cruzamos estos alias con la cantidad de datos almacenados en las planillas tenemos lo siguiente:

User	Cantidad
Alejo	11454
Aleman	3008
Russo	1769
Nosotros	1329
Chente	1321
Marcuto	885
Eslovaco	658
PuebloFlaco	570
Calamar	437
suizo	400

User	Cantidad
Burro	391
Cangrejo	270
budaa	241
Lucho	118
africa	96
Cachjaflan	66
Test	59
Pakistan	18
Valetaz	7
Guillopyme	2

Tenemos que claramente el "Alejo" es el más activo, y probablemente el líder del grupo, que actúa asociado con Alemán y Russo. Pero no tenemos mucha más información al respecto.

[7] De hecho, deberíamos quitar el test, pero no podemos descargarlo todavía, por lo que preferimos dejarlo y que queden los 20.

Palabras finales

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.

Aunque somos una fundación con base en Chile, tenemos bastante información relacionada con kits y actividades en otros países de la región, 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 y/o con policías 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

2023

Reporte Marzo 2023:

- https://finsin.cl/2023/04/18/reporte-mensual-de-phishing-marzo-2023/

Reporte Febrero 2023:

https://finsin.cl/2023/03/13/cumplimos-1-ano-de-reportes-de-phishing/

Reporte Enero 2023:

- https://finsin.cl/2023/02/13/reporte-mensual-de-phishing-enero-2023/

2022

Reporte Diciembre 2022:

- https://finsin.cl/2023/01/13/reporte-mensual-de-phishing-diciembre-2022/

Reporte Noviembre 2022:

- https://finsin.cl/2022/12/12/reporte-mensual-de-phishing-noviembre-2022/

Reporte Octubre 2022:

- https://finsin.cl/2022/11/14/reporte-mensual-de-phishing-octubre-2022/

Reporte Septiembre 2022:

- https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022

Reporte Agosto 2022:

- https://finsin.cl/2022/09/11/reporte-mensual-de-phishing-agosto-2022/

Reporte Julio 2022:

- https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/

Reporte Junio 2022:

- https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

Reporte Mayo 2022:

- https://finsin.cl/2022/06/05/reporte-mensual-de-phishing-mayo-2022/

Reporte Abril 2022:

- https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/

Reporte Marzo 2022:

- 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/