FINSIN

Reporte de Phishing

Octubre 2022

Indice

Introducción

En nuestros análisis como fundación de ciberseguridad encontramos que uno de los principales problemas que afectan a la comunidad en estos temas es la desinformación y los engaños.

Dentro de estos engaños el más prevalente y uno de los que tiene impacto más directo sobre la población en general es el "Phishing".

Este tipo de ataques es muy generalizado y al parecer es un ataque muy barato, por lo que los ciberdelincuentes pueden generar muchas "copias" diariamente, y solamente tendrían que hacer que las personas visiten el sitio para poder engañarlas y robarles sus claves u otro tipo de información.

Al analizar algunos de estos sitios encontramos que tenían patrones comunes de comportamiento, y que habían varios hechos de la misma forma, con archivos muy similares que provenían todos de un mismo "kit de phishing".

Nos dimos a la tarea de clasificar y agrupar los sitios que íbamos encontrando de manera "manual", pero luego tuvimos la problemática de que la cantidad de sitios crecía mucho y el tiempo que podíamos dedicarle a esa investigación se mantenía igual y muy reducido.

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

Con lo anterior, a principios de Febrero lanzamos la plataforma Phishing Checker de FINSIN para detectar de manera automatizada los sitios que afectan a la comunidad en Chile y también expandir un poco esta detección a los demás países en Latinoamérica que esta herramienta pueda detectar.

Ricardo Monreal Llop
Presidente FINSIN

TL;DR

A modo de resumen, tenemos los siguientes resultados para el mes de Octubre[1]:

Este mes queremos presentar un nuevo grupo: FC-04

Queremos mostrar a un poco más a detalle el funcionamiento del kit 0006 y 0003

Queremos mostrar que los FC-03 siguen activos y mantienen su infraestructura para nuevas campañas

Se asume que tanto el pack 0006 y 0003 partieron como parte del desarrollo mismo grupo

Tenemos una relación visual entre los correos, que nos ayuda a ver mejor quienes se conocen y quienes podrían ser de FC-04

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

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

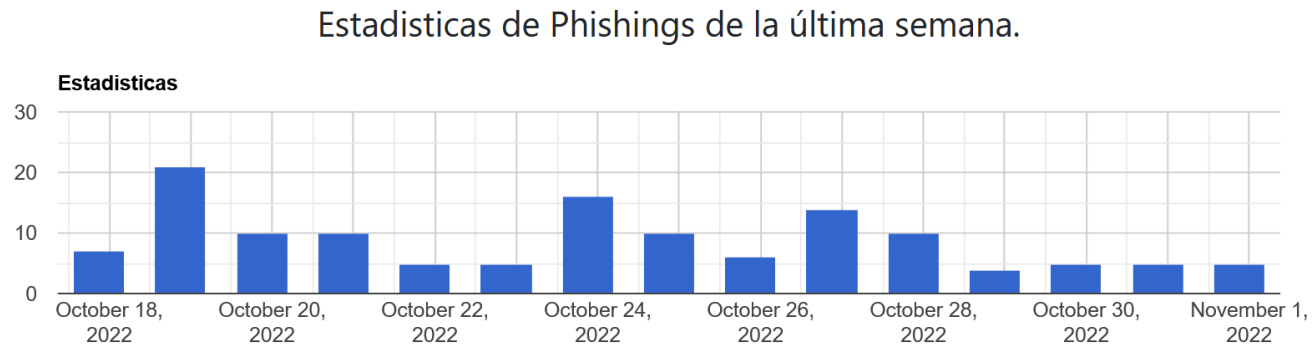
Phishing Checker

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

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

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

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



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

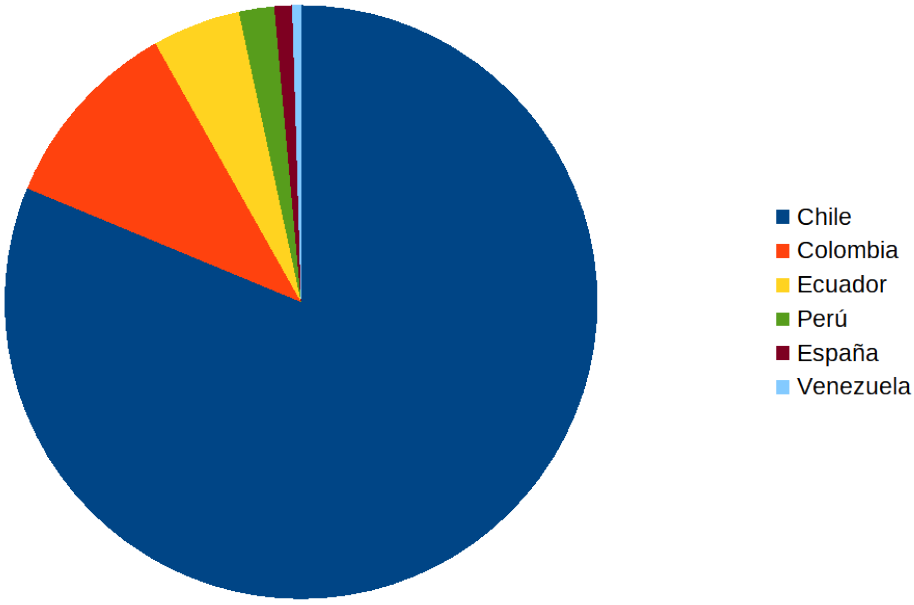
Pueden registrarse en el canal ingresando a la URL: https://t.me/Phishing_FINSIN, síguenos y ayúdanos a difundir nuestra plataforma.

Octubre 2022

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

Datos de países[2]

Si miramos los países de las marcas afectadas tenemos lo siguiente:

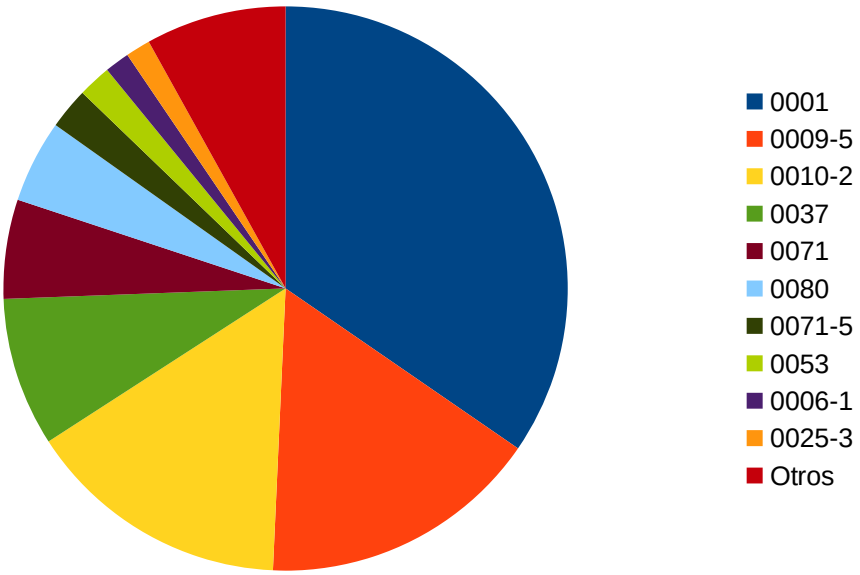


Pais	Porcentaje
Chile	81,25 %
Colombia	10,58 %
Ecuador	4,81 %
Perú	1,92 %
España	0,96 %
Venezuela	0,48 %

2 Es la distribución de los phishing que fueron detectados por la plataforma, no corresponde al total real de Chile ni constituyen un ranking del mundo.

Datos de kits

En octubre logramos agregar 5 kits nuevos y 3 variantes nuevas de Phishing que ya conocíamos antes. Si graficamos estos datos queda un poco parecido a los meses anteriores:



Este mes volvemos a la "normalidad", porque el pack 0001 vuelve a ser el primero del mes:

Pack	Porcentaje
0001	37,63 %
0009-5	16,11 %
0010-2	15,17 %
0037	8,53 %
0071	5,69 %
0080	4,74 %
0071-5	2,37 %
0053	1,90 %
0006-1	1,42 %
0025-3	1,42 %
Otros	8,06 %

Y vuelven a aparecer los kits como el 0009-5[3] y el 0010-2[4] que tienen más del 10% de las detecciones del mes cada uno. Esto nos hace validar que los kits "nuevos" que estamos detectando están para quedarse.

3 Revisado en: https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/
4 Revisado en: https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

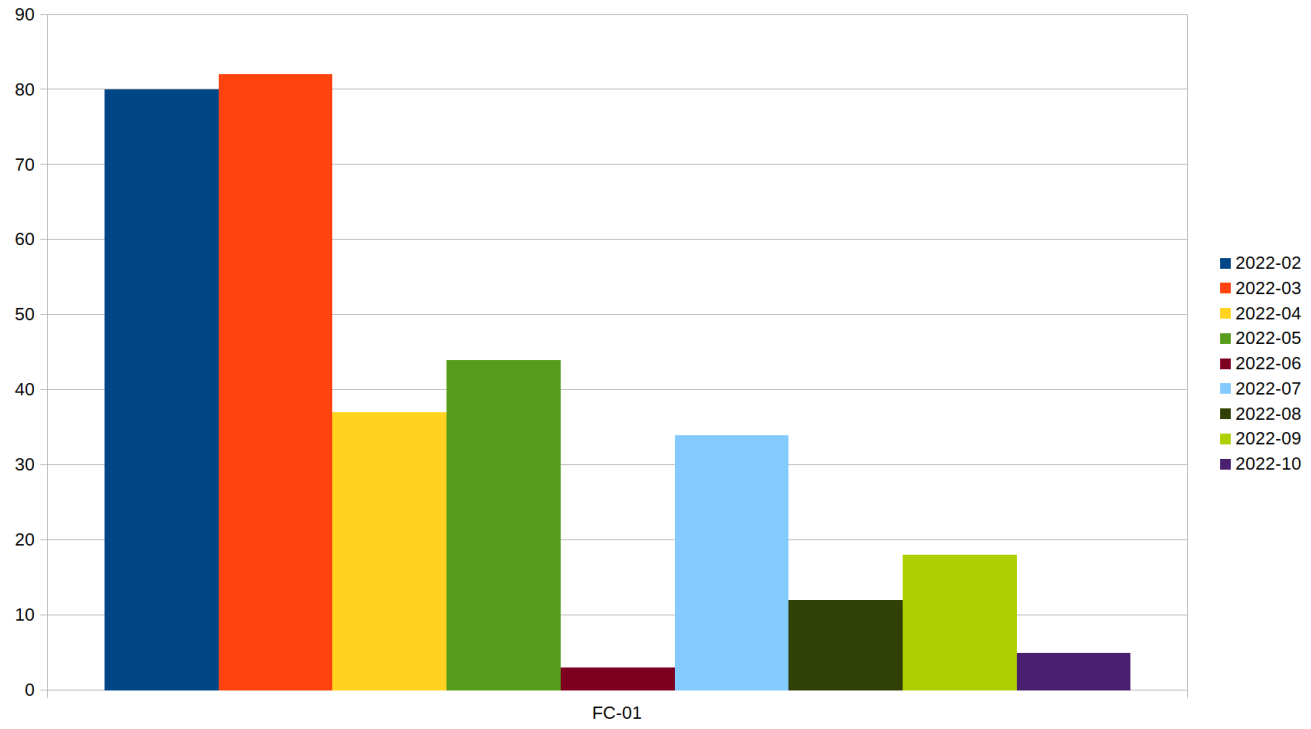
Actualización FC-01 y FC-03

Dentro de los últimos reportes hemos estado caracterizando y siguiendo a los grupos FC-01[5] y FC-03[6] que aunque tienen nombres parecidos tienen características muy distintas.

FC-01

Como hemos visto anteriormente 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.

En los últimos meses ha bajado su actividad, llegando a una actividad muy baja ahora en octubre, como podemos ver en el siguiente gráfico.



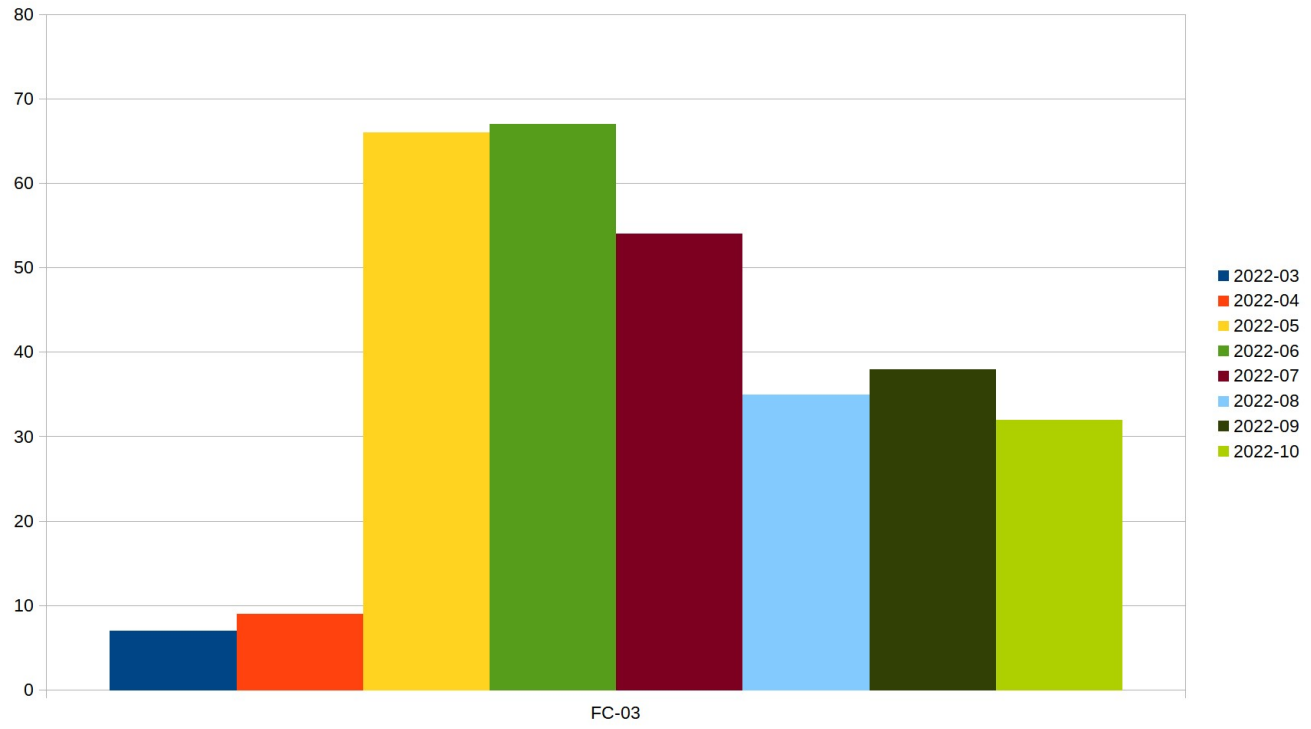
Esperamos que este grupo resurja con nuevos dominios en los meses venideros, pero ya no como los meses de febrero y marzo, que llegaron a su peak.

5 Definido en el reporte de Febrero: https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/

6 Definido en el reporte de Junio: https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/

FC-03

El grupo FC-03 es de los que más se ha "mantenido en el tiempo", Como podemos ver, aún cuando en los últimos meses se ha visto a la baja, tenemos que se mantiene con un número alto de sitios por mes.



Tanto en agosto como septiembre podemos ver que levantan un poco más de 30 sitios por mes.

Creemos que su longevidad se debe a que principalmente es de los grupos con menor gasto para la generación de sus dominios.

- Siguen usando el mismo kit "0010-2" que es el kit que han usado desde fines de Mayo, por lo que su inversión en desarrollo sigue siendo 0.
- Siguen usando la plataforma Firebase de Google para levantar sus sitios en el nivel gratis, por lo que siempre son subdominios de .firebaseapp.com o .web.app.
- Siguen usando subdominios del dominio "ehloq.xyz" como base de datos externa para sus datos robados. Lo único que necesitan aquí es mantener sus costos de dominio y de servidores, por lo que sigue siendo barato.

Revisando los dominios usados en el mes de Septiembre tenemos que son los siguientes:

Dominio BBDD	Cantidad
main-fala.ehloq.xyz	28
worker-fala.ehloq.xyz	14

Como lo habíamos visto anteriormente, estos dominios son parte de la infraestructura de FC-03 y ambos apuntan a la IP 162.0.209.127, que es parte de las IPs controladas por Namecheap[7].

Queremos mostrar que los FC-03 siguen activos y mantienen su infraestructura para nuevas campañas

Lo interesante de este mes es que aparecieron unos dominios nuevos, que afectan a otras bancas en chile, tenemos:

- security-bot.ehloq.xyz: Asociado a una campaña que afecta a Banco Security de Chile
- santa-bot.ehloq.xyz: Asociado a una campaña que afecta a Banco Santander de Chile

Con esto queremos mostrar que los FC-03 siguen activos y mantienen su infraestructura para nuevas campañas, por lo que es recomendable que se intervenga (de ser posible) el dominio o se gestionen conversaciones con el hosting para remover el control de estos dominios.

De lo contrario, lo más probable es que sigan levantando sitios, de campañas nuevas o existentes, y aunque se les haga la baja de algunos de estos de "forma rápida", sigue siendo rentable.

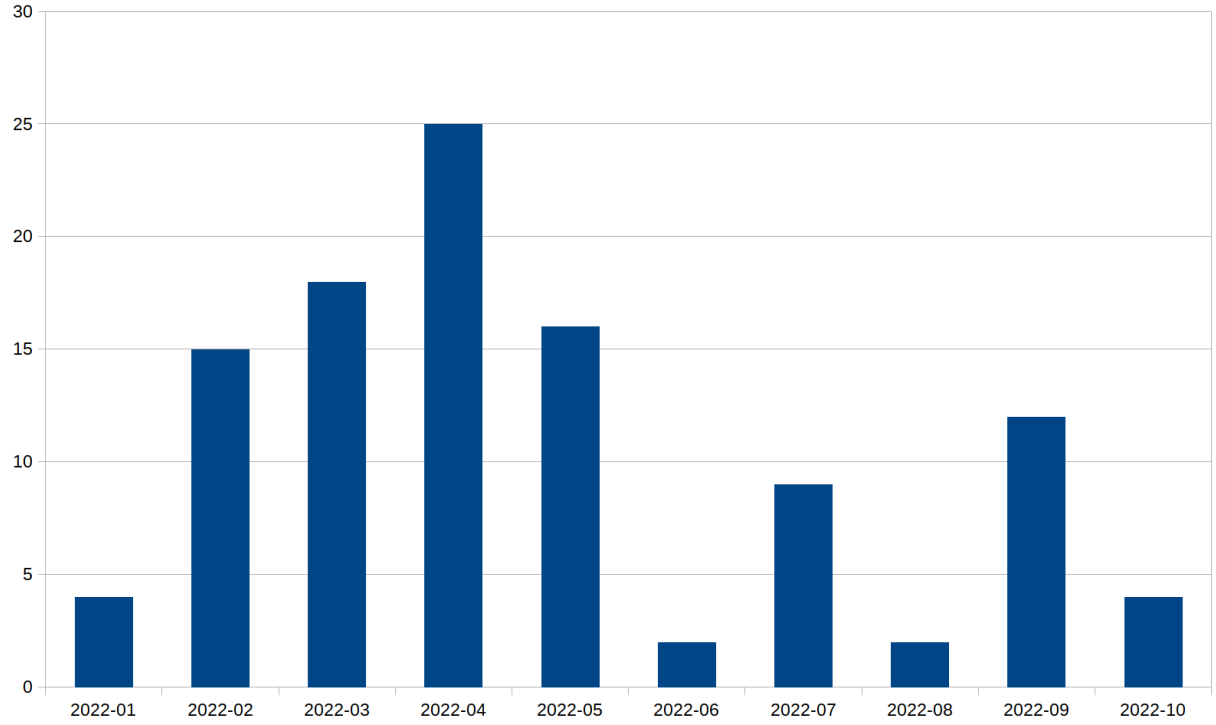
7 https://www.namecheap.com/hosting/

Presentando FC-04

Este mes queremos presentar a un "nuevo" grupo, que lo llamaremos "Fishers Constantes 04" (o FC-04 para abreviar).

Este es un grupo que la verdad no es tan nuevo en Chile, ya van varios años (por lo menos 5) en donde se tiene conocimiento de este tipo de phishing.

Como lleva mucho tiempo en estas andanzas es normal que no lo veamos tan seguido nosotros en nuestra plataforma. Lo que tenemos detectado de este grupo es:



Podemos ver que como muchos de los otros phishings, el peak de detección fue en abril de este año.

Este grupo, usa 2 tipos de kits que nosotros conocemos y tenemos catalogados: usa el kit 0006[8] (con variantes) como pasarela de autenticación, y los que nosotros tenemos catalogado como "0002" o "0003" como sitio de phishing final.

Queremos mostrar a un poco más a detalle el funcionamiento del kit 0006 y 0003

A continuación queremos mostrar a un poco más a detalle el funcionamiento del kit 0006 y 0003.

8 Este kit lo hemos visto anteriormente.

Kit 0006

Este kit nosotros lo llamamos "0006" (con algunas variantes) y también se llama "cloaking" porque es el nombre con el que se reparte en el archivo .zip. Nosotros también lo hemos discutido en las charlas que hemos hecho[9] sobre el tema y es bastante interesante como lo usan.

Cabe destacar que el FC-04 no son los únicos que lo usan, el grupo que nosotros llamamos FC-01 también usa el kit 0006, pero no tenemos evidencias suficientes para ligar a ambos, por lo que los tratamos como grupos distintos.

Este kit tiene algunos features que nos parecen interesantes, como por ejemplo:

- **Desarrollado en PHP:** Esto permite que se suba en distintos hosting, ya sea pagados o comprometidos, por el uso masivo de este lenguaje de programación. Además, se asume que este pack se desarrolló inicialmente en Perú para usarlo de pasarela para atacar a un banco local (y no se ha cambiado el default timezone desde entonces).

```php
<?php

session_start();
date_default_timezone_set('America/Lima');

require_once('class/class.web.php');

$cp = new AdsJerts();
$ipv = $cp->getClientIP();
$dates = date("d/m/Y g:i a");

$accion = $_GET['web-admin'];

switch($accion) {

    case 'jdh329xdj':
```

9 Por ejemplo, en la conferencia DragonJAR 2022 https://finsin.cl/2022/09/08/participamos-en-dragonjarcon-2022/

- **Redirige siempre con "URLs largas"**: para usar la pasarela se necesita usar una ruta específica que está definida en el archivo .htaccess, debe ser una palabra (\w+) seguida de una o dos palabras separadas por un signo menos (-) que termine con un slash (/). Si esa ruta no se cumple, no va a redirigir correctamente.

```
RewriteRule ^(\w+)/(\w+(\-\w+)?)/$ wp-chek.php  [NC,L]
RewriteRule ^intranet/$ wp-admin.php?web-admin=jdh329xdj  [NC,L]
```

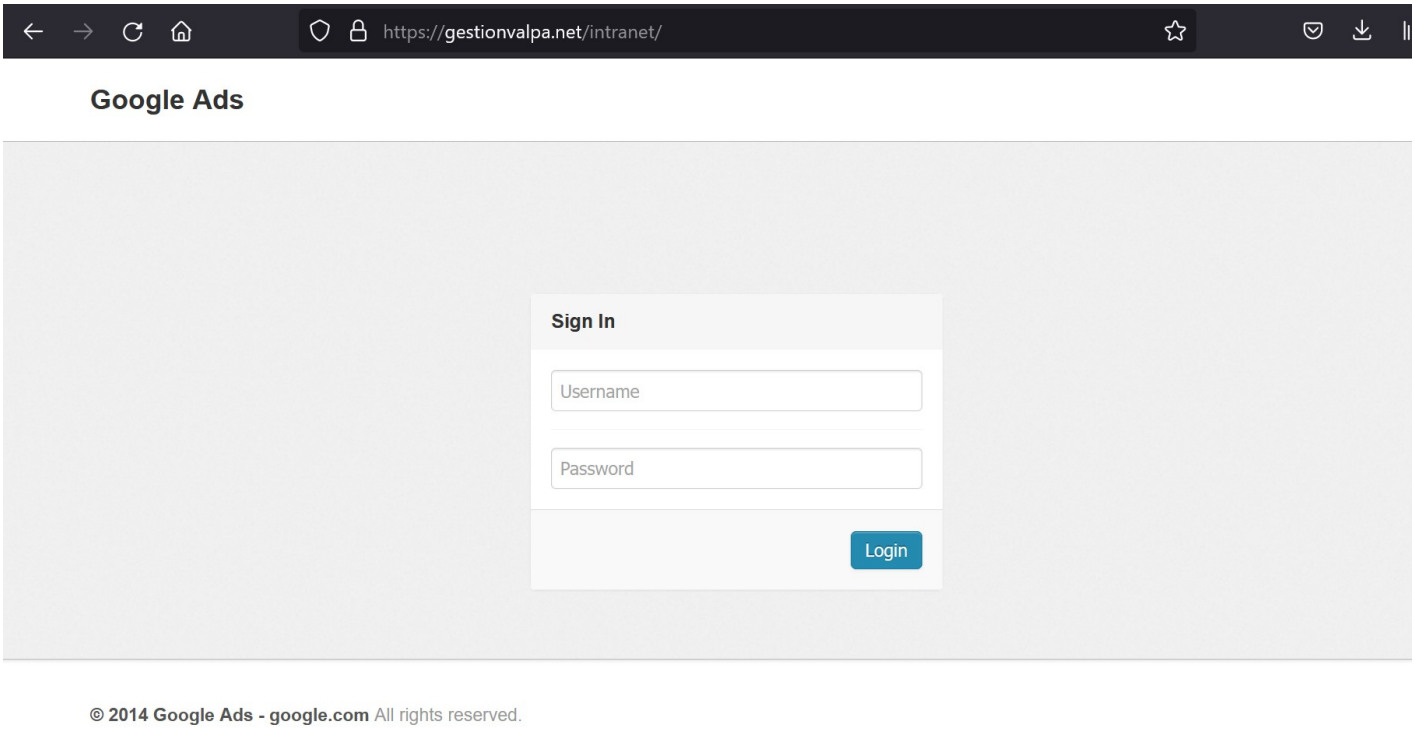
- **No tiene contenido para robar datos**: Es solo una pasarela para filtrar bots, para ello utiliza una serie de revisiones como: geolocalizacion de IP, navegador, sistema operativo. No tiene funcionalidad para robo de contraseña de correo o robo de número de tarjeta, si pasas las revisiones anteriores te lleva al sitio de phishing.

```
$code = getCountryFromIP($ipv);

if($code == $menus[0]){
            $rcase = 0;
        } else {
            $rcase = 1;
        }

switch($rcase){

    case 0:
    //Ip List Block

                $ipArray = $menus[3];
                  foreach ($ipArray as $ipTest) {
                  if (substr_count($ipv,trim($ipTest)) != "0") {
                     $blocking = true;
                    }
                  }
                  if($blocking) {
                  $injert->savelogs($ref,$menus[0],$perfect=false);
                              $injecthtml = "<meta http-equiv='Refresh' content='0; URL=".$menus[2]."'>";
                              print $injecthtml;
                              exit();
                  } else {


                              $injert->savelogs($ref,$menus[0],$perfect=true);
                              $injecthtml = "<meta http-equiv='Refresh' content='0; URL=".$menus[1]."'>";
                              print $injecthtml;
                              exit();

        }

    break;
```

- **Administración incluída en ruta fija**: Sabemos que la administración interna del sitio se accede a través de la siguiente ruta, /intranet/, aunque esta es una ruta definida por el archivo .htaccess que reescribe hacia el archivo wp-admin.php, no es una "carpeta" real.

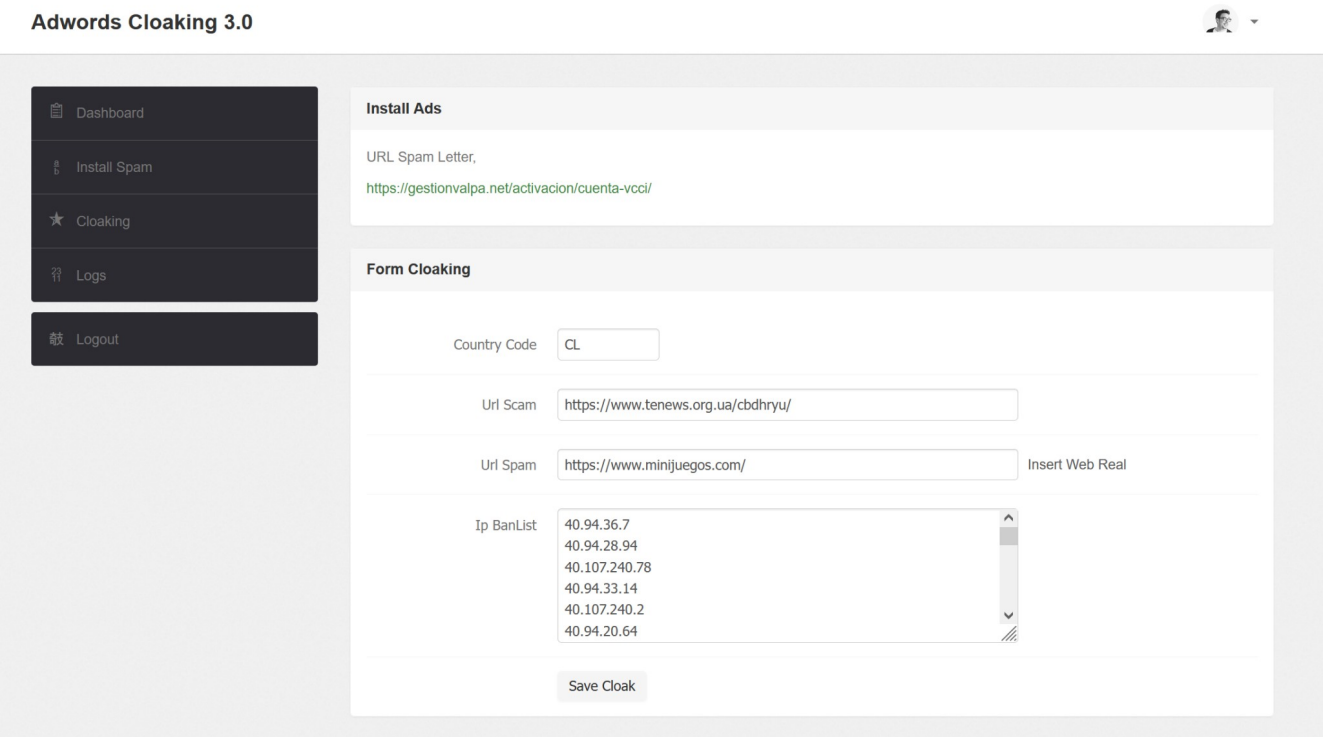
```
RewriteRule ^(\w+)/(\w+(\-\w+)?)/$ wp-chek.php  [NC,L]
RewriteRule ^intranet/$ wp-admin.php?web-admin=jdh329xdj  [NC,L]
```

Al acceder a la ruta del panel de administración, tenemos la siguiente pantalla:



Esto nos tiene que alertar que algo malo hay detrás inmediatamente. Aun cuando no sepamos exactamente qué dominio es el involucrado, Google no va a mantener un panel administración de Ads con el Copyright del año 2014 (hace 8 años!).

Al acceder dentro del panel, vemos el nombre real del kit “Adwords Cloaking 3.0” y varias configuraciones.



- **URL Spam Letter:** Esta línea no es configurable, pero te muestra la URL que le puedes enviar a las víctimas a través de correo, SMS u otros.
- **Country Code**: Configuración para forzar la geolocalización solo a IPs del país definido. Para saber el país de la IP de la víctima usa el servicio online en la siguiente URL: http://extreme-ip-lookup.com/json/[IP]. Con eso puede mantener la geolocalización actualizada.
- **Url Scam**: Es la URL del sitio de phishing que quieres que caigan luego de la pasarela. Es la URL del sitio de phishing “real”.
- **Url Spam**: Es la URL del sitio usado para despistar a bots y a IPs que no son del país “afectado”. Es una URL benigna que sirve para mantener a los scanners automáticos yendo a otro sitio y marcando como “benigno” el link.
- **Ip BanList**: Es una lista de IPs que aún cuando sean del país correcto, van a ser redirigidas a la URL definida en “Url Spam”.

Lo interesante es que la configuración anterior está guardada en el mismo servidor, y no en una

base de datos, sino que directamente en unos archivos. Al revisar el código del kit podemos ver que están siempre en la misma ruta: /data/config.pj

Como es una extensión de archivo bastante inusual, los servidores no saben bien como tratarla, por lo tanto te permiten siempre descargarla y tenemos algo como lo siguiente:

```
eJG+ZMOeo8ykoIBlZKGsvHChp6SSiJqOspeXj6GxpG2pol3InaWrom2VY6iyrHWinr+dm8FbspKpubOy
gGVez6ukc5iWmJhlqaCyl5G9oJmnZJiWY7Wst6uiZ8NikLWjZJakrKytwVusiWlgdGlnWGZ3eWl3bF/T
Wao=|
```

Lo cual no es muy entendible, pero es un algoritmo de cifrado y descifrado bastante simple. Para descifrarlo necesitamos solamente decodificar el string en base64, y luego irle restando el número de la tabla de ascii de cada carácter de la llave, muy al estilo del cifrado de Vignere[10]

Podemos saber exactamente cuál es la configuración, sin saber la contraseña

```php
function Desofuscar($string, $key) {
    $result = '';
    $string = base64_decode($string);
    for($i=0; $i<strlen($string); $i++) {
        $char = substr($string, $i, 1);
        $keychar = substr($key, ($i % strlen($key))-1, 1);
        $char = chr(ord($char)-ord($keychar));

        $result.=$char;
    }
    return $result;
}
```

Ahora podemos saber exactamente cuál es la configuración, sin necesidad de saber cual es el usuario/contraseña del panel de administración.

```
Descifrado:
CL{%}https://www.tenews.org.ua/cbdhryu/{%}https://www.minijuegos.com/{%}40.94.36.7
40.94.28.94
40.107.240.78
40.94.33.14
40.107.240.2
40.94.20.64
35.217.121.70
40.94.25.22
104.47.92.247
```

Con lo anterior podemos ser más proactivos para validar cuando se hacen los cambios en este archivo de configuración y reaccionar más rápido para dar de baja el siguiente sitio.

10 Para más información: https://es.wikipedia.org/wiki/Cifrado_de_Vigen%C3%A8re

Kits 0002 y 0003

Los kits 0002 y 0003[11] llevan bastante tiempo circulando en Chile, de hecho parte del código se mantiene intacto desde el 2016, lo cual nos hace pensar que el kit ha sido bastante útil a través de los años.

Estos dos kits son bastante similares entre ellos y tienen las siguientes características:

- **Mantiene los datos de víctimas en el servidor**: Siempre guarda los datos en el mismo servidor, dependiendo del kit es la ruta en la que están guardados los datos. Para el pack "0002" la ruta es: pagina/funcion.js; para el pack "0003" es pagina/css/style.css. En esa ruta se guardan los datos de las víctimas como: rut, tarjeta de coordenadas, tarjeta de crédito, etc.
- **Mantiene los datos de contacto del controlador en el servidor:** Siempre guarda los datos de contacto del "dueño" del kit. Estos datos son parte de la configuración del kit y se guardan en: pagina/config.js. Acá queda definido el correo de contacto a donde le van a llegar los datos de las víctimas, esto queda como respaldo de lo guardado en el punto anterior.
- **Geolocalización por país**: Utiliza un código simple para saber el país al que está asociada la IP, y luego verifica que sea el mismo país definido en el archivo de configuración (en el caso de la imagen es $valore[0]) . Si es que pasa la validación le presenta el sitio de phishing, de lo contrario muestra una página de 404.

11 Revisamos este kit inicialmente en marzo de este año: https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/

```php
$ipv = $system->getClientIP();
$country_code = $system->CountryCode();
$country_name = $system->CountryName();

$logs = $system->OpenFile(CONFIG_FILE);
$dblanding = $system->Desofuscar($logs, KEYCRYPT);
$valore = split("{%}",$dblanding);

$countryGets = $_GET['CDG'];
if( empty( $countryGets ) ){
    $countryGets = $country_code;
}

switch ($countryGets){

        case $valore[0]:
```

- **Los datos guardados están cifrados**: Usan el mismo "cifrado" que en el pack "0006", una aplicación del cifrado de Vignere. De hecho el bloque de código se escribió igual, con el mismo nombre "Desofuscar", los mismos nombres de variables, etc. Parece ser extraído del mismo código.

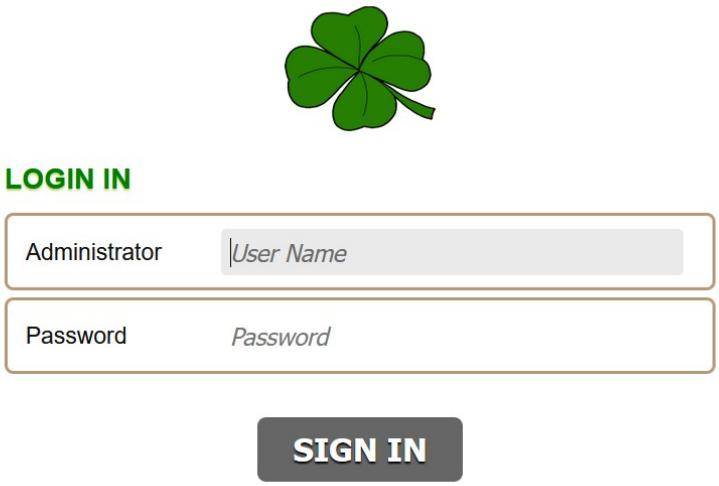
```php
function Desofuscar($string, $key) {
    $result = '';
    $string = base64_decode($string);
    for($i=0; $i<strlen($string); $i++) {
        $char = substr($string, $i, 1);
        $keychar = substr($key, ($i % strlen($key))-1, 1);
        $char = chr(ord($char)-ord($keychar));

        $result.=$char;
    }
    return $result;
}
```

Aun cuando las llaves usadas en ambos packs son distintas, como el funcionamiento es muy similar, se asume que tanto el pack 0006 y 0003 partieron como parte del desarrollo del mismo grupo.

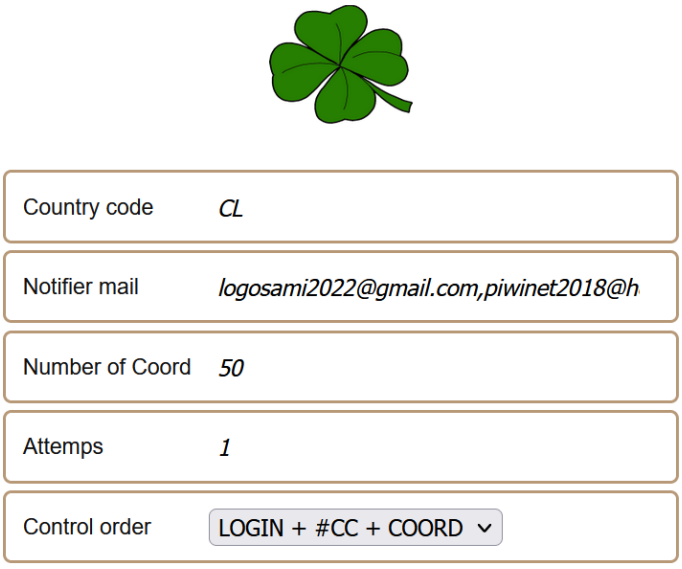
- **Tiene administración integrada**: La ruta de la administración está en admin/, pero al igual que en casos anteriores, no es un archivo, sino que es una ruta generada por un "rewrite" de .htaccess

```
RewriteRule ^admin/$ Web.php?CDG=Admin
```

Ahora, como sabemos la ruta de la administración, podemos llegar a ella y vemos lo siguiente:



Este es el panel que generalmente se ve en la ruta que nombramos previamente, pero si logramos entrar al panel con el usuario y contraseña correcto tenemos la información que se guarda como parte de la configuración (en el archivo config.js).



Aquí podemos ver los parámetros que se configura:

- **Country Code**: Es el código de 2 letras del país al cual se va a geolocalizar, en el caso de la imágen CL es para Chile.
- **Notifier mail**: Son 1 o más correos que se definen como parte de la notificación de una víctima. Cada vez que la víctima ingresa algún tipo de información en la plataforma de phishing, ésta le envía un correo a los que estén definidos en este campo.

Podemos estudiar los correos que están detrás de estos scams.

- **Number of Coord**: Es el número de coordenadas que te va a pedir, como parte del sitio de phishing. Por defecto son 50, porque son el número de coordenadas que tienen las tarjetas de coordenadas que la banca proporciona en Chile (Vertical del 1 al 5 y Horizontal de la A a la J).
- **Attemps**: Es el número de veces que se ingresan los datos de coordenadas, simulando que la víctima se pueda haber equivocado y que la segunda vez sea más consiente de lo que está haciendo.
- **Control order**: Es el flujo que se va a tener de los datos que se le piden a la víctima.

Una de las cosas más interesantes es que todas estas configuraciones, al igual que en el pack 0006, están al alcance de los investigadores en el mismo servidor del phishing. Con esto nosotros podemos guardarlos y comenzar a estudiar los correos que están detrás de estos scams.

Llegando un poco más allá

Gracias a que contamos con más de 100 detecciones y que guardamos las configuraciones utilizadas, tenemos bastante información de los sitios y de los correos de notificación de los ciberdelincuentes que están detrás de ellos.

Entonces, podemos sacar una estadística de en cuantos de estos scams ha participado cada uno:

Correo	Scams
akimicash@gmail.com	38
piwinet2018@hotmail.com	20
logosami2022@gmail.com	17
comisionverde1@gmail.com	13
loguitosdechileami@gmail.com	7
badboyblack417@gmail.com	3
chelitotrolo007@gmail.com	3
fertulum@gmail.com	3
loguitosami2022@gmail.com	2
power_dug2@hotmail.com	1
recursitosmail@gmail.com	1

Con estos correos podemos hacer algo más, podemos intentar buscar más información que esté disponible en Internet de ellos, para ello están las técnicas de OSINT (Open Source INTelligence [12]) que nos van a ayudar. Gracias a sitios como https://osintframework.com, y otras herramientas disponibles de manera "gratuita" podemos encontrar más información de algunos de ellos.

Tenemos probables nombres, números de teléfono y redes sociales de algunos, pero por seguridad tanto de ellos como de nosotros, no lo vamos a publicar directamente, pero si lo pondremos a disposición de la policía local.

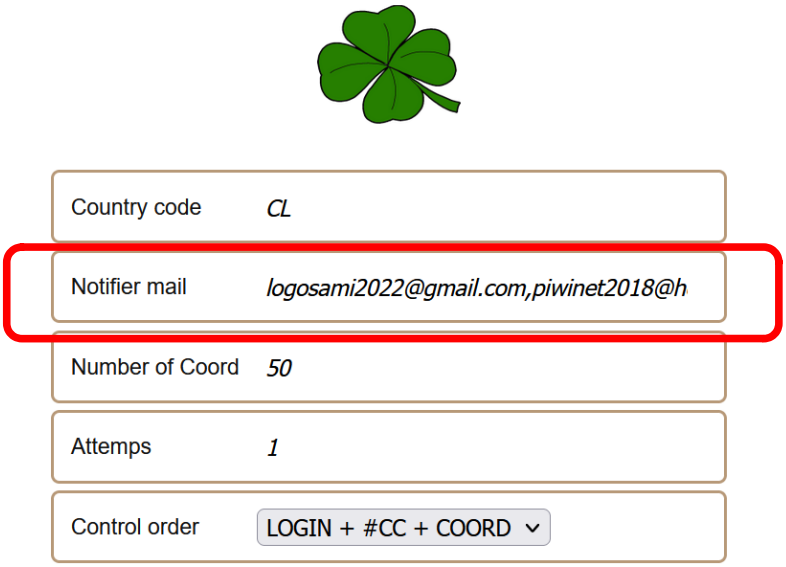
Con esto queremos demostrar que se puede ir un poco más allá, con OSINT y simplemente utilizando la información disponible en internet, podemos dar con información de alguien que podría estar detrás de esto.

Tenemos probables nombres, números de teléfono y redes sociales de algunos.

12 Para una definición más completa de OSINT revisar https://derechodelared.com/osint/

Redes de trabajo

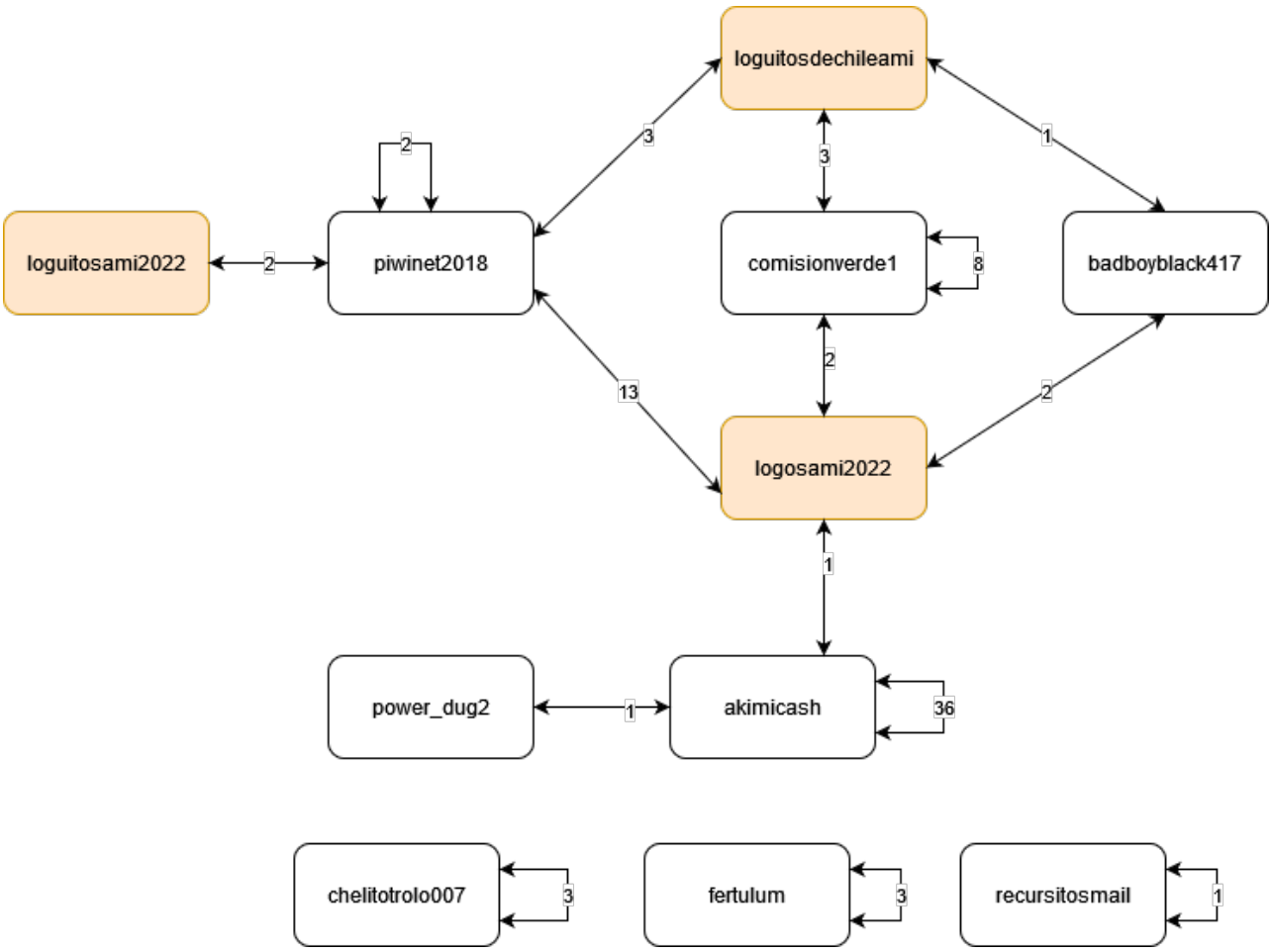
Además, como vimos anteriormente, tenemos en varios casos que se definieron más de un correo como correo de notificación.



En esos casos, podemos asumir que ambos email “trabajan juntos” en el scam. Ya sea que son de la misma persona, o que son de propiedad de 2 (o más) personas, y que están trabajando juntos.

Tenemos una relación visual entre los correos que nos ayuda a ver mejor quienes podrían ser de FC-04

Si buscamos las relaciones entre los correos tenemos el siguiente diagrama:



Con lo anterior tenemos una relación visual entre los correos que nos ayuda a ver mejor quienes se conocen y quienes podrían ser de FC-04.

Con lo anterior, podemos sacar algunas conclusiones:

- Hay actores que les gusta trabajar en conjunto siempre con los mismos email, por ejemplo, la gran mayoría de las veces que hay un scam de logosami2022@gmail.com, va a trabajar con piwinet2018@hotmail.com.
- Hay 3 correos que son bastante similares (logosami2022@gmail.com, loguitosdechileami@gmail.com, loguitosami2022@gmail.com) que siempre trabajan con los mismos otros actores. Probablemente sea el mismo actor por detrás, pero no se puede concluir nada fehacientemente

- El correo akimicash@gmail.com trata de trabajar más solo que con otros aliados, pero las veces que ha trabajado en conjunto con alguien más, es con logosami2022@gmail.com.
- Existen correos que "trabajan solos", principalmente porque no hemos detectado alguna relación con algún otro correo en las configuraciones, pero eso no indica que no se conozcan entre ellos.
- El correo fertulum@gmail.com solo participó en unos pocos sitios de phishing, pero lo interesante es que estos sitios, aunque tenían la intención de clonar la imagen de un banco en Chile tenían definida la geolocalización para IPs en Perú, lo cual lo hace muy sospechoso e inofensivo a la vez.

Por el momento esta es toda la información que podemos entregar para ayudar a los afectados o a las policías para que puedan actuar. A medida que vayamos aumentando la información guardada podemos tener más información de estos ciberdelincuentes.

Palabras finales

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

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

El "problema del Phishing" es algo que requiere una acción constante y hay que llegar un poco más allá para poder buscar el fondo del asunto. Cada institución afectada tiene el derecho de contactarse con empresas como Firebase, Replit, Namecheap o cualquier otra, para identificar y denunciar este tipo de abusos, cosa de que no solo sea el takedown una vez, sino que una investigación más a profundidad en conjunto.

También podemos "ir más allá" utilizando técnicas de OSINT, que son de simple acceso para muchos de los investigadores que hoy estamos trabajando en ciberseguridad, por lo que el llamado es a apoyarnos más en esta cruzada por generar la mayor cantidad de información para la comunidad y que se genere un círculo virtuoso a partir de esa semilla.

Con FINSIN estamos buscando llegar más allá y creemos que con este tipo de plataformas podemos dar más información tanto para las empresas afectadas, para los servicios de takedown, como para las policías que podrían buscar nexos entre estas estafas. Nuestra intención siempre es ayudar a la comunidad en general.

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

Reportes anteriores

- Reporte Septiembre
  - https://finsin.cl/2022/10/10/reporte-mensual-de-phishing-septiembre-2022/
- Reporte Agosto
  - https://finsin.cl/2022/09/11/reporte-mensual-de-phishing-agosto-2022/
- Reporte Julio
  - https://finsin.cl/2022/08/08/reporte-mensual-de-phishing-julio-2022/
- Reporte Junio
  - https://finsin.cl/2022/07/04/reporte-mensual-de-phishing-junio-2022/
- Reporte Mayo
  - https://finsin.cl/2022/06/05/reporte-mensual-de-phishing-mayo-2022/
- Reporte Abril
  - https://finsin.cl/2022/05/09/reporte-mensual-de-phishing-abril-2022/
- Reporte Marzo
  - https://finsin.cl/2022/04/04/reporte-mensual-de-phishing-marzo-2022/
- Reporte Enero-Febrero
  - https://finsin.cl/2022/03/03/reporte-mensual-de-phishing-enero-febrero-2022/