Engaños millonarios desde tu bolsillo

Lucas Paus, Security Researcher

Índice

Resumen Ejecutivo

Este whitepaper presenta detalles de los últimos dos años sobre descubrimientos de ESET Latinoamérica, basados en nuestras investigaciones de los distintos engaños propagados a través de WhatsApp y centrándose específicamente en una campaña, con el fin de ponderar su alcance. Al igual que el Phishing, esta técnica de Ingeniería social o engaño se propaga muy rápidamente, de forma masiva y casi de modo gratuito para el ciberestafador.

Nuevas funcionalidades, como videollamadas, fueron utilizados para conseguir la atención de usuarios desprevenidos. Sin embargo, las falsas encuestas que prometían un voucher al "ganador" fueron las más explotadas. Durante 2016, entre las entidades utilizadas para generar los señuelos de falsos cupones se hallaron nombres como Mc Donalds, Burguer King, Zara, Carrefour, COTO, Wallmart, Mercadona, Ikea y Amazon entre otros. A lo largo de 2017, reconocimos campañas que afectaban a Coca-Cola, Budweiser, Nike y Lancôme, entre otras.

Para dimensionar este tipo de engaño, pudimos comprobar que a partir de una sola campaña engañosa se generaron al menos 22 millones de víctimas. Analizando los países más afectados a nivel mundial, se ubicó a India, México y Brasil en el podio. Dentro de Latinoamérica, se sumaron Argentina, Perú y Ecuador como los países más afectados.

El sistema para monetizar la estafa comprende un conjunto de redirecciones que, dependiendo de la posición geográfica, llevará a cabo distintas acciones, como son la suscripción a números de SMS Premium, la visualización de contenidos diversos, la inscripción a otros servicios o webs de citas o la descarga de aplicaciones. Más allá de la acción, siempre se tratará de publicidad engañosa para llevar a cabo el robo de información.

El futuro quizá esté ligando este tipo de estafas a *exploitkits* para la explotación de vulnerabilidades, instalación de códigos maliciosos o minería de criptomonedas. La educación, combinada con el respaldo de las soluciones de seguridad, son las herramientas principales para proteger a los usuarios frente a estas amenazas, que seguirán presentes por años.

Introducción

Resulta imposible negar el éxito que ciertas aplicaciones de mensajería instantánea, como WhatsApp, han tenido en los últimos años. Durante 2017, las estadísticas indicaron que **más de mil doscientos millones** de personas en todo el mundo hicieron uso de esta aplicación para comunicarse mediante Internet sin que esto suponga un gasto adicional a su factura telefónica.

Ilustración 1 - Falsa actualización de whatsapp

Sin lugar a dudas, este escenario resulta más que tentador para los ciberdelincuentes que día a día generan nuevos señuelos y añaden tecnología para implementar sus fraudes. Actualmente, pueden encontrarse desde estafas con ingeniería social hasta falsas actualizaciones de los repositorios oficiales, como vemos en la imagen anterior.

A lo largo de esta investigación nos proponemos mostrar de qué manera se está aprovechando esta aplicación para incrementar el poder económico de los estafadores a través de los falsos premios y/o encuestas que viajan a través de ella.

Uno de los objetivos principales de los Laboratorios de ESET es alertar y concientizar sobre las distintas estafas digitales que existen y de qué modo éstas se propagan, con el fin de entender qué tipo de amenazas pueden afectar a los usuarios. En consecuencia, comenzamos a analizar diversas campañas que circulan a través de un servicio masivo de mensajería instantánea y que están vinculadas a múltiples países, entidades comerciales de amplia distribución geográfica, distintas monedas e inclusive varios idiomas.

En el presente artículo, profundizaremos en esta ciberestafa, que parece seguir incrementando su número de víctimas y su permanencia en el tiempo. Este tipo de técnicas podrían denominarse como "**Comunicaciones Sociales Potencialmente Inseguras**" (*Potentially Unwanted Social*

Comunication o **PUSC**) y si bien no son códigos maliciosos, exponen al usuario a campañas publicitarias o a peligros mayores, como ser inducidos a la instalación de malware, la explotación de vulnerabilidades, o a ser utilizados a través de la minería de criptomonedas.

Las primeras grandes campañas fueron descubiertas en el año 2015 y a fines de agosto de 2016 alcanzaron su pico máximo, afectando a **millones de usuarios desprevenidos** que hicieron clic sobre un enlace engañoso, el cual prometía un voucher de premio.

Consideraciones

Análisis de múltiples campañas

Durante estos últimos meses, si bien dentro de la aplicación de mensajería se han realizado varias mejoras de seguridad, como por ejemplo el cifrado de la comunicación de lado a lado, no se han adoptado de forma proactiva mecanismos para evitar distintos fraudes, muchas veces vinculados a la Ingeniería social. En consecuencia, se da lugar a un territorio muy fértil para los ciberdelincuentes, que, al tratarse particularmente de este canal, explotan tres características fundamentales:

1) **Masividad del uso**: la cantidad de usuarios está completamente relacionada a la cantidad de posibles víctimas.
2) **Falta de protección contra Ingeniería Social**, así como de un canal para reportar enlaces maliciosos que se estén compartiendo de manera viral.
3) **Gratuidad** en el envío de los mensajes, de manera masiva.

Si bien existe una gran cantidad de estafas circulando por medio de este servicio de mensajería, es posible dividirlas en dos clases principales según su tipo de señuelo:

a. Aquellas que ofrecen una nueva funcionalidad (Videollamadas, espionaje de contactos, nuevos emoticones, modificación de características del diseño).

Ilustración 2 - Estafa de whatsapp, 1er tipo

b. Aquellas que ofrecen un premio (cupones de tiendas, aerolíneas, aniversarios).

Ilustración 3 - Estafas de whatspp, tipo 2

A lo largo de la presente investigación nos proponemos profundizar en este segundo grupo, desvelando las tecnologías de Ingeniería Social que hay detrás y dando respuesta a distintos interrogantes.

El comienzo

De modo general, el engaño se inicia con la llegada de un mensaje dentro de un grupo de WhatsApp o de algún contacto que asegura ya haber obtenido el premio.

Una pequeña imagen o ícono acompañado de pocas líneas de texto suele ser un señuelo eficaz a la hora de atraer víctimas. Aunque el enlace que aparece en la pequeña descripción adjunta del mensaje pareciera dirigir al sitio oficial de la entidad afectada, el verdadero enlace dentro del texto del mensaje delata la estafa, redirigiendo a los usuarios a una página que no guarda relación alguna con las compañías en cuestión. Las siguientes imágenes, son solo algunos ejemplos de engaños que afectaron a empresas multinacionales:

Ilustración 4 - Falsos cupones de Burger King y McDonalds

Desde tiendas de comida rápida, mercados, cines y grandes cadenas textiles hasta compañías aéreas han sido utilizados como señuelo:

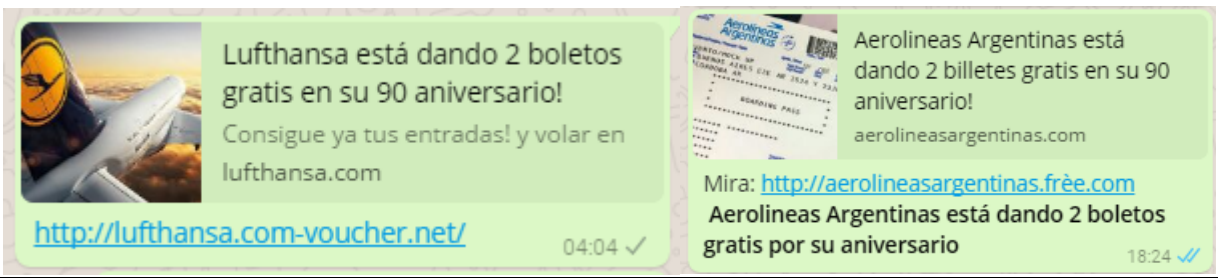


Ilustración 5 - Falso Aniversario de Lufthansa y Aerolíneas Argentinas

Por supuesto no todos los casos se presentan con el mismo diseño, algunos simplemente comparten un enlace de modo más básico, pero el hecho de no ser tan vistosos no implica que no sean funcionales,

como se muestra en los dos ejemplos siguientes, donde se han utilizado acortadores gratuitos y poco llamativos, (resultarán esenciales más adelante en la investigación para analizar y entender el comportamiento de este tipo de campañas):

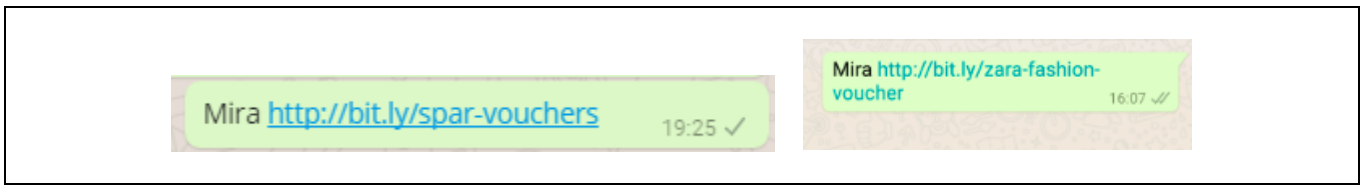


Ilustración 6 - Falsos voucher de Spar y Zara

Fechas especiales, como fin de año, Navidad o Pascuas también son aprovechadas por estas campañas para presentar un señuelo más creíble, ofreciendo grandes promociones en nombre de las entidades afectadas:

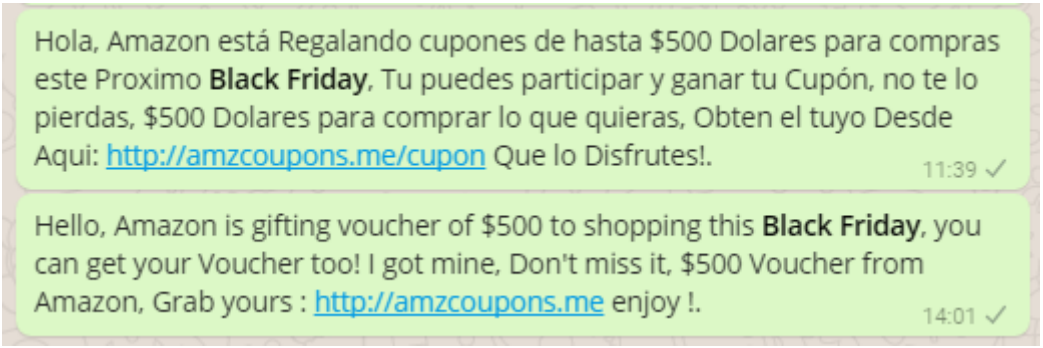


Ilustración 7- Falsos cupones/bonos de Coto y Amazon

Plantillas de Propagación

El éxito de la viralizacion de estas campañas se debe en parte a dos de sus comportamientos, como son la automatización en la personalización y la meticulosa Ingeniería Social aplicada. Resulta útil aclarar que el procedimiento para realizar este tipo de estafas no varía entre unas y otras, simplemente se modifican ciertos detalles, como el nombre de la marca o empresa utilizada como anzuelo, para aumentar la credibilidad de la misma y, en consecuencia, su éxito.

Los desarrolladores de la estafa en cuestión lograron generar un señuelo muy creíble a través del uso del protocolo HTTP y sus bondades. Cuando una víctima hace clic sobre el enlace, se genera una petición al servidor. Ésta contiene información básica sobre el navegador en distintas líneas, formando parte de los llamados headers o cabeceras, fundamentales para que se produzca una correcta comunicación. Dentro se incluyen diferentes campos, por ejemplo: tipo de navegador que realiza la petición, idioma, versión, etc... Estos campos serán fundamentales a la hora de generar una respuesta desde el servidor, que llegará de distintos modos según la petición. Así, podrá cambiarse de forma automática el idioma o la moneda, con el fin de que la víctima no despierte sospechas. Además, dependiendo de la rentabilidad de los servicios asociados y de la facilidad para monetizar la maniobra en cada país, la víctima será redirigida de modo transparente.

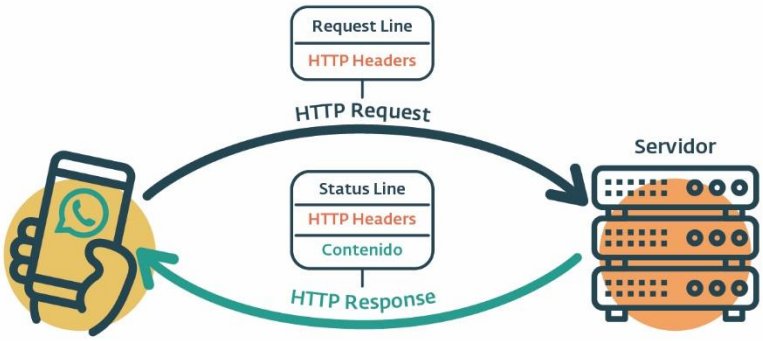


Ilustración 8 - Proceso de redirección de la estafa

Cuando analizamos cada una de las estafas, encontramos servicios asociados que generan el comportamiento de redireccionamiento. Si tomamos una de las primeras campañas, podremos dividirla en varias fases, que acaban por cerrar el flujo de la ciberestafa:

- Recepción del mensaje fraudulento.
- Primer redireccionamiento mediante Bitly.com, que servirá para esconder un dominio que no guarda relación alguna con la entidad afectada y para realizar un control estadístico.

- Segundo redireccionamiento a un servicio de tracking que, dependiendo de la geolocalización, tipo de navegador e idioma, actuará de la manera adecuada para hacer la campaña más rentable para el estafador.
- La víctima reenvía el mensaje a sus contactos conocidos.
- Una vez compartido con la cantidad de contactos necesaria, es inducido a la suscripción de distintos servicios.

Este circuito podrá visualizarse en el siguiente gráfico:

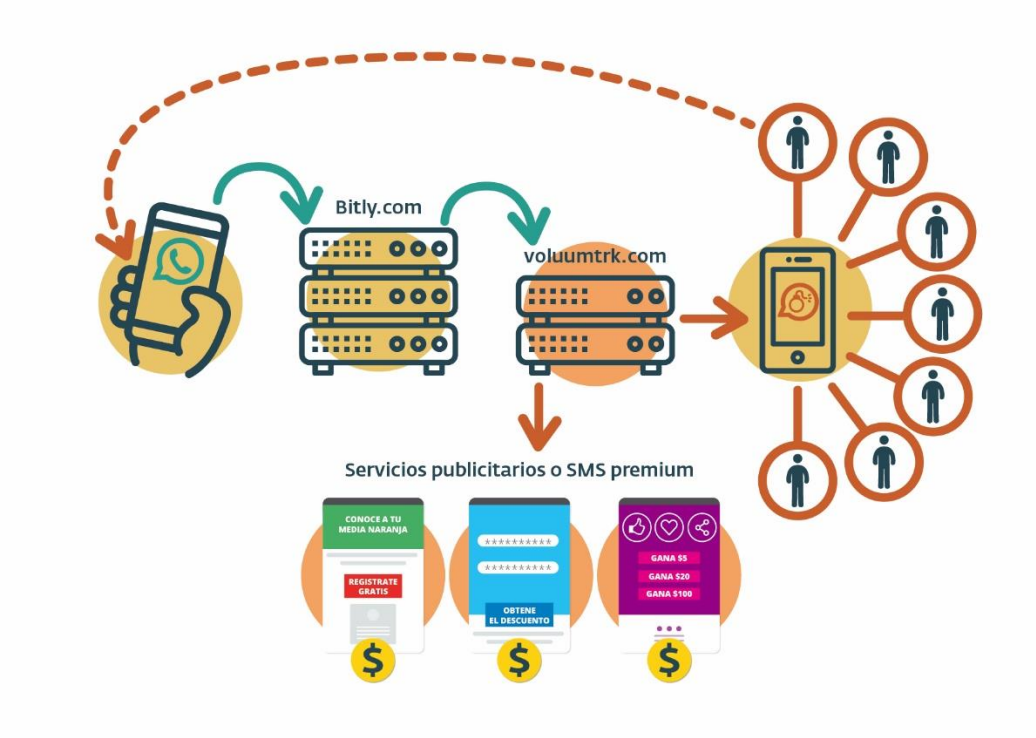


Ilustración 9 - Circuito de la ciberestafa

Al analizar la comunicación inicial de una campaña específica, en este caso afectando a la empresa de supermercados COTO, podemos ver tanto las peticiones como las respuestas, así como distintas variables, entre ellas ubicación, moneda o lenguaje, en sus campos:

http://coto.giftcar**-***o.com/?country=AR&city=cordoba&language=es&voluumdata=vid..00000003-de28-4d0d-8000-000000000000__vpid..a8c12000-6b9b-11e5-8774-e3d14faba2f3__caid..854002ff-15c7-4c2c-9d32-301c95c09ce7__rt..R__lid..cb23e0f7-26e5-4a0a-bf14-3ee1f6cd3cb8__oid1..cd1c3175-7b4d-49ac-bc58-78f365d197fa__var1..ws__rd..__aid..__sid..&s1=ws

Ilustración 10 - Campos de la estafa a nombre de Coto

Usuarios desprevenidos

La Ingeniería Social, es decir el arte de disuadir a las personas con algún fin, es uno de los puntos fuertes en este tipo de fraudes. Si se lo complementa con técnicas de geolocalización, los ciberdelincuentes lograrán una amplia propagación, convirtiendo a un usuario distraído no solo en víctima, sino también en cómplice de la difusión de la estafa.

Adicionalmente, el usuario que recibe el mensaje suele ser advertido de que su contacto de confianza ha recibido el premio, que solo quedan algunos pocos disponibles, y que la promoción terminará en solo unos minutos. Demás está decir que el fin de estas premisas es erradicar cualquier tipo de sospecha que pueda tener un usuario respecto a la veracidad de las ofertas presentadas.

Cabe aclarar también que aquí se utiliza el nombre de reconocidas tiendas o marcas de confianza, que normalmente no están ligadas a fraudes digitales ni manejan información sensible, como es el caso de entidades financieras, que históricamente se han visto afectadas por códigos maliciosos y sitios de phishing. Así, los ciberdelincuentes intentan despistar a los usuarios hogareños, explotando la relación de confianza hacia esas marcas que nunca antes fueron afectadas ni se vieron vinculadas con incidentes de seguridad.

Todas las caras de la amenaza

1° Plantilla: Cupón de descuento

Entidades Afectadas

Pueden mencionarse grandes tiendas, presentes en múltiples países, que fueron elegidas de forma minuciosa según su grado de popularidad y su conveniente distribución, en la mayor cantidad de naciones como sea posible. A continuación veremos algunas de ellas:

IKEA

Es una corporación multinacional de origen sueco, dedicada a la fabricación y venta minorista de muebles y objetos para el hogar, radicada en los Países Bajos (Holanda) que cuenta con 238 tiendas distribuidas en 44 países. Ha sido la protagonista de una de las principales campañas, debido a que únicamente para la parte inicial de la estafa, se hizo uso de cinco subdominios asociados que involucran al nombre e imagen de la empresa:

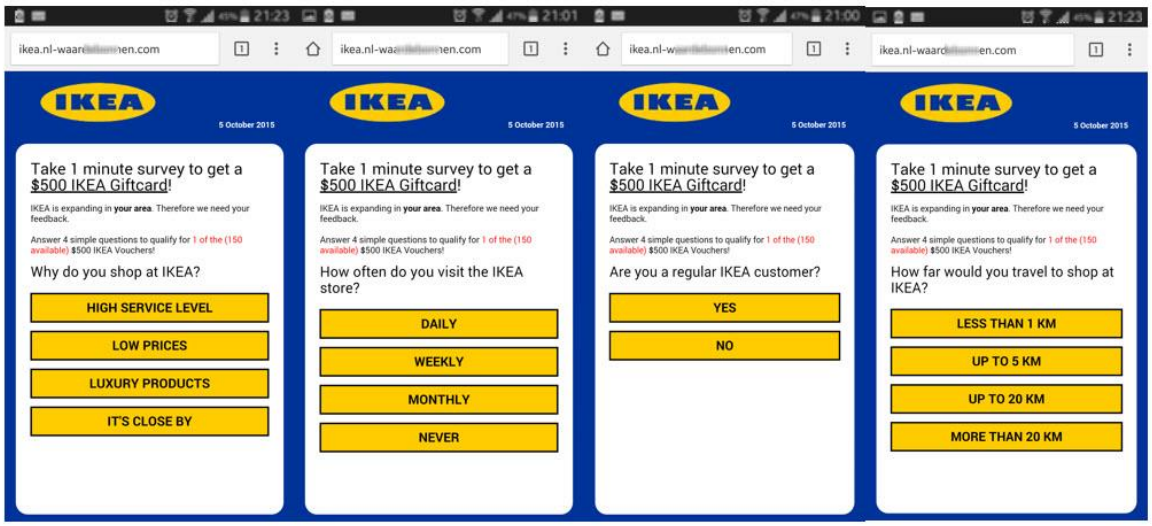


Ilustración 11 - Estafa a nombre de IKEA

H&M

Es otra cadena sueca, dedicada al negocio de indumentaria, que opera en 44 países desde Europa, Asia, África y América. La amplia distribución internacional de sus tiendas representa un gran atractivo para los ciberdelincuentes. En este caso, se utilizaron dos dominios, como veremos a continuación:

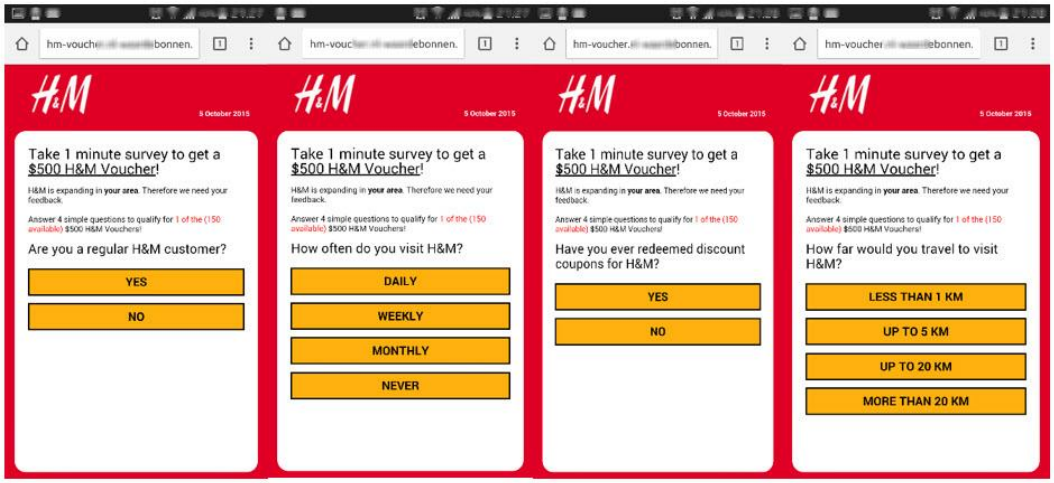


Ilustración 12 - Estafa a nombre de H&M

Zara

Una cadena de tiendas de venta de indumentaria conocida a nivel mundial, con base en España, y de gran repercusión en Latinoamérica y Europa. Las siguientes imágenes corresponden a la estafa que la tuvieron como protagonista:

Ilustración 13 - Estafa a nombre de ZARA

KFC (Kentucky Fried Chicken)

Es una tienda de comidas fundada en Estados Unidos con más de 18 mil restaurantes distribuidos en 144 países. Las siguientes imágenes corresponden a la versión del engaño que utiliza el nombre de KFC:

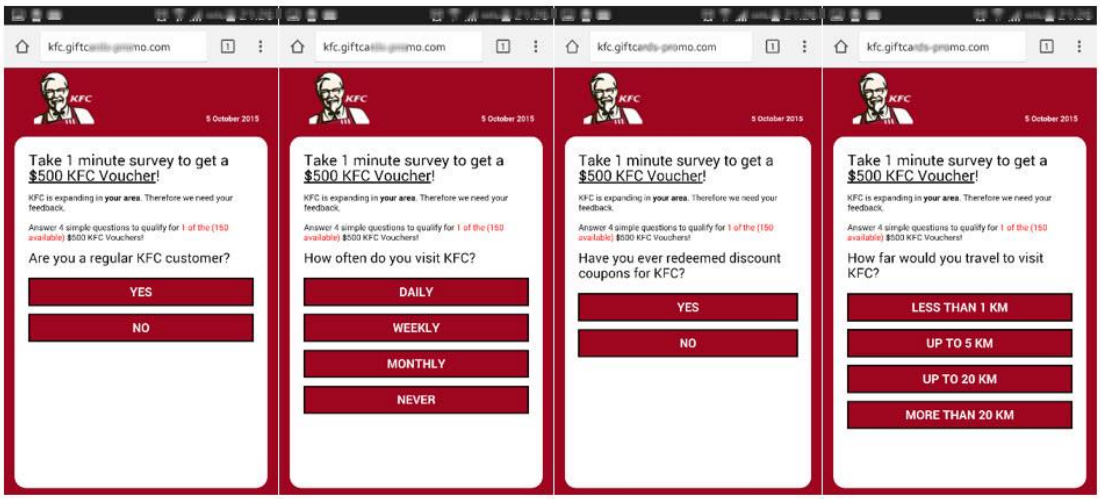


Ilustración 14 - Estafa a nombre de KFC

Otras tiendas de comida rápida con miles de sucursales por el mundo, entre las que destacan las gigantes estadounidenses McDonald's y Burger King, también fueron utilizadas con la misma plantilla:

Ilustración 15 - Estafa a nombre de McDonalds

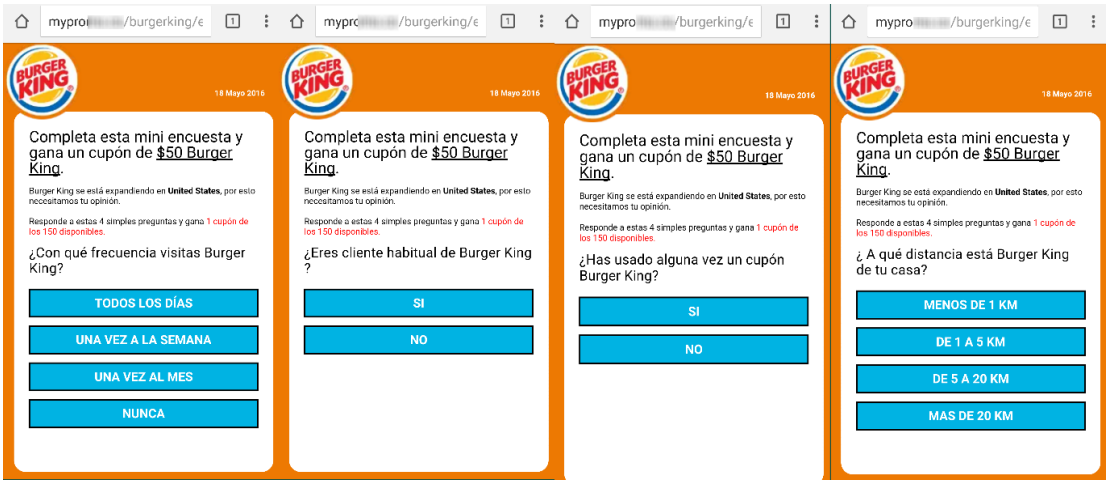


Ilustración 16 - Estafa a nombre de Burger King

SPAR

Esta mega cadena de supermercados originaria de los Países Bajos cuenta con más de 20 mil sucursales en 35 países, y así luce el engaño que utiliza su nombre.

No obstante, los ciberdelincuentes buscaron un grado mayor de penetración a nivel mundial, motivo por el cual en países donde no se encuentran presentes estas tiendas, intentaron hallar reemplazos que les permitieran obtener la misma masividad de alcance. Por ejemplo, en Argentina utilizaron la cadena de supermercados **COTO**, que posee alrededor de 120 sucursales en todo el país.

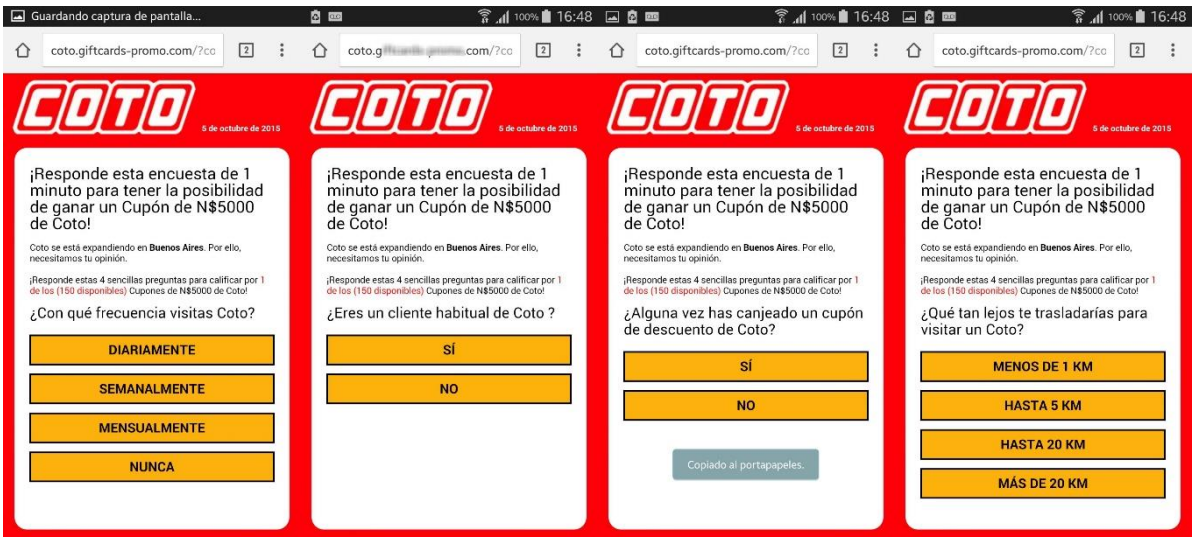


Ilustración 17 - Estafa a nombre de COTO

7-Eleven

Otra tienda utilizada para este fraude, radicada en Estados Unidos, que cuenta con 52 mil establecimientos en 16 países, especializada en la venta de consumos básicos y muy presente en América del Norte y Asia.

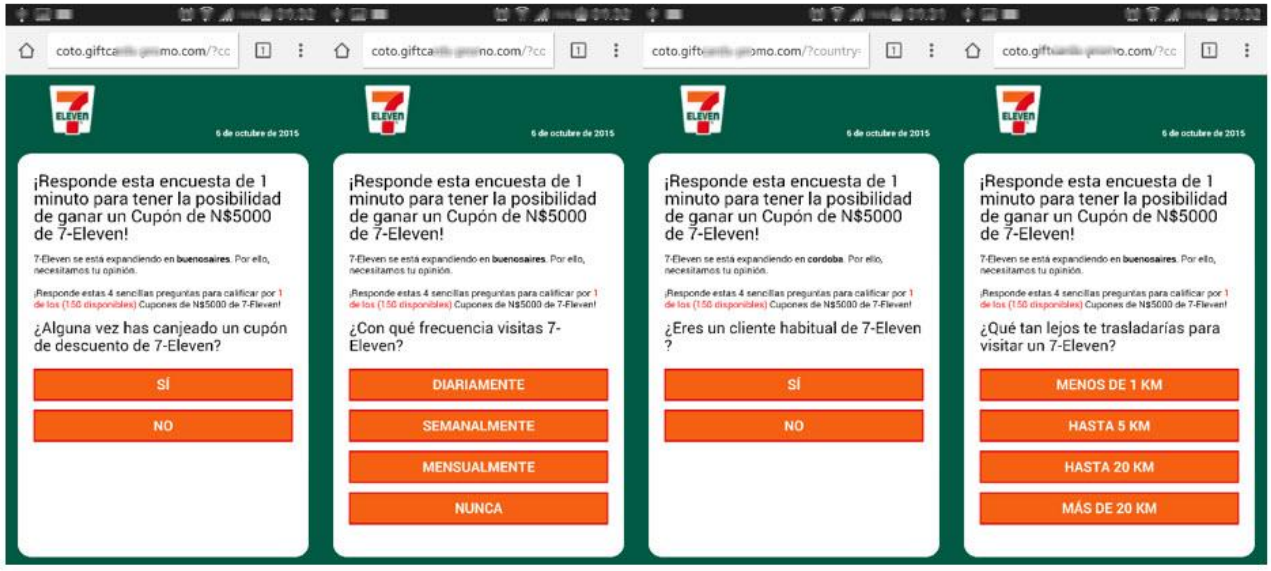


Ilustración 18 - Estafa a nombre de 7-Eleven

Wallmart

Otra empresa del mismo rubro afectada fue la cadena de supermercados Wallmart, que posee 11 mil tiendas en 28 países.

Ilustración 18 - Estafa a nombre de Wallmart

DIA

Sus **tiendas** están presentes en varios países de Latinoamérica, como Argentina y Brasil, y naturalmente en España, donde nació la cadena y cuenta con 4941 tiendas. Pero también tiene una fuerte presencia en China, con 381 tiendas, siendo una de las razones por las que esta estafa se halla en varios idiomas. Como vemos en las siguientes capturas, la misma campaña se distribuye en inglés, alemán, portugués e italiano, entre otros.

Ilustración 20 - Estafa a nombre de Dia

Y como éstas, son muchas otras las tiendas y cadenas del rubro de las que se aprovechan estas campañas, entre ellas, la española Mercadona, y Lidl, de origen alemán.

2° Plantilla: Aniversarios y vuelos gratis

Las compañías áreas tampoco quedaron exentas de ser utilizadas para este tipo de estafas. A continuación, algunos ejemplos:

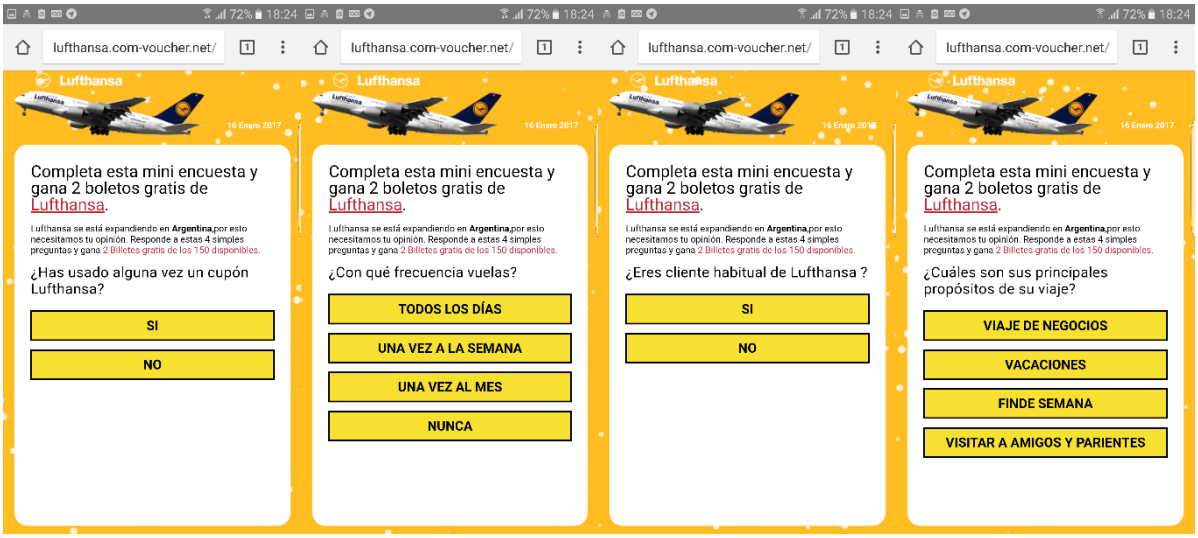


Ilustración 19 - Estafa a nombre de Lufthansa

Al analizar estas campañas, vemos como intenta camuflarse el dominio realmente utilizado por las estafas mediante el uso de un subdominio, que será el nombre de la entidad tomada como señuelo, como podremos visualizar en las siguientes imágenes:

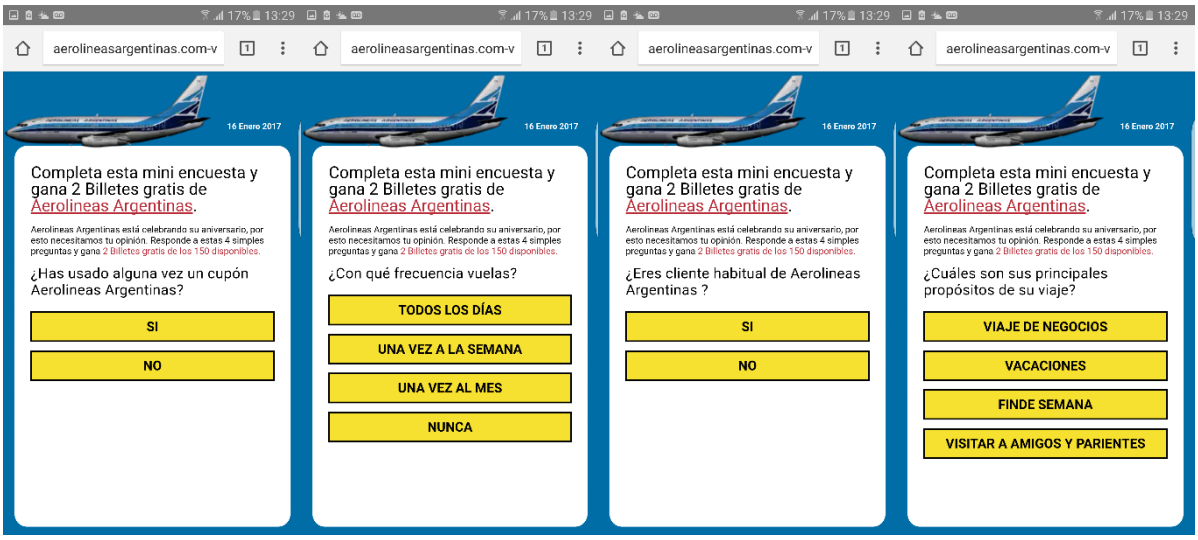


Ilustración 20 - Estafa a nombre de Aerolíneas Argentinas

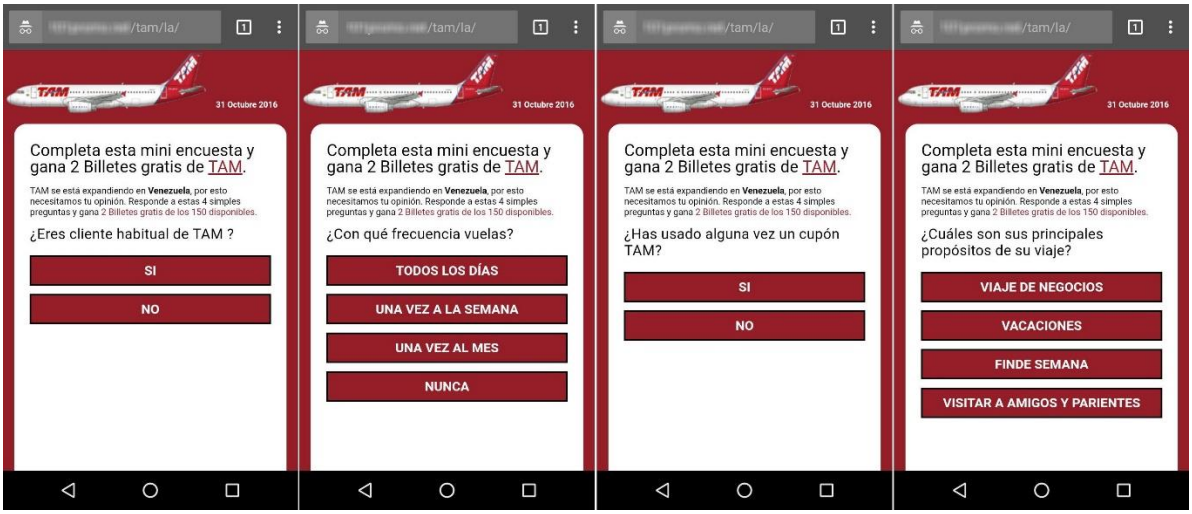


Ilustración 21 - Estafa a nombre de TAM

3° Plantilla: SuperBono

Quizá por un decrecimiento en la performance de usuarios que hacen clic en relación a los usuarios que realmente se convierten en víctima de las campañas anteriores, los estafadores han notado que aun los usuarios más distraídos no caen dos veces en el mismo engaño con tanta facilidad. Naturalmente, esto podría haber impulsado la aparición de una nueva familia de señuelos, ligados a la famosa **rueda de la fortuna**. Además, otras bandas de estafadores podrían utilizar un nuevo engaño o campaña al conocer las ganancias económicas de sus antecesores. De cualquier modo, si bien a grandes rasgos las últimas plantillas cumplen la misma función, las cuatro preguntas estándar que se ven en las imágenes anteriores han migrado.

Existe entonces, siempre manteniendo el objetivo presentado en un comienzo de la estafa, un método a través del cual el usuario podría “probar su suerte“ haciendo girar una rueda de la fortuna. En todos los casos, ocurrirá que al primer intento de juego de la víctima, la suerte no estará de su lado, pero el sistema le permitirá una segunda chance. Y en esta ocasión, la segunda es la vencida, ya que entonces el usuario resultará ganador. Entonces terminará la etapa de Ingeniería Social, y comenzarán a actuar los distintos redireccionamientos, como en el resto de las plantillas.

Ilustración 22 - Estafa a nombre de COTO

4° Plantilla: Búsqueda de empleo

Inicialmente, este tipo de campaña se difundió por Europa, afectando, entre otros, a España, con el señuelo de trabajar por un interesante sueldo en Marcadona. En la actualidad, esto se está propagando por distintos países de Latinoamérica, como Argentina, a través la firma COTO como principal entidad afectada. Estas campañas difieren de las anteriores, inclusive en el mensaje inicial que recibe la víctima, como vemos en las siguientes capturas:

Ilustración 23 - Estafa a nombre de Mercadona – parte 1

Cuando el usuario hace clic sobre el enlace, es redireccionado a las siguientes pantallas, para responder 3 sencillas preguntas y poder finalmente “asegurar su vacante“:

Ilustración 24 - Estafa a nombre de Mercadona – parte 2

En el caso de la tienda COTO, podemos ver a simple vista la similitud respecto de la estafa anterior:

Ilustración 258 - Estafa similar a nombre de COTO

Edad, experiencia y disponibilidad parecen ser las características de este señuelo, que curiosamente solo permite una respuesta correcta.

5° Plantilla: El estafador oportunista

Según la época del año, los usuarios son más permeables a recibir determinadas ofertas altamente ofensivas que llaman su atención. Justamente en esos días suelen aparecer distintas campañas que intentan camuflarse con tan llamativas ofertas. Un claro ejemplo afectó a Amazon, la gran tienda de e-commerce, en plena época de rebajas y ofertas como es la de Black Friday, previa a la temporada navideña:

Ilustración 269 - Estafa a nombre de Amazon durante Black Friday

Las pascuas, fiestas de origen religioso en las que suele regalarse huevos de chocolate, también fueron utilizadas de señuelo, como podemos ver en la siguiente imagen:

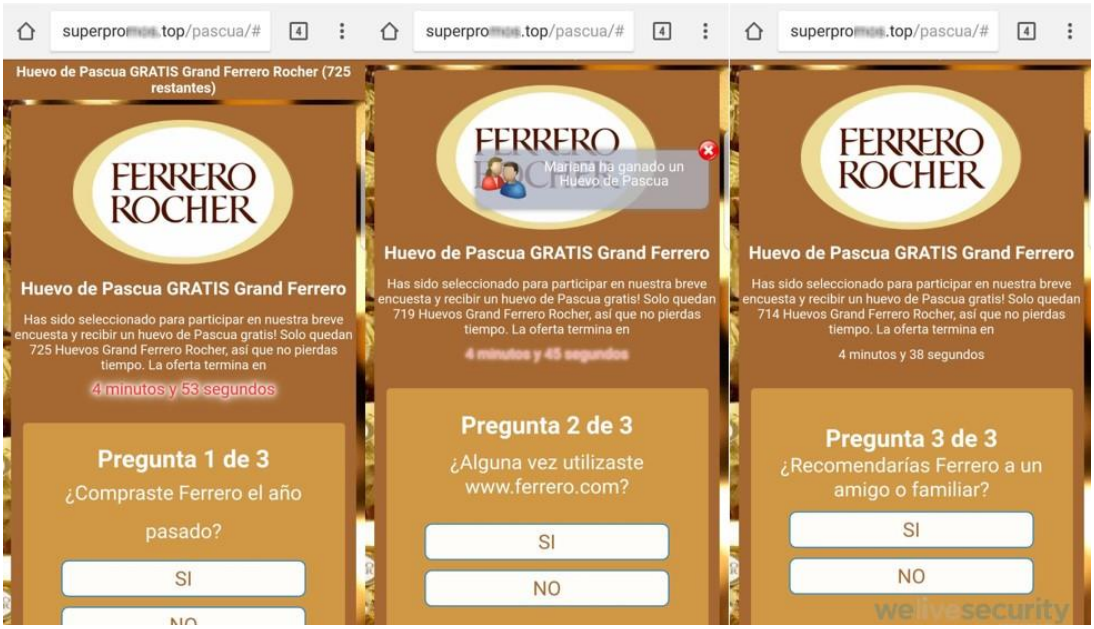


Ilustración 27 - Estafa a nombre de Ferrero Rocher durante Pascuas

Sin lugar a dudas, los ciberestafadores no dejarán de generar nuevas plantillas ligadas a sucesos del momento que llamen la atención de víctimas desprevenidas. Por este motivo, no debería sorprendernos ver constantes innovaciones fraudulentas, ya sean cupones, encuestas, premios o propuestas laborales, entre otras.

Atravesando barreras de contactos telefónicos

Mediante el uso de nuevas funcionalidades, como el WhatsApp Web, los desarrolladores de las campañas maliciosas comenzaron a emplear recursos que inducen a las víctimas que hayan ingresado desde su PC a propagar la estafa a través de Facebook, la mayor red social a nivel mundial. Al analizar el código fuente vemos el siguiente método utilizado:

```
window.exitUrl = "http://adsmdi      /track/5/nbwupleb-xdbd-xpam-a4gz-ilw0i0iwbi9c";
window.countryCode = "BR";
window.countryName = "Brazil";
window.offerUrl = "http://adsmd      /track/5/nbwupleb-xdbd-xpam-a4gz-ilw0i0iwbi9c";
window.shareUrl = "http://myprc      /burgerking/";
window.shareType = "whatsapp";
window.shareUrlFB = "https://www.facebook.com/";
window.shareCount = 10;
```

Ilustración 28 - Código fuente de estafa de Whatsapp a propagarse vía Facebook

Al cambiar la óptica y mirarlo desde la red social, podremos ver que en varios perfiles se viralizaron noticias como las que se ven en la imagen siguiente, ligada a este tipo de estafas:

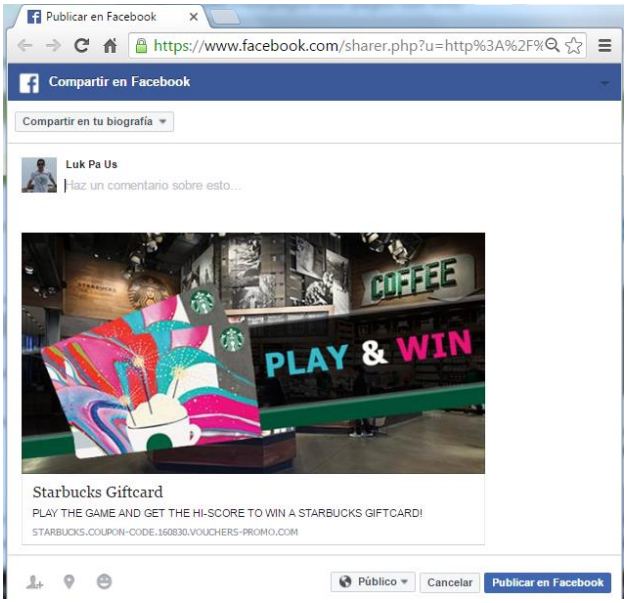


Ilustración 29 - Misma estafa, vista desde la plantilla de Facebook

Este tipo de propagación parece ser de gran conveniencia para el ciberdelincuente, dado que con una simple publicación se llega a hacer visible el mensaje señuelo para miles de víctimas y de manera más rápida que por WhatsApp. Por el contrario, podemos observar que, a diferencia de WhatsApp, en esta red social sí es posible reportar un enlace malicioso. Dicho punto es crucial, ya que naturalmente este tipo de enlace solo permanece funcional por un par de horas, dándose de baja tras sucesivas denuncias de otros usuarios que comprobaron el engaño y lo notificaron. El mensaje es eliminado e informado a la víctima del siguiente modo:

Ilustración 30 - Mensaje enviado a la víctima tras varias denuncias a la publicación

Cifras, performance y peculiaridades

El comportamiento de personalización automática fue detectado en varias campañas con el fin de alcanzar una mayor cantidad de víctimas. A través de esta técnica, los usuarios no pueden detectar ninguna sospecha que pueda originarse por no tener el idioma del país o región afectada, dado que este tipo de trampa es capaz de detectar el idioma correcto de la víctima en potencia y redireccionarse automáticamente de forma transparente, para que el visitante no despierte sospecha alguna. Estos son algunos ejemplos:

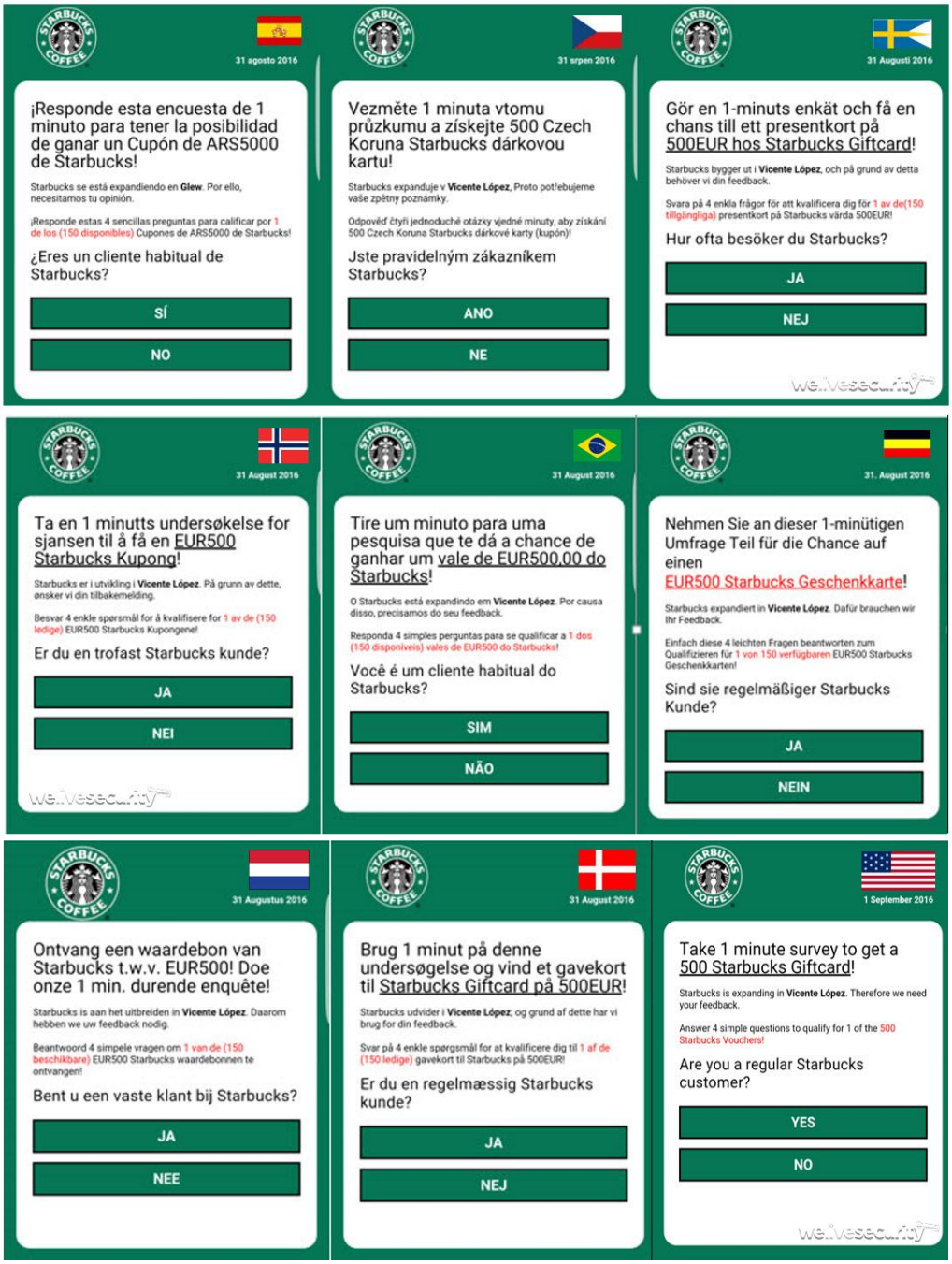


Ilustración 31- Estafa a nombre de Starbucks en diversos idiomas

Reforzando el señuelo

Además de inducir al usuario a propagar la campaña rápidamente con la excusa de una limitada disponibilidad de premios, son más las técnicas de Ingeniería Social compartidas en estas campañas.

En ocasiones, el primer mensaje que recibe la víctima muestra una línea de texto en la que advierte al receptor que un tercero (alguien en quien confía y tiene entre sus contactos) recibió el premio. No obstante, los ciberestafadores también generan una interfaz que haría creer que muchos usuarios agradecen haber sido ganadores a través de Facebook. La siguiente imagen proviene de una estafa que utilizaba la marca de **Spotify** con su servicio Premium como señuelo principal.

Ilustración 32 - Estafa a nombre de Spotify compartida en Facebook

Al analizar el código fuente, podemos ver que se trata de un script en java, que nada tiene que ver con Facebook, y que las imágenes son importadas de otro sitio con dominio ibb.co:

```
<div class="like-imgs">
    <div><img src="https://image.ibb.co/cngVyb/img2.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/hKAZPG/btn.png" width="16"
    <div><img src="https://image.ibb.co/fLaerw/img1.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/k4SEPG/love.png" width="16'
    <div><img src="https://image.ibb.co/mBj5Ww/img3.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/hKAZPG/btn.png" width="16"
    <div><img src="https://image.ibb.co/c4f14G/img4.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/hKAZPG/btn.png" width="16"
    <div><img src="https://image.ibb.co/eRQqyb/img8.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/hKAZPG/btn.png" width="16"
    <div><img src="https://image.ibb.co/c4f14G/img4.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/hKAZPG/btn.png" width="16"
    <div><img src="https://image.ibb.co/dQSQWw/img9.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/k4SEPG/love.png" width="16'
    <div><img src="https://image.ibb.co/eu0OJb/img5.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/k4SEPG/love.png" width="16'
    <div><img src="https://image.ibb.co/cVu5Ww/img7.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/hKAZPG/btn.png" width="16"
    <div><img src="https://image.ibb.co/fJ7g4G/img6.jpg" width="32" height="32" /><img class="reaction-img" src="https://image.ibb.co/k4SEPG/love.png" width="16'
```

Ilustración 336 - Código fuente de la estafa de Spotify

¿Es sencillo detectar la estafa para un usuario hogareño?

En ocasiones se agregan múltiples capas de camuflaje, haciendo más compleja la detección de mensajería apócrifa. Si bien muchos usuarios con conocimientos técnicos podrían a simple vista sospechar de la veracidad de estas campañas, quizá un usuario común cuente con menos herramientas. En el mejor de los casos, esto podría validarse si el sitio al que se es redirigido tiene un certificado de sitio seguro (HTTPS). Esta campaña podría pasar desapercibida, al menos en primera instancia, ya que utiliza un certificado válido, como se ve en el siguiente caso que también afectó a la empresa Spotify:

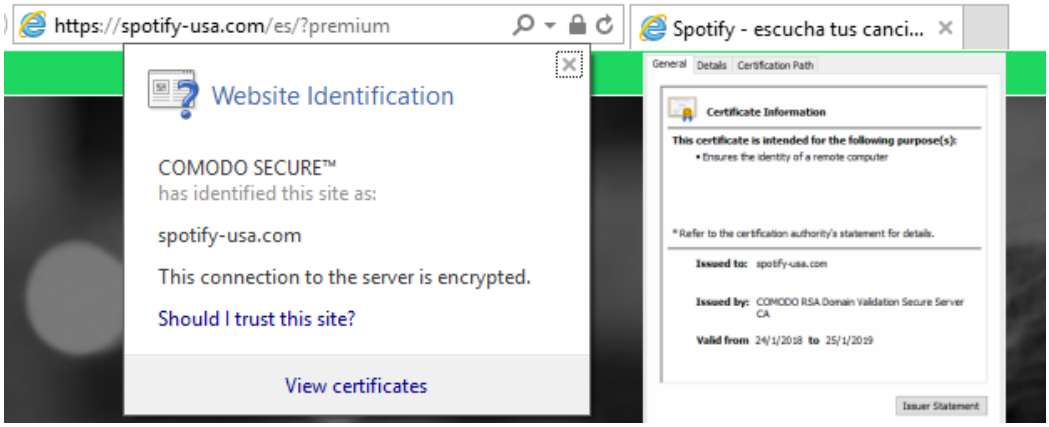


Ilustración 34 - Estafa a nombre de Spotify con certificado válido

Como se observa en la imagen anterior, el sitio al que los usuarios eran redireccionados constaba de un certificado válido. Sin embargo, no se trataba del sitio oficial del servicio, como podremos diferenciar en la siguiente captura.

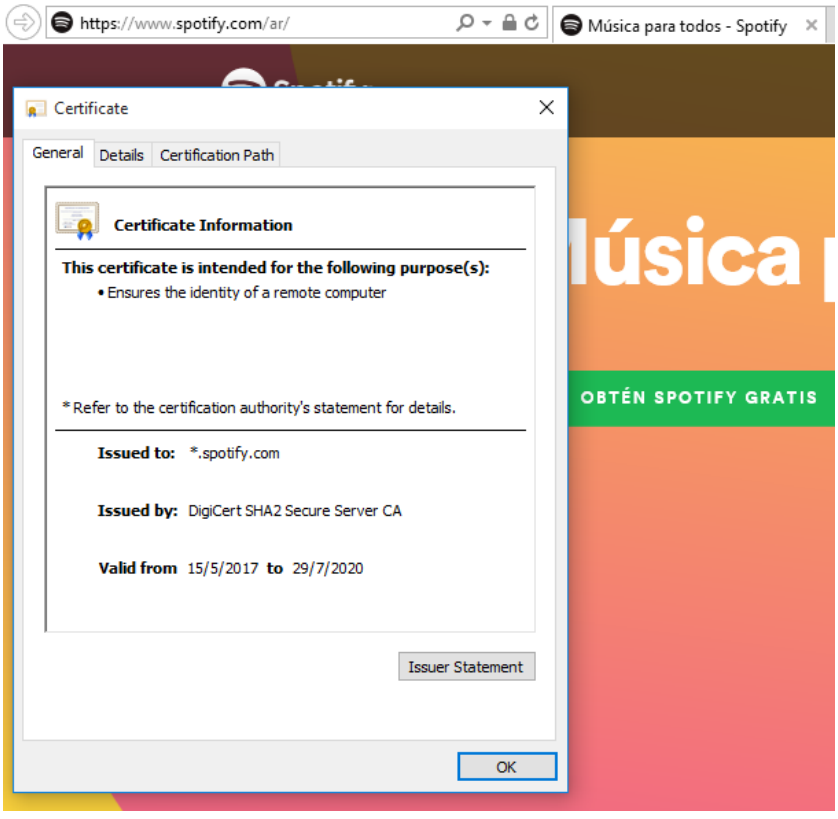


Ilustración 35 - Sitio oficial de Spotify

Una campaña similar afectó a otro servicio multimedia muy utilizado, como es Netflix. La misma tenía la capacidad de afectar a múltiples países al estar diseñada en varios idiomas, y, a su vez, utilizaba un dominio similar con uso de un certificado válido (HTTPS).

Ilustración 369 - Estafa a nombre de Netflix con certifiacdo válido

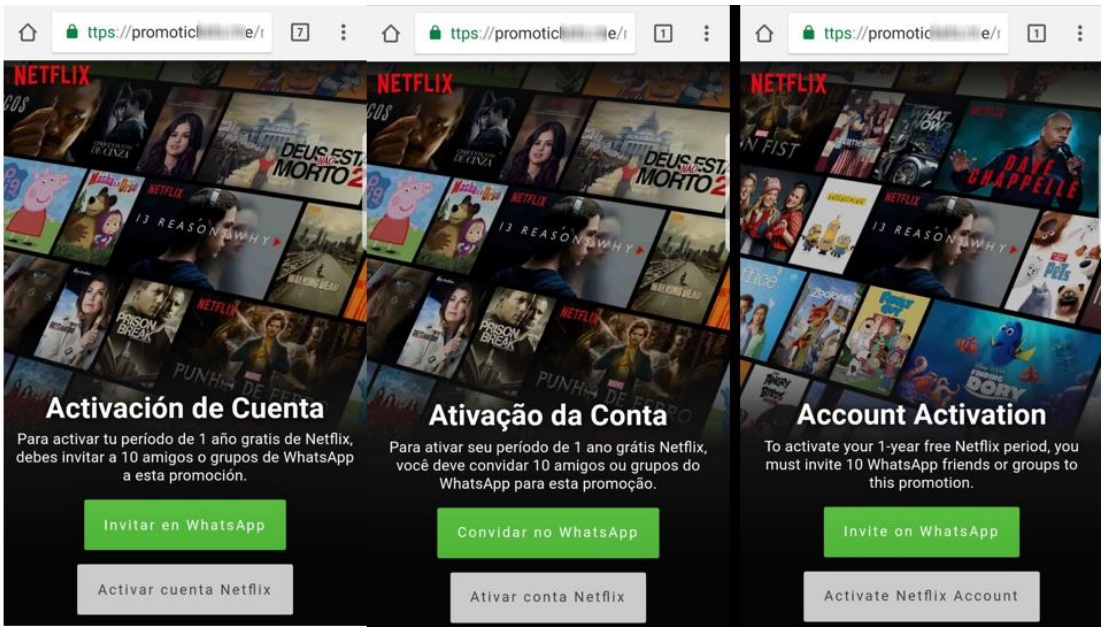


Ilustración 370 - Misma estafa disponible en varios idiomas

Si bien estas campañas han sido detectadas y se ha alertado sobre ellas, presentan un grado de dificultad mayor para un usuario hogareño al intentar descubrir su veracidad. Pero ahí no termina todo, las campañas pueden tener incluso una capa extra de camuflaje.

Ataques homográficos

Si todavía consideras que todas estas campañas son fácilmente detectables, este caso puede que te haga reflexionar al respecto. Para entender la campaña es necesario conocer estas técnicas desde un aspecto teórico. Los ataques homográficos utilizan caracteres diferentes a los del alfabeto que usamos cotidianamente, pero que son muy similares visualmente. Es decir, explotando la utilización de caracteres Unicode en otros idiomas, como griego o ruso, pueden encontrarse caracteres similares o, muchas veces, iguales a los que utilizamos habitualmente en las URL. Por tal motivo, este recurso está siendo utilizado por los ciberestafadores. A continuación, presentamos un ejemplo:

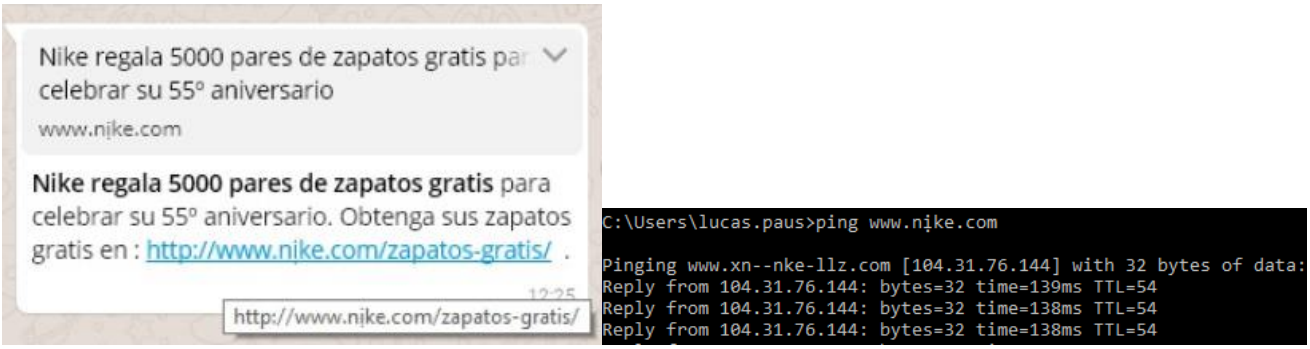


Ilustración 38 - Estafa a nombre de Nike que explota el uso de caracteres Unicode

A simple vista, parece ser que el dominio se tratara de **http://nike.com**, cuando en realidad el dominio es **http://www.xn--nke-llz.com**, codificado según el navegador de manera tal que se asemeje al dominio señuelo: de manera sencilla, con una simple comprobación de su ping, se visualiza el nombre real del dominio.

Luego de que la víctima haga clic en el enlace, será redirigida a otro sitio con un subdominio similar al real y sometido entonces a las preguntas habituales, como en las campañas anteriores, visible en la siguiente imagen:

Ilustración 39 - Clásica estafa a nombre de Nike

¿Cuántos usuarios distraídos caen producto del engaño?

La respuesta a este gran interrogante dependerá de cada campaña, de cuántos señuelos o trucos técnicos se hayan incorporado en ellas. La gestión de este tipo de incidentes se vuelve un tema controversial a la hora de identificar a los responsables de solicitar la baja de estos sitios fraudulentos. Quizá este sea uno de los motivos por los cuales los engaños en cuestión pueden permanecer en línea por un tiempo prolongado.

Por supuesto, cuanto mayor sea el tiempo en línea, mayor será la ventana para que más usuarios desprevenidos se conviertan en víctimas de estos engaños. Al analizar y comparar la cantidad de enlaces compartidos a través de las estadísticas públicas de los acortadores utilizados, podemos reflexionar acerca de los resultados encontrados.

En primera instancia analizaremos dos campañas idénticas, que usaron la misma entidad afectada (**Mc Donalds**), con el señuelo de un falso cupón. El primer caso registró **535000** clics, afectando principalmente a Argentina, Uruguay y Paraguay.

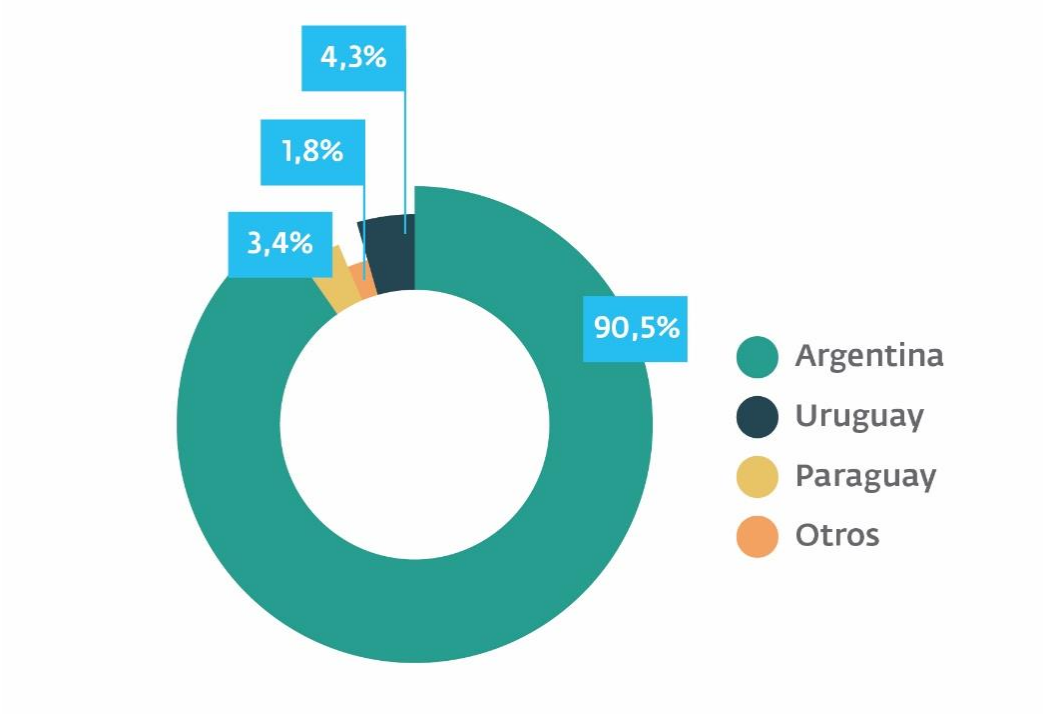


Ilustración 403 – Caso 1: estafa de Mc Donalds

Unos tres meses después de que el dominio de la estafa se diera de baja, se generó una segunda campaña, con aún más usuarios afectados, llegando casi a los **660000**. En esta ocasión fueron Panamá y Paraguay quienes completaron el podio, por detrás de Argentina.

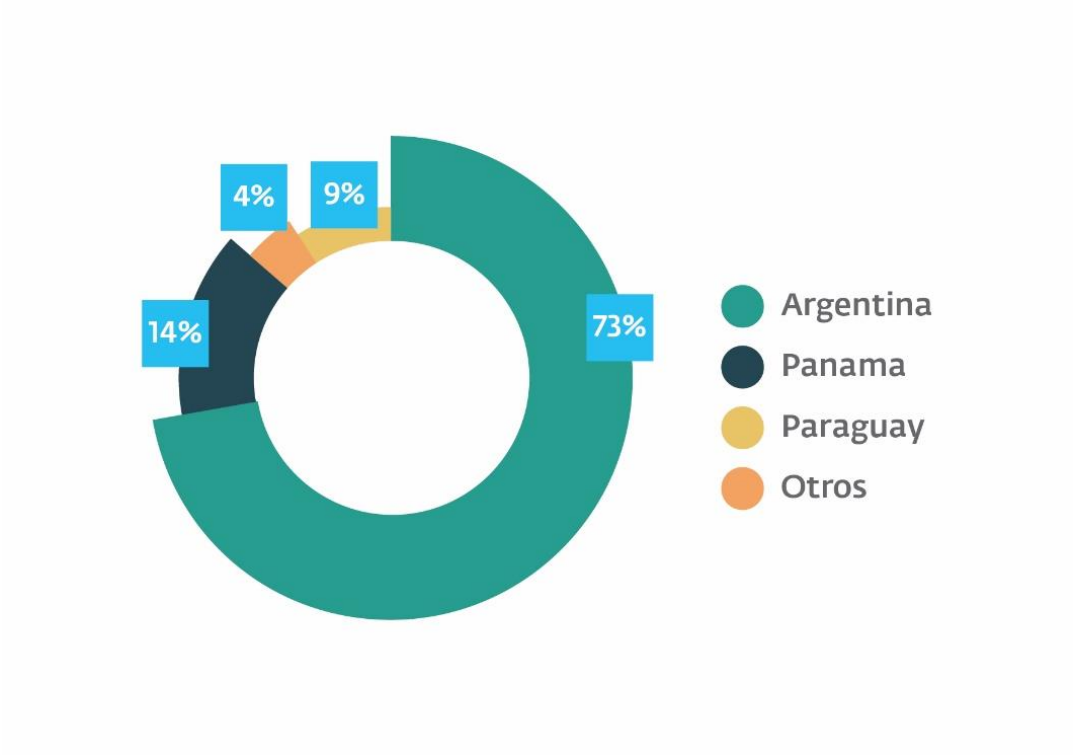


Ilustración 414 – Caso 2: misma estafa de Mc Donalds, pero en una nueva campaña

Con este ejemplo, podemos ser testigos del crecimiento que tuvo este tipo de amenazas a lo largo de un período relativamente corto de tiempo.

Al tiempo de estudiar estas campañas, se detectó que un mismo dominio estaba siendo utilizado para la misma estafa, pero con señuelos que afectaban a distintas entidades. Al recopilar la información obtenida de las distintas estadísticas, hallamos una suma cercana a los **22 millones de clics** relacionadas a este dominio, distribuidos a nivel mundial.

En el siguiente cuadro, se muestran las entidades utilizadas y la cantidad de clics obtenidos dentro de los tres países más relevantes en cuanto a sus víctimas.

ENTIDADES	Clics	Países			
H&M	2.464.127	Malasia (25%)	India (16%)	Chile (9%)	Otros (51%)
		615235	3954685	217405	1265950
Carrefour	5.636.792	EAU (29%)	Indonesia (27%)	Egipto (10%)	Otros (34%)
		1661050	1528950	540485	1906350
Starbucks	5.231.248	México (67%)	Perú (18%)	EE.UU (6%)	Otros (9%)
		3529703	957985	304735	438825
KFC	462.428	Ecuador (69%)	Jamaica (16%)	EE.UU (4%)	Otros (12%)
		319075	73988	18497	55491,36
IKEA	266.273	Israel (43%)	Irlanda (9%)	Arabia Saudita (6%)	Otros (42%)
		114647	23112	14919	113595
Spar	1.726.226	Sudáfrica (85%)	Namibia (4%)	Botswana (4%)	Otros (7%)
		1473570	71439	63244	117973
Zara	6.118.046	Brasil (33%)	España (27%)	Argentina (18%)	Otros (30%)
		2018955	1651872	1101248	1835413,8
Lidl	10.075	Croacia (39%)	Rep. Checa (20%)	Bélgica (13%)	Otros (28%)
		3923	1989	1296	2867
Jumbo	68.702	Holanda (98%)	Bélgica (1%)	Alemania (1%)	Otros (1%)
		67408	284	224	786

Ilustración 42 - Distribución mundial del N° de clics y las entidades afectadas

Cuando miramos el panorama de Latinoamérica, hallamos a los siguientes países como los más afectados:

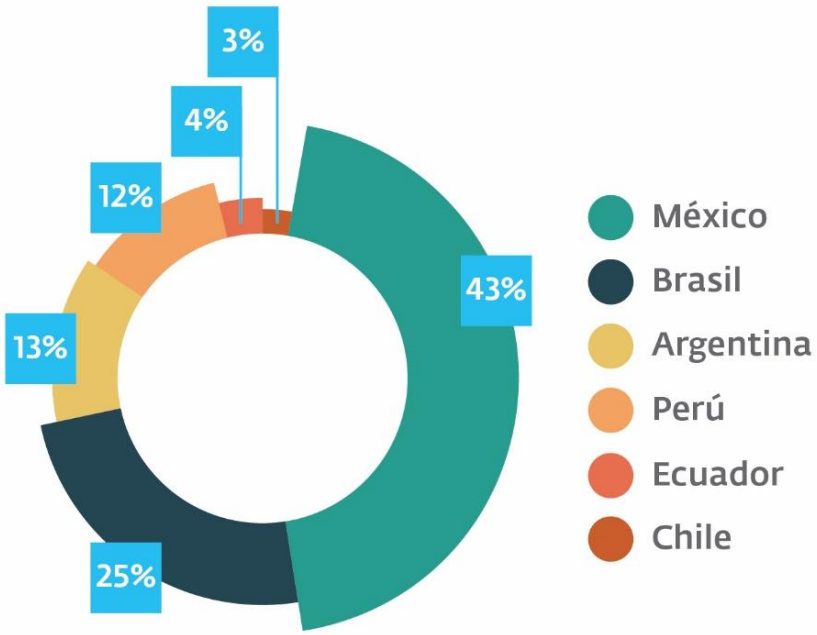


Ilustración 43 - Distribución mundial del N° de clics y las entidades afectadas

¿Qué servicios se utilizan detrás de la estafa?

Podría uno pensar que los ciberdelincuentes utilizan distintos recursos de programación para generar la inteligencia que hay detrás de los engaños. Sin embargo, vemos que en muchas ocasiones se contratan servicios de redireccionamiento, normalmente utilizados en casos ligados a campañas publicitarias. Junto con la evolución de estas campañas, observamos como los cibercriminales migraron del uso de servicios gratuitos y mayormente limitados, como **bitly**, a otros servicios pagos, con muchas más funcionalidades de web analytics, como las que posee el servicio de **Volum**, entre otros. A través de técnicas de tracking o rastreo de pixeles, y utilizando páginas intermediarias entre saltos, los cibercriminales logran almacenar toda la información para luego direccionar al visitante según se haya parametrizado con anterioridad. De este modo, se puede conocer el país en que se encuentra el usuario y a qué sitio será más rentable dirigirlo.

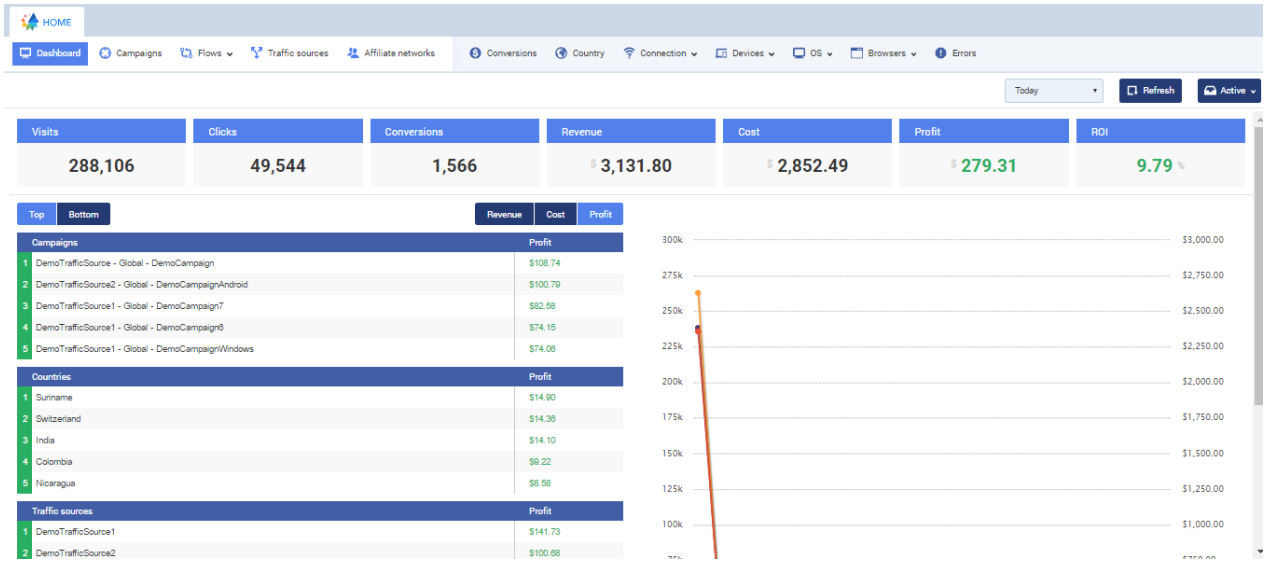
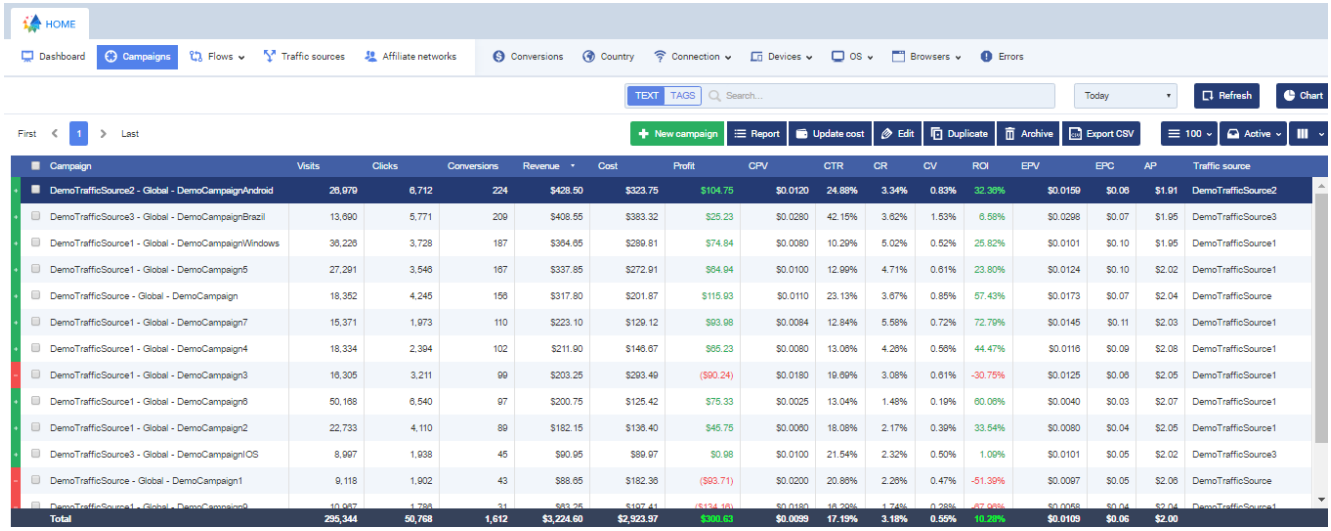


Ilustración 44 - Información de los dispositivos desde los que los usuarios acceden a la estafa

Como vemos en la captura de pantalla, también se puede observar información más precisa de los dispositivos, como la versión del navegador o el sistema operativo que utilizan. Este tipo de funcionalidad, si bien en la actualidad no es aprovechada con un propósito, podría en futuro complementarse con la explotación de vulnerabilidades propias del sistema operativo detectado.

Por otro lado, desde un punto de vista del gerenciamiento de ganancias, estos paneles revelan, luego de configurarse correctamente, las estadísticas por país y cantidad de clics, entre otros datos.



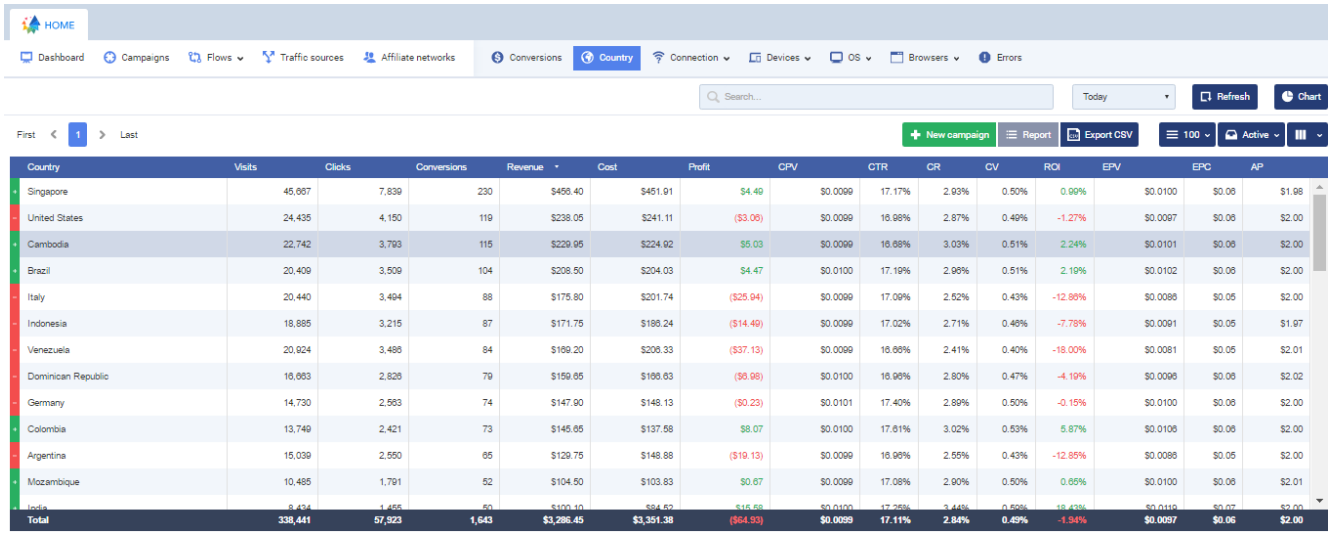


Ilustración 45 - Estadísticas por país y cantidad de clics

Asimismo, se distinguirá el tipo de dispositivo, ya sea una tablet, un computador de escritorio o un teléfono móvil, e incluso el tipo de conexión que utilizan, como vemos en la siguiente imagen:

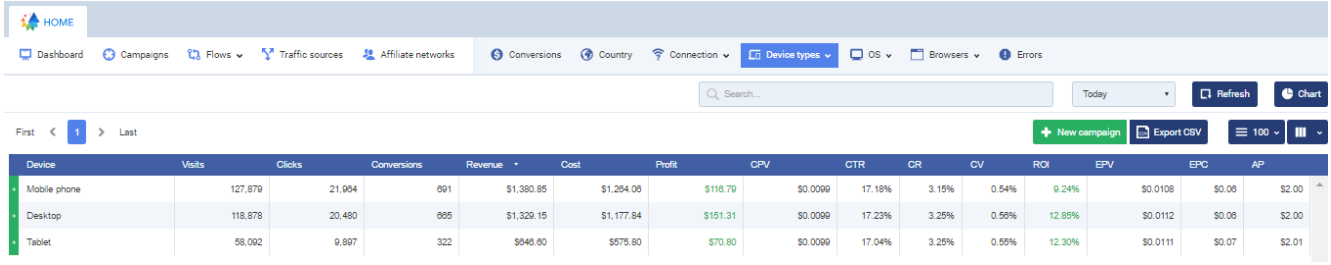
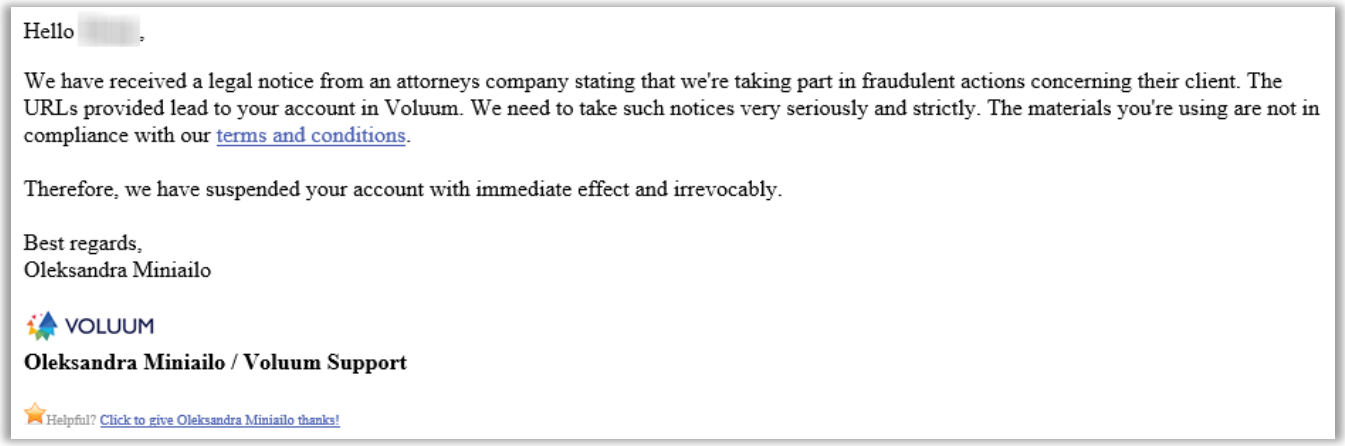


Ilustración 46 - Distinción según tipo de dispositivo

Desde los laboratorios de ESET Latinoamérica detectamos y reportamos estos sitios de estafas. En este caso, la campaña afectaba a más de diez empresas multinacionales. Luego de reportarlo, y gracias a la cooperación de las entidades involucradas, recibimos este correo en forma de copia, confirmando la baja de los sitios que permitían el re-direccionamiento y, en consecuencia, los fraudes fueron detenidos.



Hello [redacted],

We have received a legal notice from an attorneys company stating that we're taking part in fraudulent actions concerning their client. The URLs provided lead to your account in Voluum. We need to take such notices very seriously and strictly. The materials you're using are not in compliance with our terms and conditions.

Therefore, we have suspended your account with immediate effect and irrevocably.

Best regards,
Oleksandra Miniailo

VOLUUM

Oleksandra Miniailo / Voluum Support

Helpful? Click to give Oleksandra Miniailo thanks!

Ilustración 47 - Correo recibido por ESET confirmando la baja de los sitios que permitían el redireccionamiento

La monetización de la estafa

Sin lugar a dudas, el objetivo de este tipo de campañas maliciosas es recolectar la mayor cantidad de información y dinero posible, lamentablemente a costas de las víctimas y los usuarios desprevenidos.

Así como el mercado regula en muchos casos los precios de los productos por la oferta y demanda, la geolocalización en estas estafas funcionará de modo similar. Es decir, dependiendo del país donde se encuentre la víctima, el mercado cambia, y la estafa se elegirá en función del camino más rentable para el ciberdelincuente. De este modo, el usuario desprevenido habrá atravesado distintos caminos al culminar la etapa de Ingeniera Social. Estos son solo algunos:

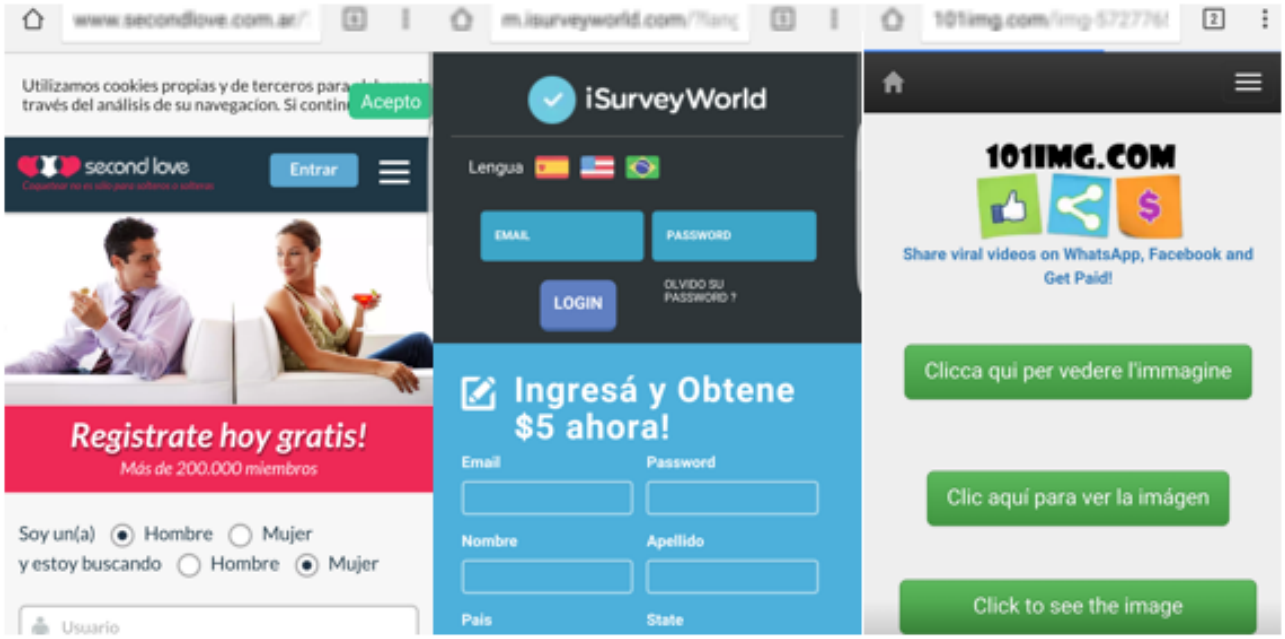


Ilustración 48 - Distintas etapas del trabajo de Ingeniería Social de la estafa

Es importante entender que, en la mayor parte de los casos, estos servicios no están al tanto del engaño y la manera en que llegan los usuarios a inscribirse a estos sitios, lo que significa que el servicio en sí no es malicioso, sino que, en realidad, el mecanismo por el cual los usuarios son inducidos a los registros conlleva una actividad maliciosa.

SMS Premium

Quizá sea este uno de los métodos más comunes y a la vez más rentables en esta clase de estafas. En ciertos países de Latinoamérica, son los operadores de red los grandes beneficiados con las suscripciones de SMS Premium, quedándose con una ganancia en torno al 50% del precio que pagan los usuarios desprevenidos al anotarse en estos servicios. El resto de la ganancia es dirigida hacia el estafador. En países como Argentina, el costo de la recepción de estos mensajes ronda el dólar o dólar y medio por persona que lo recibe. Quizá a primera vista pareciera no ser mucho, sin embargo, si se tiene en cuenta el volumen de gente que cae en el engaño, estos números se multiplican y crecen muy rápidamente.

Ilustración 49 - Condiciones del servicio detalladas en el apartado de 'Términos y Condiciones'

De manera casi automática, el usuario pasa por alto las notas de términos y condiciones donde se explica que el mismo se está suscribiendo a estos servicios, que tendrá una renovación automática del mismo e incluso cuáles son los costos de la recepción de mensajes.

Encuestas

Otra de las técnicas utilizadas para capitalizar el engaño, es hacer que el usuario víctima se involucre con aplicaciones que realizan encuestas. Este tipo de servicios paga una comisión de dinero a los reclutadores por cada persona suscrita. En la página anterior, podemos ver una captura de este tipo de servicios.

Videos e imágenes

Otro tipo de campaña cuya monetización no parece tan simple de detectar a simple vista, está vinculado a las vistas o visitas de determinadas imágenes de publicidad. En la siguiente tabla podemos visualizar como, dependiendo del país en donde se encuentre el visitante, éste pertenecerá a distintos grupos (A, B, C, D) y su valor por visita variará.

Earnings per 1000 views	
Group A	$8.00
Group B	$5.00
Group C	$1.00
Group D	$0.01

- A: United Kingdom, Australia, New Zeland, Canada.
- B: Italy, Netherlands, Denmark, Austria, Spain, Belgium, Switzerland, France, Germany, Luxembourg, Norway, Portugal, Greece, Sweden.
- C: Brazil, Russia, Japan, Cyprus, Estonia, Latvia, Slovakia, Hungary, Israel, Lithuania, Poland, Czech Republic.
- D: All Others Country.

Ilustración 50 - Ganancias por países cada 1000 visitas

Esta es una de las principales cuestiones por las cuales no todas las campañas son iguales entre sí, ya que, sin lugar a dudas, los ciberdelincuentes buscan el modo más sencillo para hacer sus redirecciones lo más rentable posibles.

Sitios publicitarios

Otro modo de generar ganancias es redirigiendo a los usuarios a determinados sitios con nuevas ofertas o suscripciones de naturaleza completamente distinta, y, una vez más, por cada visita el ciberdelincuente hará de su trampa algo rentable.

Ilustración 51 - Estafas escondidas en publicidades que captan la atención del usuario

Instalación de aplicaciones

En ocasiones, las redirecciones pueden también inducir al usuario a instalar aplicaciones que no necesariamente son maliciosas, pero sí podrán monetizarse mediante la afiliación de los usuarios a las mismas.

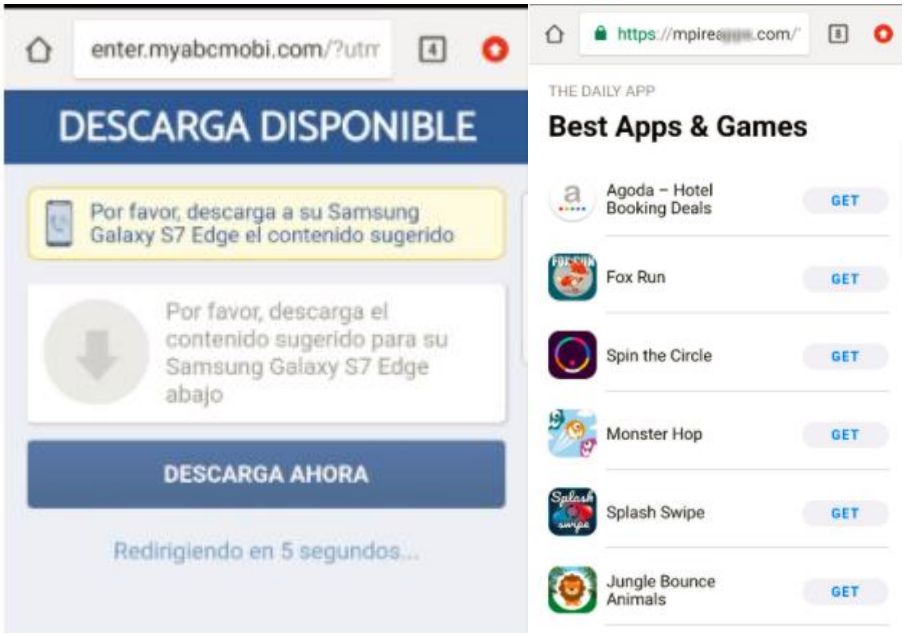


Ilustración 52 - Estafas que inducen a la instalación de aplicaciones

Rogueware o scareware

Poca memoria disponible, un virus que daña la batería o una nueva actualización requerida, son algunos de los señuelos utilizados para inducir al usuario a ingresar los datos de su tarjeta de crédito. Con le excusa de reparar el dispositivo, en ocasiones sus datos serán utilizados para realizar un cargo y "solucionar el problema", o podrían también ser robados para venderlos o hacer compras fraudulentas. A continuación, algunos ejemplos:

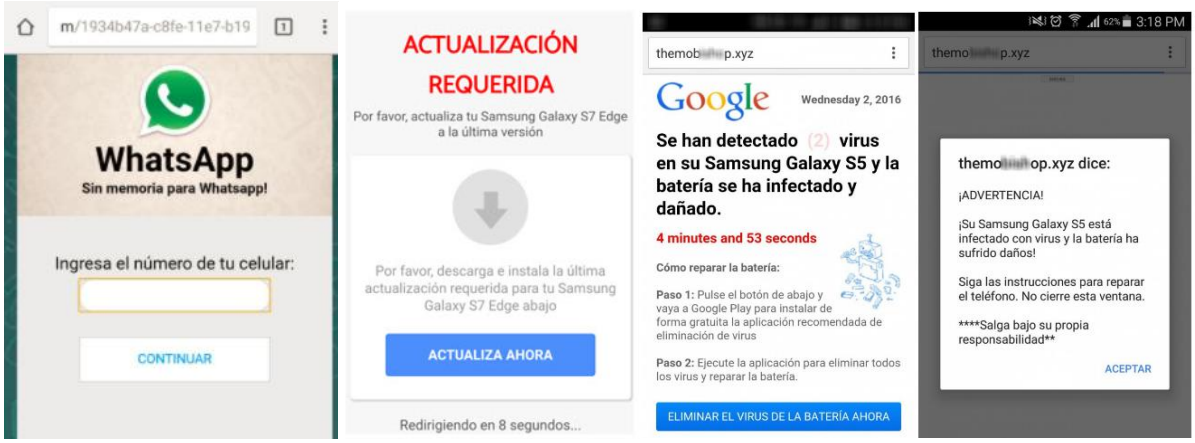


Ilustración 53 - Más ejemplos de señuelos que buscan engañar a los usuarios

Tomando conciencia

Sería muy extraño que este tipo de engaño no comience a fusionarse con otras campañas maliciosas. Puede observarse este comportamiento en múltiples códigos maliciosos que incorporan nuevas funcionalidades, entre ellos el **Ransomware**, que inicialmente solo cifraba la información para pedir un rescate, y en la actualidad también es capaz de robar credenciales y/o criptomonedas. Otro ejemplo lo constituyen las **botnets**, que inicialmente se utilizaban para espiar y enviar spam y que hoy en día pueden también ser utilizadas para minar criptomonedas o generar DDoS.

Desde este punto de vista, no debería extrañarnos ver estas campañas ligadas a exploitkits o rutinas Java maliciosas apuntando a diversos dispositivos o smartphones con el fin de acceder a cierta información, cifrarla o incluso utilizar la computadora de la víctima para ejecutar robos o minado.

Sin embargo, haciendo un análisis algo más positivo, debemos resaltar que la educación respecto a este tipo de amenaza ha avanzado, y si bien queda camino por recorrer, son muchos los usuarios que ya reconocen estas estafas. A su vez, las soluciones de seguridad continúan mejorando día a día en su detección temprana.

Protección y concientización

Los diversos e innovadores señuelos, junto con la naturaleza humana, son un cóctel peligroso, del cual, en la mayoría de los casos, sacará provecho el estafador. Tanto nuevos usuarios como aquellos más experimentados pueden caer en este tipo de trampa si se usa el señuelo correcto. Por este motivo, resulta fundamental trabajar sobre la educación y concientización, buscando que se genere al menos la duda en el usuario respecto de la veracidad de dichas estafas.

Independientemente de si se trata de un usuario avezado en el mundo de la Seguridad Informática, o bien se haya capacitado y concientizado sobre las amenazas más frecuentes, será vital tener en consideración el uso de múltiples capas de seguridad para mitigar más riesgos.

En este sentido, ya sea en computadores o dispositivos móviles, las soluciones de seguridad tendrán un rol protagónico, dado que, a través de sus módulos de detección, generarán alertas de seguridad en esos casos en que el usuario no haya reparado en la dirección del enlace al que sería dirigido.

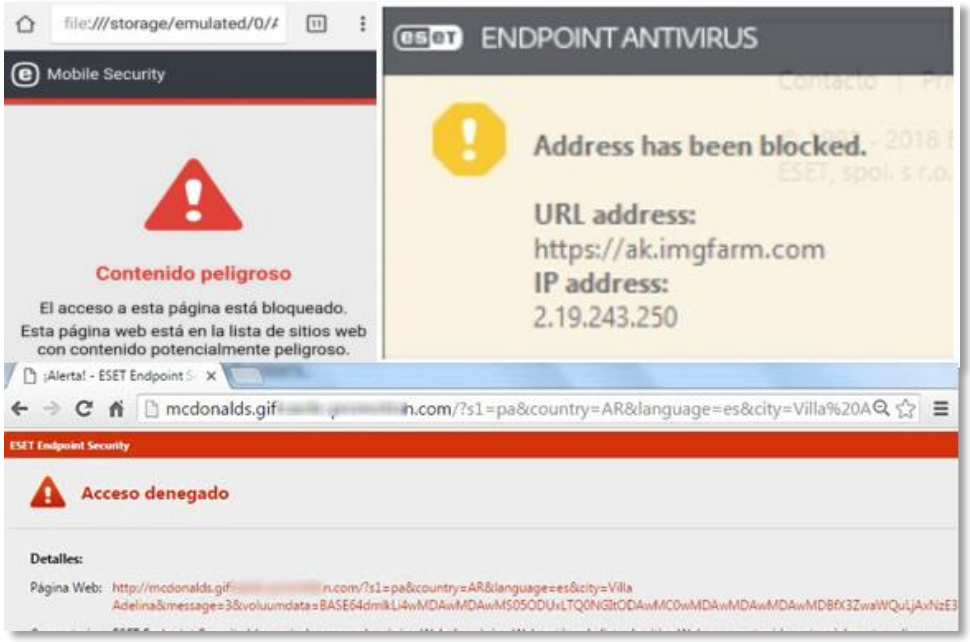


Ilustración 54 - Alertas de las soluciones de ESET al registrar enlaces sospechosos

¿A qué detalles se debe estar alertas? Basado en las campañas analizadas, no alcanza solamente con la verificación del dominio ni con la presencia de un certificado de seguridad en un portal bajo protocolo seguro o "HTTPS". Ya sea por ataques homográficos o mediante la compra y/o el registro de certificados gratuitos, los estafadores han encontrado el modo de burlar estos consejos, que han sido válidos durante años.

En consecuencia, los usuarios deben ver más allá de esas precauciones. Compartir el mensaje con amigos es una bandera de alerta inicial, a la que se sumarán cuestiones como: la poca disponibilidad de premios o de tiempo para ganar, la opinión de un conjunto de usuarios sobre sus experiencias ganando en una interfaz similar, o el volver a ingresar a la estafa y ver la misma cantidad de premios disponibles, es decir, validando la no veracidad, son solo algunos de los detalles que podrían dar la idea de que se trata de una estafa.

En algunos pocos casos las empresas afectadas reconocen públicamente que esas campañas no fueron hechas por ellas y que se trata de una estafa. En este sentido, verificar en las redes sociales de las entidades afectadas puede ser una forma de cerciorarse, y aunque no siempre resultará efectivo, merece el intento para evitar caer en la trampa.

Por último, al finalizar la estafa, los usuarios suelen ser inducidos a ingresar su número telefónico en servicios de SMS Premium, aclarado en la letra chica de los términos y condiciones. Por ello, se debe prestar total atención a estos detalles, con el fin de evitar sorpresas en la próxima facturación del teléfono.

Conclusión

Durante este último tiempo, WhatsApp ha implementado nuevas medidas de seguridad, como el cifrado punto a punto. Pero, ¿es esto útil para mitigar las estafas? La respuesta es **negativa**.

Quizá reforzar las leyes sobre los tantos grises que afectan a esta problemática podría ayudar… ¿Existe un vacío legal donde quedan desprotegidos los usuarios desprevenidos? Es posible, pero en la actualidad ya existe la tendencia a pensar que en un breve período de tiempo estas amenazas podrán ser frenadas, denunciando estos mensajes apócrifos desde WhatsApp, lo que, desde el punto de vista de la practicidad, parecería ser la mejor solución.

Por otro lado, es interesante destacar la gran cantidad de recursos utilizados en estas operaciones, teniendo en cuenta que son dirigidas a múltiples países, distintas monedas y en diversos idiomas. Con la flexibilidad y automatización de estos ataques, sumado a la naturaleza de las entidades afectadas y teniendo en cuenta que no hay muchos antecedentes a este tipo de procedimientos en cuanto a incidentes de seguridad, es natural que exista una cantidad elevada de usuarios víctima que inclusive aún no lo hayan notado.

Este tipo de estafa demuestra por qué la educación, en este caso, es la primera barrera de protección. En ese sentido, nos proponemos hacer reflexionar a los usuarios y alertarlos sobre estas nuevas tendencias que utilizan antiguas técnicas en canales como WhatsApp.

Ya hemos visto algo más de 20 marcas internacionales de alcance mundial utilizadas en distintas campañas, y con certeza, el correr de los días nos permitirá conocer nuevos casos.

Como complemento, las previsiones hechas por la consultora Gartner suponen que para el año 2021 más del 50% de las empresas gastará más dinero por año en la creación de bots y chatbots que en el desarrollo de aplicaciones móviles tradicionales. Estas cifras son un fuerte indicador de que muchas empresas comenzarán a utilizar estos canales para atraer al cliente o generar publicidad, lo que, sin lugar a dudas, también será explotado por los estafadores.

Desde ESET, nos comprometemos a mantener informados a todos los usuarios sobre los avances en esta tendencia de estafas multimarca, a fin de que nadie más sea una víctima, y cómplice a la vez, de una estafa millonaria desde su propio bolsillo.

Anexo

Enlaces utilizados para la obtención de estadísticas:

https://bitly.com/mcdonaldsvouchers+
https://bitly.com/mcdonalds-vouchers+
https://bitly.com/kfc-vouchers+
https://bitly.com/zara-fashion-voucher+
https://bitly.com/starbucks-vouchers+
https://bitly.com/IKEA-vouchers+
https://bitly.com/spar-vouchers+
https://bitly.com/jumbo-vouchers+
https://bitly.com/lidl-vouchers+
https://bitly.com/carrefour-vouchers+
https://bitly.com/hm-vouchers+
http://zara.giftcard-party.com/
http://mcdonalds.giftcard-party.com/
http://kfc.giftcard-party.com/
http://starbucks.giftcard-party.com/
http://ikea.giftcard-party.com/
http://amazon.giftcard-party.com/
http://spar.giftcard-party.com/
http://jumbo.giftcardswinnen.com/
http://lidl.giftcard-party.com/
http://mercadona.giftcard-party.com/
http://carrefour.giftcard-party.com/
http://walmart.giftcard-party.com/
http://latam.com-voucher-barato.pro/
https://spotify-usa.com/es/?premium

Saltos

http://jd4hw.voluumtrk.com/b83a6290-2b9b-4c68-9aa0-6fd732f2ba0b?s1=vbitly	(KFC)
http://jd4hw.voluumtrk.com/da8da0fc-8946-48ae-8035-9f6ab5b75ab0?s1=vbitly	(zara)
http://jd4hw.voluumtrk.com/4fca479a-1749-4053-9655-76a92efbc64b?s1=vbitly	(Starbucks)
http://jd4hw.voluumtrk.com/8ec6b7be-40a0-45a7-97d0-19264446ca1e?s1=vbitly	(Ikea)
http://jd4hw.voluumtrk.com/82995a24-f5f7-4fd9-b21d-743f7eff42a0?s1=vbitly	(Spar)
http://jd4hw.voluumtrk.com/5e95f013-843e-47b8-b7bc-365d883b8c2c?s1=vbitly	(jumbo)
http://jd4hw.voluumtrk.com/a634d132-a908-4d31-b03c-649fb28a4278?s1=vbitly	(Lidl)
http://jd4hw.voluumtrk.com/fe380d2a-ff1f-447f-b5f7-080027790b20?s1=vbitly	(hm)