Mercados

COLCAP
1.515,35
▲ 0,47%

DOW JONES
26.026,32
▲ 0,43%

IBOVESPA
94.603,75
▼ 1,03%

Commodities

MAÍZ (Bushel)
US$3,73
▲ 0,61%

COBRE (Libra)
US$2,92
▼ 0,85%

AZÚCAR (Libra)
US$0,12
▼ 1,25%

ORO (Onza troy)
US$1.293
▼ 1,74%

Divisas

DÓLAR (DATA IFX)
$ 3.096
▲ 0,49%

PESO MEXICANO
US$ 0,0519
▲ 0,10%

EURO
$3.605,20
▲ 2,62%

REAL
US$ 0,2649
▼ 0,49%

Acciones BVC

ACCIÓN MÁS:
Valorizada
MINEROS
▲ 6,67%

Transada
ECOPETROL
7.656.986 títulos

ACCIÓN MÁS:
Desvalorizada
CLH
▼ 1,10%

ACCIÓN MENOS:
Transada
BOGOTA
10.029 títulos

560.000

de barriles diarios de petróleo fue en lo que se redujo la producción de los 14 miembros de la OPEP en febrero de 2019.

Temadeldía

Pueden incluso usar la capacidad de su máquina para minar criptomonedas sin su permiso

WhatsApp, foco atractivo para el cibercrimen

Mensualmente esta aplicación reúne a más de 1.500 millones de usuarios, un escenario que resulta propicio para que cibercriminales adelanten sus campañas, como aquella en la que prometían kits de regalo de una marca de maquillaje.

DIEGO OJEDA

dojeda@elespectador.com
@DiegoOjeda95

Marcas como la de McDonald's, Starbucks, KFC o Netflix han sido utilizadas para este tipo de fraudes. / Getty Images

Tiquetes de avión gratuitos, bonos para realizar compras en supermercados y celebraciones de aniversario de distinguidas marcas con las que supuestamente regalan miles de pares de zapatos hacen parte de los atractivos mensajes que millones de personas en todo el mundo han recibido por lo menos una vez mediante la aplicación de mensajería instantánea WhatsApp.

Una regla general que se aplica en el mundo físico, pero que muy pocos llevan a lo virtual, es que "de eso tan bueno no dan tanto". Empresas de seguridad informática han encontrado que detrás de estos mensajes se esconden redes criminales que buscan engañar a la gente para sacar algún tipo de ganancia.

Ejemplo de lo anterior es una amenaza que en los últimos días se ha propagado en Colombia vía WhatsApp. En ella se anuncia la oportunidad de ganar un *kit* de productos de belleza de forma gratuita.

Al ingresar al enlace contenido en el mensaje, la persona se encuentra con una página web en la que aparece el logo de la marca L'Oréal, imágenes de sus productos y una encuesta que aparenta ser la puerta para recibir el premio.

"Contesta una preguntas de manera muy rápida y Gana el kit L'oréal. Kit disponibles 414", así, con todo y errores de redacción, es presentada la invitación para que la gente llene la encuesta en la que se pregunta por su sexo y edad.

Al finalizar el cuestionario, se le pide al interesado realizar un último paso, que consiste en enviar la promoción a cinco contactos de WhatsApp. De más está decir que esto nada tiene que ver con L'Oréal, las personas no obtienen un premio, todo es un montaje para redireccionarlos a diversas amenazas y usarlos como cómplices en la difusión de la estafa.

¿Qué es esta amenaza?

El anterior es un comportamiento que ha sido analizado por profesionales que se dedican a combatir las ciberamenazas. Informes como "Engaños millonarios desde tu bolsillo", publicado por la empresa de seguridad informática ESET, detallan que Colombia no es el único país en el que se han propagado este tipo de mensajes; L'Oréal tampoco ha sido la única marca con la que los atacantes han fabricado sus fachadas, pues compañías como McDonald's, Starbucks, KFC, Netflix, Zara y H&M, entre otras, también han sido utilizadas con este fin.

Parte de los hallazgos del investigador de ESET Lucas Paus es que estos ataques han alcanzado un grado de complejidad que les permite acoplarse al perfil de la víctima; es decir, el mismo mensaje puede ser visto en todo el mundo en diferentes idiomas y con marcas diferentes. Por ejemplo, mientras en Argentina una persona ve el mensaje con el logo del supermercado Coto, en Colombia otro podría apreciarlo con el de almacenes Éxito.

» Una de estas campañas puede llegar a 22 millones de víctimas y generar ganancias superiores a los US$176.000.

En suma, esta jugada no es más que un anzuelo para que las personas ingresen a un sitio web determinado. Aquí es cuando lo dañino comienza a suceder.

Las consecuencias de caer en estas trampas

El Espectador consultó al Dmitry Bestuzhev, director de investigación de estas y otras amenazas en Kaspersky Lab. El profesional aseguró que este tipo de campañas tiene la característica de redireccionar a la víctima a páginas en las que, por ejemplo, se le invita a descargar archivos de código malicioso con los que eventualmente podría poner en riesgo su información financiera.

Por su parte, Camilo Gutiérrez, profesional de seguridad informática de ESET, afirmó que el mismo ataque puede direccionar a las víctimas a páginas donde pueden robar sus datos personales, mostrar publicidad indeseada, usar su equipo para minar criptomonedas (obtener monedas virtuales) y hasta suscribirlo sutilmente en servicios premium de mensajes de texto que terminarán por verse reflejados en las facturas telefónicas.

¿Cómo blindarse ante estos ataques?

En la región, según el citado informe, se detalla que el *top* cinco de los países más atacados por este tipo de amenazas en América Latina lo lidera México, con un 43 % de los casos, seguido por Brasil (25 %), Argentina (13 %), Perú (12 %) y Ecuador (4 %). Si bien Colombia no se ubica en dicho escalafón, casos como el de L'Oréal demuestran que estos ataques sí se realizan aquí, por lo que es necesario tomar ciertas precauciones.

En primer lugar, se recomienda identificar los elementos que pueden indicar que un mensaje recibido vía WhatsApp, correo electrónico o red social tiene el potencial de ser malicioso.

Parte de las recomendaciones más populares es fijarse si la página web en la que se está navegando es segura, esto puede identificarse si la barra que contiene la dirección de la página aparece un candado cerrado, o si la URL comienza con "https". Sin embargo, para sorpresa de muchos, se ha demostrado que esto no es garantía, ya que hay sitios con potencial malicioso que tienen un candado cerrado. Aquí es necesario fijarse en la dirección web, ya que por ejemplo en el caso de L'Oréal, el dominio falso finaliza en .corn, algo inusual si se tiene en cuenta que la mayoría termina en .co o .com.

Por otro lado, compañías de seguridad informática invitan a sospechar si en las supuestas promociones se pide compartir el mensaje a un determinado número de contactos, si aseguran tener poca disponibilidad de premios o tiempo para ganarlos, y si vienen acompañadas de la opinión de personas que aseguran haber ganado; elementos característicos que se repiten en estas amenazas. Identificarlas se convierte en un arma poderosa para mitigar el número de víctimas y ganancias económicas que pueden generar los cibercriminales.