Tecnología

500 VUELOS RETRASADOS

Una falla del programa de gestión de carga de vuelos AeroData provocó retrasos en algunos de los principales aeropuertos de EE. UU. Cerca de 500 vuelos se vieron afectados.

Con este ataque pueden robar su información cuando compra en línea

Los usuarios pueden hacer sus compras, recibir sus productos y no darse cuenta jamás de que fueron víctimas del *formjacking*, una amenaza en el mundo del *e-commerce*.

LINDA PATIÑO REDACCIÓN TECNÓSFERA | @LinndaPC

La forma en que usted entrega gustosamente la información de sus tarjetas para comprar esa camiseta estampada con los personajes de la película de moda o los aretes de los que se enamoró por un anuncio en internet puede exponerlo al *formjacking*, una técnica con la que ciberciminales 'inyectan código' en una página y mediante formularios fraudulentos buscan robar su información financiera, vender sus datos en el mercado negro o clonar sus tarjetas.

El *formjacking*, según un reciente estudio de la firma de ciberseguridad Symantec, se está perfilando para ser el ciberataque más popular del 2019, por encima incluso del popular *ransomware*, con el que atacantes secuestran los datos de sus víctimas para exigir un rescate.

En términos generales, esta forma de ataque en alza es una manera altamente rentable de explotar las vulnerabilidades de un sitio web de compras en línea para enviar una copia de la información de los cibernautas a un servidor diferente. Lo más grave, según los expertos, es que los usuarios pueden hacer sus compras, recibir sus productos y no darse cuenta jamás de que fueron víctimas.

¿Cómo funciona?

Según Axel Díaz Ortega, abogado sénior de Adalid y experto en seguridad de la información, al contrario de lo que se podría creer, el *formjacking* no es una técnica nueva.

"Es una forma de aprovechar las vulnerabilidades de los navegadores que se ha utilizado desde los comienzos de los pagos electrónicos".

De acuerdo con los expertos, el atacante inyecta código (como un *JavaScript* que se adecua fácilmente al *frontend* de una página) para generar accesos ocultos y robarse la información de los cibernautas.

"Es una forma de ataque que ha tomado mucha fuerza este año. Nadie lo vio venir, el sector no esperaba un crecimiento tan repentino porque, en su mayoría, los navegadores han adoptado protocolos más seguros para las páginas de pagos en línea".

Para el estratega de seguridad para América Latina y el Caribe de Symantec Sebastián Brenner, el surgimiento de estos ataques se debe a la búsqueda de rentabilidad.

"Los ciberatacantes se inclinan por lo más lucrativo, buscan generar un rédito económico rápido". Para Symantec, en parte, el *ransomware* habría dejado de ser tan rentable con víctimas individuales.

En ese sentido, el *formjacking* no requiere interlocución alguna con la víctima y puede tener un alcance más masivo. En un solo sitio, miles de usuarios pueden realizar sus transacciones exitosamente y no ser conscientes de su vulnerabilidad durante meses. Según cifras de Symantec, durante el 2018 se encontraron, en promedio, unos 4.800 sitios web infectados por mes.

Según Brenner, estos ataques tienen dos fases: la primera es aquella en la cual se compromete el servidor y la segunda, esperar a que lleguen las víctimas.

El ciberatacante busca primero entrar al servidor para modificar o agregar código que capta la información del usuario.

Según el ejecutivo, "hablamos de ataques a cadenas de abastecimiento, proveedores que sirvan servicios y aplicaciones". Los delincuentes buscan afectar pequeños proveedores que suplan servicios a varios sitios de *e-commerce*. Sin embargo, sitios como la aerolínea British Airways o Ticket Master también han resultado afectados. Según Brenner, Symantec ha detenido desde 2018 unos 4 millones de ataques de *formjacking* a nivel global.

En el segundo paso, los atacantes 'esperan la presa', el usuario hace una compra común y corriente, pasa al formulario de pago y hace clic en 'pagar'. "Todo parece transparente; se realiza la compra, pero el código insertado hace una copia de la información y la envía a escondidas a las direcciones estipuladas por el atacante".

Es sabido que los sitios de compras en línea, al menos los más confiables, tienen protocolos de seguridad para que terceros no puedan ver legiblemente la información de pago de los usuarios. El éxito del *formjacking* es que no requiere acceder a esos datos cifrados, sino que funciona más como un 'espejo'. El servidor real recibe la petición de compra y la almacena en forma cifrada, pero antes envía una copia a otra dirección, escogida por el delincuente.

La solución está en mantener actualizado el navegador y desconfiar de las ofertas (ver recuadro).

Compre tranquilo

En el caso de las empresas, lo mejor es la consultoría profesional. Una firma de *e-commerce*, por ejemplo, debería, al menos una vez al año, hacer una revisión a cargo de un especialista en *ethical hacking* para identificar sus puntos débiles.

Los expertos coinciden en que no hay soluciones mágicas, pero tener los sistemas operativos de los dispositivos y las versiones más actualizadas tanto de los programas como de los navegadores es una medida fundamental.

Otras recomendaciones son utilizar portales de confianza, revisar las URL, no descargar ejecutables extraños, tener un antivirus reciente y revisar la validez del sitio y del origen de ofertas que lucen demasiado buenas para ser verdad.

¿Cuáles operadores tienen más fallas de servicio?

La Comisión de Regulación de Comunicaciones (CRC) evaluó los servicios de telefonía e internet en Colombia durante el 2018 en Barranquilla, Bogotá, Bucaramanga, Manizales, Medellín, Neiva, Popayán, Quibdó, Santa Marta y Tunja, Bogotá, Cali y Cúcuta.

Los criterios fueron los niveles de llamadas no exitosas, llamadas caídas, velocidad media, latencia y tiempo de carga web en operadores como Claro, Éxito, Avantel, Tigo, ETB, Virgin y Movistar.

En problemas en telefonía, Claro tiene el primer lugar con el 35 por ciento en llamadas no exitosas y el 34 por ciento en llamadas caídas. Por su parte, Tigo-Une presentó las cifras más bajas con 20 y 18 por ciento, respectivamente.

En tiempo de carga (término que obedece a la velocidad con la que se pueden subir y bajar contenidos a una página, en el que cuanto menos se tarde, mejor es la experiencia), los operadores se encuentran en un promedio de 7 segundos, con excepción de Claro y Avantel, que tienen 12 y 11 segundos, respectivamente.

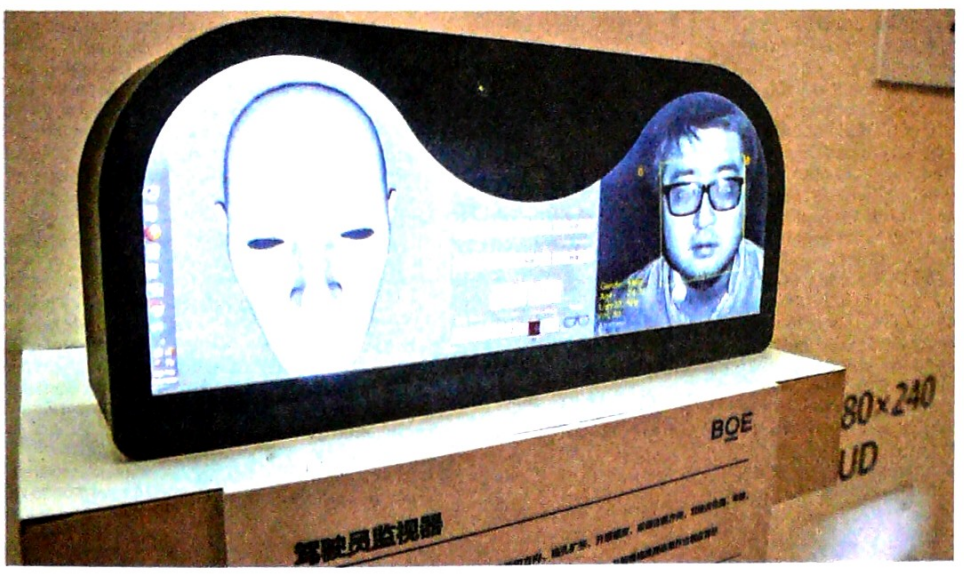
En latencia (que evalúa la rapidez de los datos para acceder a audios, videos y juegos), en el cual mientras menor sea el tiempo, mejor es la experiencia, Movistar obtuvo el mejor tiempo con un promedio de 234 milisegundos, mientras que Éxito y Claro están en los últimos lugares con 519 y 508 milisegundos, respectivamente.

"La información de estas mediciones le permite al usuario conocer cuál es la calidad de los servicios fijos o móviles ofrecidos por los operadores en cada uno de los municipios, con lo cual podrá tomar decisiones más informadas", manifestó Carlos Lugo Silva, comisionado y director ejecutivo de la CRC.

13
ciudades y municipios
EL ESTUDIO DE CALIDAD EN LOS SERVICIOS SE HIZO EN 13 CIUDADES Y MUNICIPIOS DE COLOMBIA.

Del borde de la quiebra al éxito tecnológico

Fotonoticia



UN MONITOR DE FATIGA SE EXHIBE EN EL SHOWROOM de la sede de BOE en Pekín. Este grupo estuvo al borde de la quiebra hace 25 años, pero miles de millones de dólares lo salvaron y hoy hace negocios con Apple y otras firmas, para las que quiere ser el proveedor de pantallas de próxima generación. BLOOMBERG

BREVES NOTICIAS DE TECNOLOGÍA

Aplicaciones

'Culebrita', en Google Maps

El clásico juego de la 'Culebrita', en el que una serpiente debía comer frutas sin parar, volvió con motivo de la celebración del April Fools' Day, el día de las bromas, en Estados Unidos. Esta vez, un tren va por distintos países recogiendo pasajeros en Google Maps. Para jugar, vaya a la aplicación móvil o de escritorio y presione el ícono del menú en la esquina superior izquierda.

El juego estará disponible durante una semana en dispositivos Android y iOS. **GOOGLE**

Bienestar

Un algoritmo que dice prevenir el suicidio

El proyecto 'Algoritmo de la vida' es una iniciativa de la revista *Rolling Stone* para prevenir los suicidios en Brasil. Con análisis de casos como el de la escritora Virginia Woolf o el del cantante Kurt Cobain, se desarrolló un algoritmo que lee mensajes en las redes sociales y alerta a grupos de prevención. Cada 45 minutos una persona se suicida en ese país.

Redes sociales

¿Por qué veo esto?, lo nuevo de Facebook

Facebook anunció una nueva opción llamada '¿Por qué veo esto?' que entregará al usuario información sobre por qué un *post* apareció en su *news feed*. La red social mostrará cuántas veces se interactuó con el autor del mensaje en el pasado. Una función similar, para avisos, funciona desde 2014.