# Formjacking, el ciberdelito de moda este año

**A pesar de la importancia que siguen teniendo los delitos relacionados con el *hackeo* de criptodivisas, una nueva modalidad delictiva se abre paso en las redes: el *formjacking*. Este formato implica contaminar con programas maliciosos los formularios de compras de las páginas de comercio electrónico para robar los datos bancarios de los clientes. Se trata de un factor que puede minar la confianza del consumidor en la compra *online*.**

Al igual que sucede en la economía física de toda la vida, los negocios en red requieren de un entorno de seguridad y confianza en el que tanto los vendedores como los consumidores puedan desarrollar su actividad despreocupadamente. El usuario y comprador en la economía digital cada vez eleva más las expectativas de las experiencias que va a recibir, y las empresas intentan por todos los medios crear productos y servicios cada vez más diferenciados y personalizados.

No obstante, el vertiginoso ritmo que lleva la transformación digital impide con frecuencia que las compañías puedan mantener el nivel de seguridad necesario para poder garantizar ese entorno de confianza que todo esquema de relaciones comerciales requiere.

El problema es que las ciberamenazas cada vez resultan más sofisticadas y su volumen y capacidad de hacer daño crece constantemente. Las empresas deben entender que la ciberseguridad debe estar en el corazón de sus procesos de transformación digital, si bien algunas centran sus estrategias de crecimiento en la incorporación de nueva tecnología, y no tanto en los posibles riesgos presentes en las redes.

La empresa Eleven Paths lo explica claramente en un reciente informe sobre ciberseguridad:

> “La industria de la ciberseguridad se enfrenta a dos realidades opuestas: por un lado, es necesario que todas las organizaciones incrementen el nivel de sofisticación de sus defensas para poder protegerse ante amenazas cada vez más avanzadas; por otro, hay una gran escasez de profesionales expertos y los presupuestos, aunque crecientes, siguen siendo limitados. Por ello, construir una ciberdefensa avanzada está lejos de las capacidades de la mayoría de las empresas”.

Y lo cierto es que los tipos de ciberdelitos y las modalidades de ataque no dejan de evolucionar, convirtiendo en ardua tarea la protección de empresas y particulares. El año pasado despuntaban en las estadísticas los fraudes relacionados con el *criptohackeo* de bitcoins; 2019, en sus escasos cuatro meses de vida, ya se perfila como el del *formjacking*, la nueva modalidad de estafa digital.

A grandes rasgos, el formjacking consiste en hackear los formularios de las páginas comerciales de las empresas para sustraer la información confidencial del cliente, incluidas los números y las claves de las tarjetas.

## Los criptoataques dan paso al *formjacking*

La última gran tendencia en ciberdelitos fue el *criptohackeo*, es decir, la práctica consistente en secuestrar el ordenador de terceras personas con el fin de utilizarlo para minar criptomonedas. Entre 2017 y 2018 su importancia fue creciendo, llegando incluso a superar a formatos delictivos tan conocidos como el *ransomware*, la encriptación de ordenadores mediante un virus y la exigencia de un rescate para su liberación (como el célebre WannaCry de mayo de 2017).

Sin embargo, a largo de 2018, el *cryptojacking*, como se conoce en inglés, va perdiendo fuerza. El pico de este tipo de delitos tuvo lugar entre diciembre de 2017 y febrero de 2018, periodo en el que la empresa de seguridad Symantec llegó a bloquear hasta ocho millones de eventos de *criptohackeo* al mes; alrededor de sesenta y nueve millones en los doce meses del pasado año, frente a los dieciséis millones del anterior. Pero lo cierto es que esta actividad fue cayendo, hasta un 52%, entre enero y diciembre de 2018.

Symantec atribuye la bajada de este tipo de delitos al desplome del valor de las criptodivisas (que llegó a un 90%, a lo largo de 2018, en el caso de la criptomoneda Monero), tras haber alcanzado cotizaciones record a finales de 2017. Esto no quiere decir que los delincuentes abandonaran por completo el *criptohackeo* –que ha seguido manteniendo un elevado volumen de actividad-, pero sí que ha supuesto que en muchos casos hayan buscado fuentes de ingresos ilegales alternativas, como es el caso del *formjacking*.

## De los cajeros automáticos a la red

La manera de actuar a través de *formjacking* no es nueva. Se trata de una variante *online* del clásico timo de los cajeros automáticos, en el que los delincuentes introducen algún dispositivo camuflado en la máquina capaz de leer la información de seguridad de la tarjeta, copiarla o bloquear la salida del dinero que se quiere retirar. Desde teclados falsos a cámaras ocultas, silicona o incluso lectores de bandas magnéticas, todos estos medios contribuyen al mismo objetivo.

Por su parte, el formjacking afecta a las webs y plataformas de comercio electrónico. Opera a través de un código JavasScript malicioso introducido en los formularios de pago online, cuya función es robar toda la información de las tarjetas de crédito de los compradores. El proceso seguido es el siguiente:

1. El atacante introduce el código malicioso en la web comercial objeto del ataque.
2. El cliente de esa web introduce los datos de compra en el formulario infectado.
3. Cuando el comprador formaliza la adquisición a través del botón de envío, toda la información sobre la compra le llega al vendedor, pero el atacante también recibe una copia de la misma.

De acuerdo con los datos proporcionados por Symantec, una media de 4 818 sitios web sufrió ataques de tipo *formjacking* durante cada mes de 2018. Los datos robados de una sola tarjeta de crédito pueden alcanzar hasta 45 dólares en el mercado negro, de forma que con tan solo diez tarjetas robadas los delincuentes pueden ingresar al mes más de dos millones de dólares. La rentabilidad de este ciberdelito es evidente.

## Un año negro para el comercio electrónico

El modelo de ciberdelito *formjacking* ha ido creciendo en importancia a lo largo de 2018, especialmente en los meses finales, si bien mayo registró igualmente un pico importante de ataques (hasta 556 000).

Las principales empresas afectadas por esta actividad fraudulenta fueron la compañía aérea British Airways, el portal de venta de entradas TicketMaster, el suministrador de electrónica Kitronik y VisionDirect, del sector de la óptica. Y parece ser que los ladrones son viejos conocidos del mundo de la ciberdelincuencia, pues se cree que detrás de los mayores ataques está Magecart.

Magecart es un colectivo de hackers o, más bien, un paraguas que engloba a siete grupos de cibercriminales a los que se responsabiliza del crecimiento de los robos de datos bancarios en el último año. Cada uno de los grupos tiene un *modus operandi* propio altamente sofisticado, que ha sido estudiado minuciosamente por la empresa de seguridad californiana RiskIQ en su informe *Inside Magecart*.

## Más vale prevenir

El problema que surge con el *formjacking* es que, una vez robados los datos del usuario, todo parece funcionar normal en la web comercial, de forma que nadie sospecha que se ha cometido un fraude, a diferencia de otros tipos de ataques en los que la presencia del código malicioso se hace evidente.

Con todo, existen medidas preventivas que, si las seguimos, nos pueden proteger de esta amenaza. Una de ellas es utilizar siempre pasarelas especializadas para realizar los pagos, en vez de abonar a través de la web del vendedor. Plataformas como PayPal, Apple Pay o Google Pay, reciben la información bancaria y no la comparten con la web de comercio electrónico, con lo que esta queda protegida.

Otras recomendaciones pasan por manejar siempre la última versión actualizada de los navegadores, para garantizar que llevan instalados los más recientes parches de seguridad, y tener cuidado con los sitios web que pueden usar Javascript.

Los vendedores también deberían tomar precauciones, como, por ejemplo, utilizar un sistema de gestión eventos e información de seguridad (SIEM, del inglés *security information and event management*), para detectar mediante analítica web un comportamiento anómalo del tráfico de la web, que pueda delatar si está contaminada.

Para aquellas plataformas de *eCommerce* que trabajan con otros proveedores o socios, resulta recomendable revisar el *script* de las páginas de venta de terceros para comprobar que está limpia de *malware*. Precisamente, el ataque de *formjacking* sufrido por TicketMaster entró a través del código de un *chatbot* de atención al cliente utilizado por otra empresa.

La realización de auditorías de vulnerabilidad de los sistemas de la empresa puede también ayudar a detectar si los formularios de pago han sido hackeados, antes de que se produzca el mal.

## La confianza del consumidor

El éxito y la expansión del comercio electrónico se basa en la confianza del consumidor, es decir, en que el comprador *online* lo perciba como un medio por lo menos tan seguro como la compra física.

Ninguna empresa, por protegida que esté, puede asegurar que nunca va a sufrir un ciberataque. En caso de que esto suceda, es primordial poder recuperar la confianza del usuario. KPMG ha realizado una encuesta recientemente en la que preguntaba a un grupo de consumidores qué debería hacer una empresa para recuperarles como cliente, si a causa de una brecha de seguridad en un servicio financiero *online* les fuese sustraído dinero o datos personales.

Después de la respuesta más evidente, que es compensarle por las pérdidas, un 35% de los encuestados respondió que la compañía tendría que demostrar que había solventado las vulnerabilidades. Es decir, asegurar que era de nuevo fiable.

Curiosamente, la transparencia también es valorada por los usuarios, dado que casi la quinta parte contestó que la empresa debería informarles de cualquier posible brecha de seguridad, antes de que saltase a los

medios.

La ciberseguridad es un tema muy mediático y los consumidores muestran su preocupación por las vulnerabilidades que puedan tener las empresas de las que reciben servicios, en particular, sobre cómo les puede perjudicar como clientes. En concreto, el 68% de los que respondieron a la encuesta se mostraron muy preocupados por que uno de sus proveedores pueda ser *hackeado*, y hasta el 71% teme que una empresa de la que es cliente habitual pueda hacer un mal uso de sus datos personales.

También fueron preguntados por KPMG hasta qué punto están dispuestos a que sus datos sean utilizados para personalizar la oferta que reciben de las empresas. Las respuestas fueron:

- El 45% espera que su vendedor habitual mantenga su información en secreto y no la comparta con otros.
- El 23% estaría dispuesto a ceder su información personal a empresas de comercio online si obtiene un beneficio económico a cambio.
- Al 34% no le interesa la personalización de la oferta siempre y cuando pueda mantener el control de cómo se almacena y comparte su información en manos del proveedor.
- Únicamente un 11% de la muestra manifiesta que no le importa lo que se haga con sus datos personales siempre que pueda recibir una oferta personalizada.

Para Akhilesh Tuteja, responsable de ciberseguridad global de KPMG, las empresas que en su proceso de transformación digital sean capaces de gestionar correctamente las preocupaciones de los consumidores, podrán convertirlo en un factor de competitividad.

*Imagen de Pixabay*

**Eleven Paths** (2019) "Whitepaper. Informe de tendencias en ciberseguridad 2019". Disponible en: https://www.elevenpaths.com/wp-content/uploads/2019/04/whitepaper-tendencias-ciberseguridad-2019.pdf

**Fundación Telefónica** (2019) "Sociedad Digital en España 2018". Disponible en: https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/655/

**Hiba** (2019) "What is Formjacking? The Latest Internet Threat" en *The VPN Guru*. Disponible en: https://thevpn.guru/formjacking-explained/

**Jiménez, J.** (2019) "Qué es el formjacking y cómo pone en peligro tu información y datos bancarios" en *RedesZone*. Disponible en: https://www.redeszone.net/2019/03/25/que-es-formjacking-datos-bancarios/

**Jolera** (2019) "The Formjacking Threat Explained". Disponible en: https://www.jolera.com/the-formjacking-threat-explained/

**KPMG** (2019) "Consumer Loss Barometer. The economics of trust". Disponible en: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/consumer-loss-barometer-2019.pdf

**Symantec** (2019) "Internet Security Threat Report. Volume 24. February 2019". Disponible en: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

**Symantec Security Response** (2018) "Formjacking: Major Increase in Attacks on Online Retailers" en *Symantec Blogs*. Disponible en:

https://www.symantec.com/blogs/threat-intelligence/formjacking-attacks-retailers

**Team RiskIQ** (2018) “Inside Magecart: RiskIQ and Flashpoint Release Comprehensive Report on Cybercrime and the Assault on E-Commerce” en *RiskIQ*. Disponible en: https://www.riskiq.com/blog/external-threat-management/inside-magecart/

**Whittaker, Z.** (2018) “Meet the Magecart hackers, a persistent credit card skimmer group of groups you’ve never heard of” en *TechCrunch*. Disponible en: https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/