NEWSLETTER | totalsec

Expertos en Ciberseguridad

No. 285 | Ago 16 - Ago 20

T-MOBILE INVESTIGA UNA POSIBLE FILTRACIÓN DE DATOS MASIVA

AGOSTO 18, 2021/FUENTE: CYBERSECURITY NEWS[1]

La tercera semana del mes de agosto ha empezado con fuerza en relación al robo de datos. Empezamos con el robo a Zurich España, a lo que debemos sumar otro de mayor envergadura si cabe. En este caso, la compañía afectada no es otra que T-Mobile, una de las compañías de telecomunicaciones más grandes del mundo. La empresa alemana ha informado recientemente que podría haber sufrido una filtración masiva de datos; una filtración que podría haber comprometido la información de, nada menos, 100 millones de usuarios. La cifra es para tenerla muy en cuenta, pues los daños causados por ella podrían ser enormes. T-Mobile fue alertada de la filtración, supuestamente, por un post encontrado en un foro. El gigante de las telecomunicaciones alemán ya se encuentra investigando qué ha pasado. T-Mobile investiga una posible filtración de datos masiva.

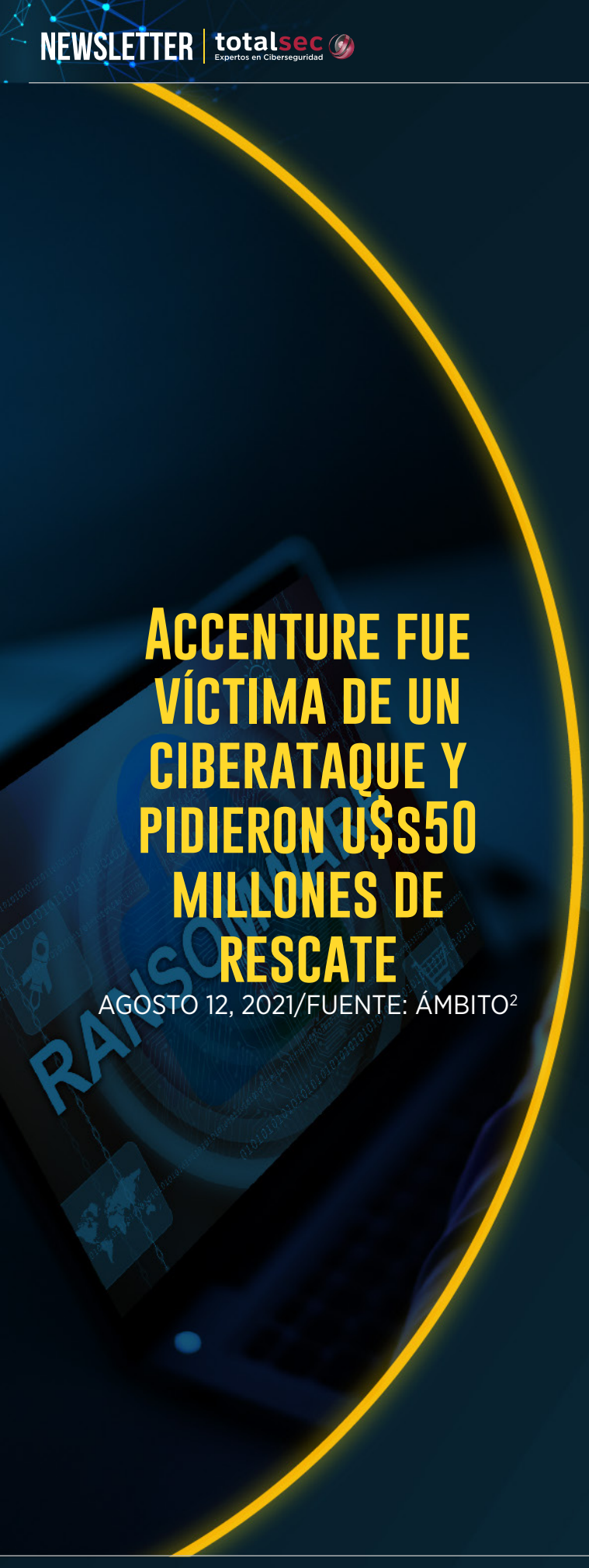
En dicho foro, al parecer, apareció este pasado fin de semana un hilo en el que se ofrecían los datos robados a cambio de criptomonedas como Bitcoin. Si bien no se menciona en el hilo a la propia compañía alemana, el ciberdelincuente se ha encargado de sugerir que la información procede de los servidores del gigante de las telecomunicaciones. Dejó un mensaje que rezaba lo siguiente: -«T-Mobile USA. Toda información de sus clientes«-. En relación al valor que solicita el ciberdelincuente para vender la información, estamos hablando de 6 Bitcoin, es decir, unos 274000 dólares al cambio. A modo de gancho, el perpetrador del robo esta ofreciendo hasta 30 millones de licencias de conducir y números de la seguridad social. En cuanto al resto de la BB.DD., se ofrecerá por privados.

T-Mobile investiga una posible filtración de datos masiva que podría afectar a 100 millones de clientes en todo el mundo

Tipo de datos filtrados e investigación de T-Mobile

Los datos filtrados, según se ha revelado, podrían incluir números de la seguridad social, teléfonos, nombres, direcciones y carnets de conducir. Las licencias y números de la SS se están usando como cebo. T-Mobile es consciente del problema, pero no quieren ahondar mucho en declaraciones. Un portavoz de la compañía ha comentado estar al tanto de las reivindicaciones hechas en el foro y de estar investigando su veracidad. De momento, ha añadido, no tienen más información que compartir al respecto. Quien sí ha hecho unas declaraciones ha sido el ciberdelincuente, concretamente en relación a la expulsión del servidor que había atacado. Según comentó: -«Creo que se han dado cuenta porque hemos perdido acceso en los servidores que tenían puertas traseras«-. A pesar de haber sido expulsado, logró guardar copias de seguridad de los datos. Estaremos pendientes del desarrollo de esta grave situación.

[1]Fuente: https://cybersecuritynews.es/t-mobile-investiga-una-posible-filtracion-de-datos-masiva/



ACCENTURE FUE VÍCTIMA DE UN CIBERATAQUE Y PIDIERON U$S50 MILLONES DE RESCATE

AGOSTO 12, 2021/FUENTE: ÁMBITO[2]

La consultora internacional Accenture fue víctima de un ataque del ransomware a manos de Lockbit 2.0. Esta última publicó el nombre de Accenture en el sitio que se utiliza para publicar la información robada de las víctimas y así, presionarlas para que paguen un rescate.

Si bien la consultora confirmó que identificó actividad irregular en sus sistemas, también afirmó que lo sucedido no había afectado a sus operaciones ni a los sistemas de sus clientes.

Por su parte, la compañía Cyble informó que los actores de amenazas aseguran haber robado 6TB de información y que están solicitando un rescate por u$s50 millones, a través de su cuenta de Twitter.

Stacey Jones, una portavoz de Accenture, ratificó la existencia de un incidente de ciberseguridad, pero no reconoció explícitamente un ataque de ransomware, en diálogo con CNN Business el miércoles.

"A través de nuestros controles y protocolos de seguridad, identificamos una actividad irregular en uno de nuestros entornos", dijo Jones en un comunicado. "Contuvimos inmediatamente el asunto y aislamos los servidores afectados. Hemos restaurado completamente nuestros sistemas afectados desde una copia de seguridad", explicó.

La consultora confirmó que identificó actividad irregular en sus sistemas, pero que el hecho no había afectado a sus operaciones ni a los sistemas de sus clientes

Según un perfil del grupo que hizo Emsisoft, la banda de ransomware LockBit surgió por primera vez en septiembre de 2019.

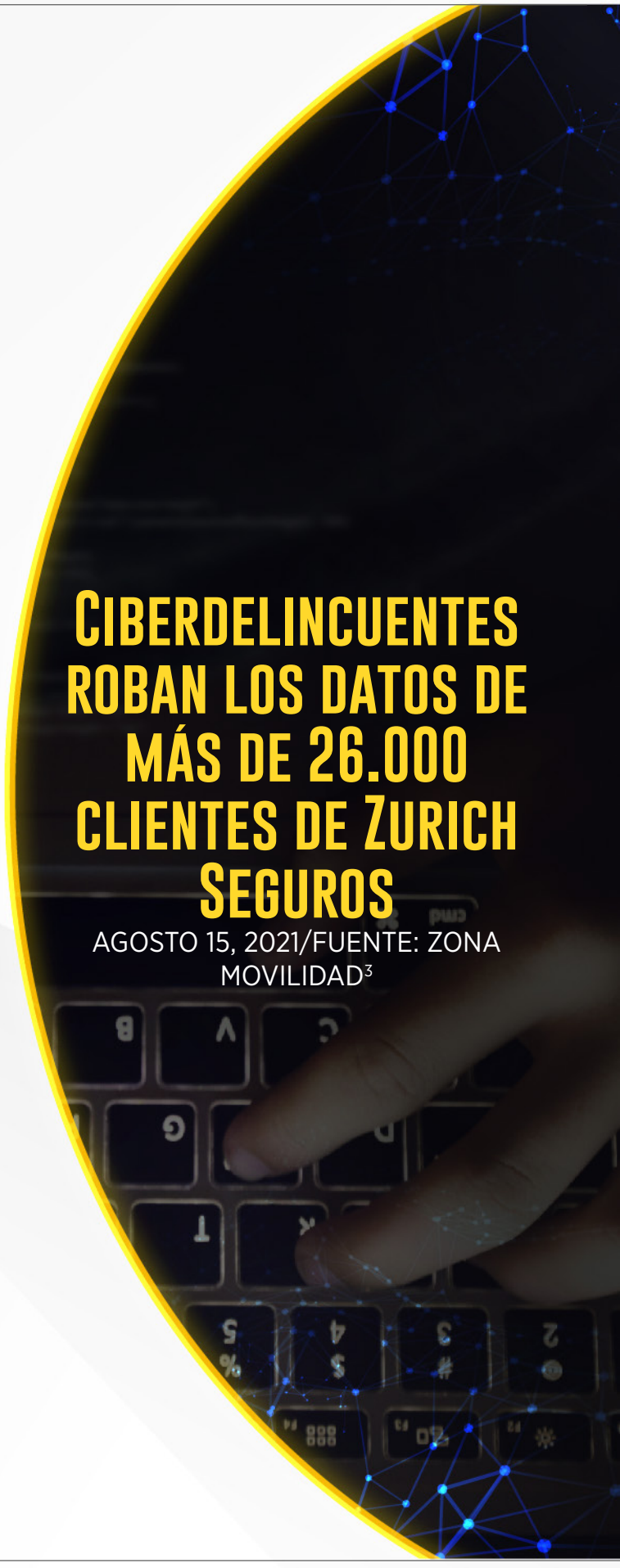
LockBit se encarga de alquilar su software malicioso a terceros afiliados criminales que luego reciben una parte de los rescates a cambio de plantar el código en las redes de las víctimas.

En agosto de 2020, la Interpol ya había advertido un aumento de los ataques con el software malicioso LockBit. Asimismo, la semana pasada, el Centro de Ciberseguridad Australiano (ACSC) emitió un comunicado advirtiendo sobre el incremento de los ataques del ransomware Lockbit 2.0 contra entidades de Australia.

[2]Fuente: https://www.forbes.com.mx/hacker-regresa-258-mdd-en-criptodivisas-despues-de-robar-600-mdd/

CIBERDELINCUENTES ROBAN LOS DATOS DE MÁS DE 26.000 CLIENTES DE ZURICH SEGUROS

AGOSTO 15, 2021/FUENTE: ZONA MOVILIDAD[3]



Zurich Seguros ha sufrido un ciberataque esta semana. Un conjunto de ciberdelincuentes se ha hecho con la información de los clientes. La empresa sufrió entre el 12 y 13 de agosto obtenciones ilícitas de información de determinados clientes en España. La empresa ha activado sus mecanismos de control y gestión de ciberseguridad para identificar la causa y el origen de este incidente.

Zurich Seguros, ha sufrido el robo de las bases de datos de sus clientes españoles. La aseguradora cuenta con una base de datos que tiene más de 4,7 millones de líneas de información. Asimismo, los ciberdelincuentes han difundido un archivo en el que se encuentran los datos de más de 26.000 personas y empresas.

INFORMACIÓN HACKEADA

El tipo de información robada a sus clientes han sido Nombre y apellidos, DNI, vehículo asegurado: modelo, matrícula y prestaciones, teléfono, dirección de su domicilio, correo electrónico, y fecha de la póliza de seguros.

> La información robada de la base de datos tiene un precio, 1.000 dólares en bitcoins

En este aspecto, fuentes de dirección de la empresa de seguros han explicado que “los mecanismos de control y gestión de ciberseguridad de Zurich se activaron desde el primer momento para determinar la causa y el origen del incidente. Los primeros análisis y a la espera de los resultados del informe de investigación, indican que se trataría de una afectación limitada a una línea de negocio lo que supondría un limitado porcentaje de clientes”.

Paralelamente, Vicente Delgado, detective, hacker, especializado en ciberseguridad, ha señalado que "hay suficiente información como para poder suplantar la identidad de un tercero, conocer los vehículos que tiene a su nombre una persona, usar los datos personales para contratar líneas de telefonía, hacerse pasar por clientes de Zurich para obtener la cuenta corriente vinculada a los pagos”.

Por otro lado, la Policía y la Agencia Española de Protección de Datos, que están llevando a cabo los mecanismos de comunicación con sus clientes y mediadores, están al tanto de lo ocurrido. Además, los equipos y servicios de Zurich Seguros siguen estando operativos. En este momento, se está esperando a los resultado del informe de investigación. La información robada de la base de datos tiene un precio, 1.000 dólares en bitcoins.

Con el robo de datos de Zurich Seguros ya son varias las empresas y administraciones públicas españolas las que han sufrido ciberataques.

[3]Fuente: https://www.zonamovilidad.es/ciberdelincuentes-se-hacen-con-datos-mas-26-000-clientes-zurich-seguros

UN NUEVO MALWARE ATERRIZA EN ANDROID: FLYTRAP

AGOSTO 18, 2021/FUENTE: CYBER SECURITY NEWS[4]

Navegar por Internet, ya sea a través de un PC o de un Smartphone, es cada vez más inseguro por culpa de las distintas amenazas que surgen. Lamentablemente, lejos de desaparecer, estas amenazas se multiplica con las setas tras un día de lluvia. La última de la que tenemos constancia se llama FlyTrap y se está extendiendo en dispositivos Android. Este nuevo troyano, el cual ha sido descubierto por el equipo de expertos en seguridad informática de Zeimperium zLabs, está afectando al S.O. de Google en más de 140 países diferentes, por lo que estamos hablando de una expansión bastante rápida. Flytrap apareció el pasado mes de marzo, y desde entonces ha experimentado un crecimiento muy veloz. Según Zeimperium zLabs, este malware se introduce por medio de técnicas de ingeniería social. Un nuevo malware aterriza en Android y su nombre es Flytrap.

Un nuevo malware aterriza en Android y su nombre es Flytrap, el cual se introduce en dispositivos por medio de técnicas de ingeniería social

Los objetivos de este troyano están siendo, principalmente, personas que hacen un uso frecuente de Facebook, la conocida red social creada por Mark Zuckerberg. Se calcula que, hasta el día de hoy, el número de afectados por FlyTrap podría ascender hasta los 10000. Sin duda, estamos hablando de una cifra importante. El modus operandi de este malware es muy sencillo, pues busca introducirse en Android engañando a los usuarios con ofertas de toda clase. Entre esas ofertas podemos encontrar: productos electrónicos, aplicaciones, códigos gratuitos o servicios de streaming. Todos ellos a precios ridículos. Como se puede observar, el método usado no es precisamente novedoso. A pesar de ello, tal y como revelan los datos, aún hay gente que pica en el anzuelo. Una vez que FlyTrap toma el control tiene acceso a todos los datos privados de la víctima.

Datos sensibles en manos de FlyTrap

Antes de tomar el control del dispositivo debe hacer que la víctima caiga en la trampa, algo que intentará solicitando el inicio de sesión en Facebook para acceder a los cupones de descuento. Si lo hacemos, el malware podrá acceder a datos de identificación de Facebook, ubicación de la dirección IP, e-mail y hasta datos de las cookies. Hay que tener mucho cuidado con estas cosas. La clave para evitar caer en la trampa es desconfiar siempre de cualquier pop-up, correo o mensaje que nos llegue desde una fuente de dudosa procedencia. Por último, comentar que Zeimperium zLabs ha compartido una lista con las app y nombres de los APK infectados por FlyTrap.

- com.luxcarad.cardid: GG Voucher
- com.gardenguides.plantingfree: Vote European Football
- com.free_coupon.gg_free_coupon: GG Coupon Ads
- com.m_application.app_moi_6: GG Voucher Ads
- com.free.voucher: GG Voucher
- com.ynsuper.chatfuel: Chatfuel
- Com.free_coupon.net_coupon: Net Coupon
- com.movie.net_coupon: Net Coupon
- com.euro2021: EURO 2021 Official

[4]Fuente: https://cybersecuritynews.es/un-nuevo-malware-aterriza-en-android-flytrap/

NEWSLETTER

totalsec
Expertos en Ciberseguridad