iTQ latam

CyberSOC iTQ latam

INFORME SEMANAL DE CIBERAMENAZAS

W37-2023

www.itqlatam.com

Cuidado con las extensiones que instalas en Chrome, Safari o Firefox: muchas están recopilando tus contraseñas según este estudio

A día de hoy son muchas las extensiones que podemos encontrar para nuestros navegadores, y la proliferación de las IA hacen que tengamos nuevas opciones encima de la mesa que nos prometen una navegación más eficiente. Pero debemos tener en cuenta que algunas de estas opciones pueden llegar a ser inseguras, tal y como apuntan diferentes estudios.

https://www.genbeta.com/actualidad/cuidado-extensiones-que-instalas-chrome-safari-firefox-muchas-estan-recopilando-tus-contrasenas-este-estudio

Mucho cuidado con lo que dices nada más descolgar el teléfono: podrías caer en la trampa de esta nueva estafa

Suena el teléfono, lo coges, descuelgas y, ¿qué es lo primero que dices? Bueno, en mi experiencia, en casi un 50% de los casos nos inclinamos por el 'Diga'/'Dígame'... y en otro casi 50% optamos por el mucho más sencillo y escueto "¿Sí?".

Pues bien, si eres de los que suele preferir esta última opción, tienes todas las papeletas para terminar teniendo problemas con los ciberestafadores.

https://www.genbeta.com/seguridad/mucho-cuidado-que-dices-nada-descolgar-telefono-podrias-caer-trampa-esta-nueva-estafa

ESET analiza Spacecolon, el conjunto de herramientas que propaga ransomware por todo el mundo y roba datos confidenciales

ESET Research ha publicado su análisis de Spacecolon, un pequeño conjunto de herramientas utilizado para desplegar variantes del ransomware Scarab a víctimas de todo el mundo. Probablemente accede a las organizaciones víctimas a través de operadores que comprometen servidores web vulnerables o mediante la rotura de credenciales RDP por fuerza bruta. Varias variantes de Spacecolon contienen muchos comentarios dentro del código en turco, por tanto, ESET cree que está escrito por un desarrollador de habla turca. La compañía líder en ciberseguridad pudo rastrear los orígenes de Spacecolon al menos hasta mayo de 2020, y sus campañas siguen en curso.

https://blogs.protegerse.com/2023/08/22/eset-analiza-spacecolon-el-conjunto-de-herramientas-que-propaga-ransomware-por-todo-el-mundo-y-roba-datos-confidenciales/

América Latina en la mira de SpyLoan, malware detrás de las apps de préstamos conocidas como “montadeudas”

Especialistas de Kaspersky alertan sobre el malware SpyLoan como una de las principales amenazas para usuarios móviles de América Latina: se trata de aplicaciones que se difunden a través de anuncios en redes sociales y que ofrecen préstamos inmediatos, pero a tasas de interés muy altas. Ante el incumplimiento de pago, las aplicaciones desarrollan una fase maliciosa que roba información personal, fotos de la víctima y hasta bloquea su teléfono para extorsionarla y así, forzar el pago de la deuda.

https://www.ciberseguridadlatam.com/2023/09/09/america-latina-en-la-mira-de-spyloan-malware-detras-de-las-apps-de-prestamos-conocidas-como-montadeudas/

A pocos días del lanzamiento del nuevo iPhone 15, las estafas se disparan

En anticipación al inminente lanzamiento del iPhone 15 de Apple, los expertos de Kaspersky han descubierto una serie de estafas que aprovechan la emoción que rodea esta innovación tecnológica. Estas estafas abarcan varios esquemas fraudulentos, cada uno con riesgos distintos para los consumidores desprevenidos, incluyendo posibles pérdidas de datos y financieras.

https://www.ciberseguridadlatam.com/2023/09/08/a-pocos-dias-del-lanzamiento-del-nuevo-iphone-15-las-estafas-se-disparan/

Estados Unidos acusa a los fundadores del mezclador Tornado Cash, utilizado por los piratas informáticos de Lazarus

El Departamento de Justicia de Estados Unidos acusó a dos fundadores de Tornado Cash de ayudar a delincuentes, incluido el notorio grupo de piratería norcoreano Lazarus, a lavar más de mil millones de dólares en criptomonedas robadas a través de su servicio descentralizado de mezcla de criptomonedas.

Lazarus usó el criptovaso creado por Roman Storm y Roman Semenov para lavar alrededor de $455 millones robados en el mayor atraco de criptomonedas conocido después del hackeo del puente de la red Ronin de Axie Infinity.

https://www.ciberseguridadlatam.com/2023/08/24/estados-unidos-acusa-a-los-fundadores-del-mezclador-tornado-cash-utilizado-por-los-piratas-informaticos-de-lazarus/

LockBit: El Grupo de Hackers detrás del ataque al Ayuntamiento de Sevilla (España) exige 5 millones de euros

El Ayuntamiento de Sevilla se enfrenta a una crisis informática desencadenada por un ciberataque de ransomware que ha paralizado sus sistemas y servicios telemáticos. La situación se volvió crítica el 5 de septiembre, cuando el Consistorio confirmó la intrusión y decidió suspender los servicios como medida preventiva, a la espera de evaluar la magnitud del ataque. Sin embargo, hasta la fecha, la situación no ha sido resuelta y persisten las dificultades.

https://cybersecuritynews.es/lockbit-el-grupo-de-hackers-detras-del-ataque-al-ayuntamiento-de-sevilla-exige-5-millones-de-euros/

Latam: Sólo 25% de empresas en la región tienen plan de ciberseguridad

En los últimos 12 meses, 80% de las empresas que sufrieron ciberataques en América Latina pagaron para poner fin al incidente y recuperar sus datos, alerta.

Además, en la región una de cuatro empresas considera que sus programas de riesgos en ciberseguridad funcionan bien, en medio del aumento en los ataques cibernéticos. Muchas compañías siguen presentando fallas en sus sistemas, como una documentación no actualizada o errónea, así como, falta de pruebas formales y reportes, información en silos, entre otros elementos, señaló Rick Vanover, director senior de Estrategia de Producto de Veeam.

https://www.paradavisual.com/latam-solo-25-de-empresas-en-la-region-tienen-plan-de-ciberseguridad/

INFORME SEMANAL DE
CIBERAMENAZAS

W37-2023