iTQ latam

CyberSOC iTQ latam

INFORME SEMANAL DE CIBERAMENAZAS

W38-2023

www.itqlatam.com

Robar dinero de aplicaciones de billeteras móviles con una vulnerabilidad de Android

Un intruso podría utilizar una vulnerabilidad de seguridad en la función de App Pinning de Android para realizar compras ilegales utilizando Google Wallet si está lo suficientemente decidido a hacerlo. Debido a la vulnerabilidad, un atacante puede acceder al número completo de la tarjeta, así como a la fecha de vencimiento, desde un dispositivo bloqueado. Para aprovechar la vulnerabilidad identificada como CVE-2023-35671, un atacante necesitaría acceso físico al dispositivo de la víctima. Después de eso, tendrían que poner el dispositivo en modo App Pin y mantenerlo cerca de un escáner NFC . Una vez leídos los datos de la tarjeta, el autor puede utilizarla para realizar un pago ilícito.

https://noticiasseguridad.com/seguridad-movil/robar-dinero-de-aplicaciones-de-billeteras-moviles-con-una-vulnerabilidad-de-android/

Las vulnerabilidades de Protonmail permiten robar correos cifrados y hacer spoofing

Un servicio de correo web conocido por su énfasis en la privacidad de los usuarios, Proton Mail , tiene graves fallos en el código que fueron descubiertos por un grupo de investigadores. Estas vulnerabilidades podrían haber puesto en peligro a los usuarios del servicio. Estas vulnerabilidades revelaron un posible eslabón débil en la cadena de seguridad, a pesar de que Proton Mail utiliza un potente cifrado de extremo a extremo con el fin de salvaguardar los mensajes tanto en tránsito como mientras están almacenados.

https://noticiasseguridad.com/seguridad-informatica/las-vulnerabilidades-de-protonmail-permiten-robar-correos-cifrados-y-hacer-spoofing/

Ciberataque contra sitios estatales de Panamá, Chile y Colombia

Ciberdelincuentes concretaron un exitoso ciberataque sobre cientos de sitios web de Panamá, Chile y Colombia. Entre los sitios afectados, se encuentran los de algunos servicios estatales. «Es un ataque de ransomware en donde atacaron a IFX Networks», un proveedor estadounidense de servicios de tecnología. Así lo señaló Radio Saúl Kattan, consejero presidencial para la transformación digital de Colombia.

https://www.ciberseguridadlatam.com/2023/09/18/ciberataque-contra-sitios-estatales-de-panama-chile-y-colombia/

El grupo Lazarus de Corea del Norte es sospechoso de atraco a CoinEx por 31 millones de dólares

El Grupo Lazarus, afiliado a Corea del Norte, ha robado casi 240 millones de dólares en criptomonedas desde junio de 2023, lo que marca una escalada significativa de sus ataques.

Según múltiples informes de Certik, Elliptic y ZachXBT, se dice que el infame grupo de ciberdelincuentes, es sospechoso de estar detrás del robo de 31 millones de dólares en activos digitales del intercambio CoinEx el 12 de septiembre de 2023.

El robo de criptomonedas dirigido a CoinEx se suma a una serie de ataques recientes dirigidos a Atomic Wallet ($100 millones), CoinsPaid ($37,3 millones), Alphapo ($60 millones) y Stake.com ($41 millones).

https://www.ciberseguridadlatam.com/2023/09/18/el-grupo-lazarus-de-corea-del-norte-es-sospechoso-de-atraco-a-coinex-por-31-millones-de-dolares/

Las vulnerabilidades en la nube aumentan un 200% en un año

IBM rastreó 632 nuevas vulnerabilidades relacionadas con la nube (CVE) entre junio de 2022 y junio de 2023, un aumento del 194% con respecto al año anterior, según un nuevo informe del gigante tecnológico.

El Informe sobre el panorama de amenazas de IBM X-Force Cloud 2023 se compiló a partir de la inteligencia de amenazas, los compromisos de respuesta a incidentes y las pruebas de penetración de la empresa, junto con análisis de la web oscura, aportes de Cybersixgill y el servicio Red Hat Insights.

https://www.ciberseguridadlatam.com/2023/09/17/las-vulnerabilidades-en-la-nube-aumentan-un-200-en-un-ano/

Ransomware paraliza servicios en múltiples países: IFX Networks bajo escrutinio por falta de transparencia

En medio del caos desencadenado por el ciberataque ransomware que afectó a IFX Networks, una preocupación significativa ha surgido: la falta de transparencia de la compañía en torno a la magnitud del incidente y las medidas tomadas para abordarlo. Esta falta de claridad ha generado un profundo desconcierto entre las miles de empresas que dependen de los servicios de IFX Networks y ha dejado a los afectados en un estado de incertidumbre innecesario.

https://www.ciberseguridadlatam.com/2023/09/15/ransomware-paraliza-servicios-en-multiples-paises-ifx-networks-bajo-escrutinio-por-falta-de-transparencia/

Anubis, AhMyth y SpinOk: tres malwares de móviles más usados por los ciberdelincuentes

En el vertiginoso mundo de la ciberseguridad, los malwares móviles son una preocupación constante. Durante el mes de agosto, tres peligrosos malwares móviles han estado acechando a usuarios de Android, poniendo en riesgo la seguridad de sus dispositivos y datos personales. Aquí te presentamos un resumen de los tres malwares móviles más usados en el último mes.

https://cybersecuritynews.es/anubis-ahmyth-y-spinok-tres-malwares-de-moviles-mas-usados-por-los-ciberdelincuentes/

Microsoft Teams en el punto de mira de los ciberdelincuentes, así puedes protegerte

Con el avance de la digitalización y la implementación generalizada del teletrabajo, la comunicación online se ha convertido en la columna vertebral de las interacciones entre compañeros de trabajo, jefes, proveedores y clientes. En este nuevo panorama, multitud de soluciones tecnológicas han buscado facilitar la conexión de personas sin importar su ubicación física y una de las más utilizadas en todo el mundo es Microsoft Teams. En medio de su creciente popularidad, se están poniendo de manifiesto los posibles riesgos cibernéticos que puede conllevar su uso y diferentes investigadores han encontrado fallas de ciberseguridad que pueden comprometer el trabajo de las empresas a través de esta herramienta.

https://blogs.protegerse.com/2023/09/08/microsoft-teams-en-el-punto-de-mira-de-los-ciberdelincuentes-asi-puedes-protegerte/

Microsoft expuso 38 terabytes de datos privados internos por error

Microsoft, como cualquier empresa volcada en la actualidad en el desarrollo y comercialización de productos y servicios basados en inteligencia artificial, trabaja día a día con volúmenes de datos impensables hace unos pocos años. Y, claro, a mayor volumen y segregación de los mismos (es decir, a tenerlos distribuidos en distintos lugares), crece el riesgo de que alguno de estos conjuntos se pueda ver expuesto públicamente por algún problema de seguridad.

https://www.muycomputer.com/2023/09/18/microsoft-expuso-38tb-de-datos-privados-internos/

Balancer sufre nuevo ataque y pierde 238,000 dólares en el último exploit contra DeFi

El protocolo de finanzas descentralizadas (DeFi) Balancer ha sido atacado en lo que parece ser el último exploit de la industria. El protocolo alertó a los usuarios de la incursión, advirtiéndoles que no interactuaran con ella.

El 20 de septiembre, Balancer alertó a los usuarios que su interfaz estaba bajo ataque. “El asunto está actualmente bajo investigación”, señaló hace unas cinco horas.

https://cryptocity.press/noticias/balancer-sufre-nuevo-ataque-y-pierde-238000-dolares-en-el-ultimo-exploit-contra-defi


iTQ latam
CyberSOC
iTQ latam
INFORME SEMANAL DE
CIBERAMENAZAS
W38-2023
www.itqlatam.com