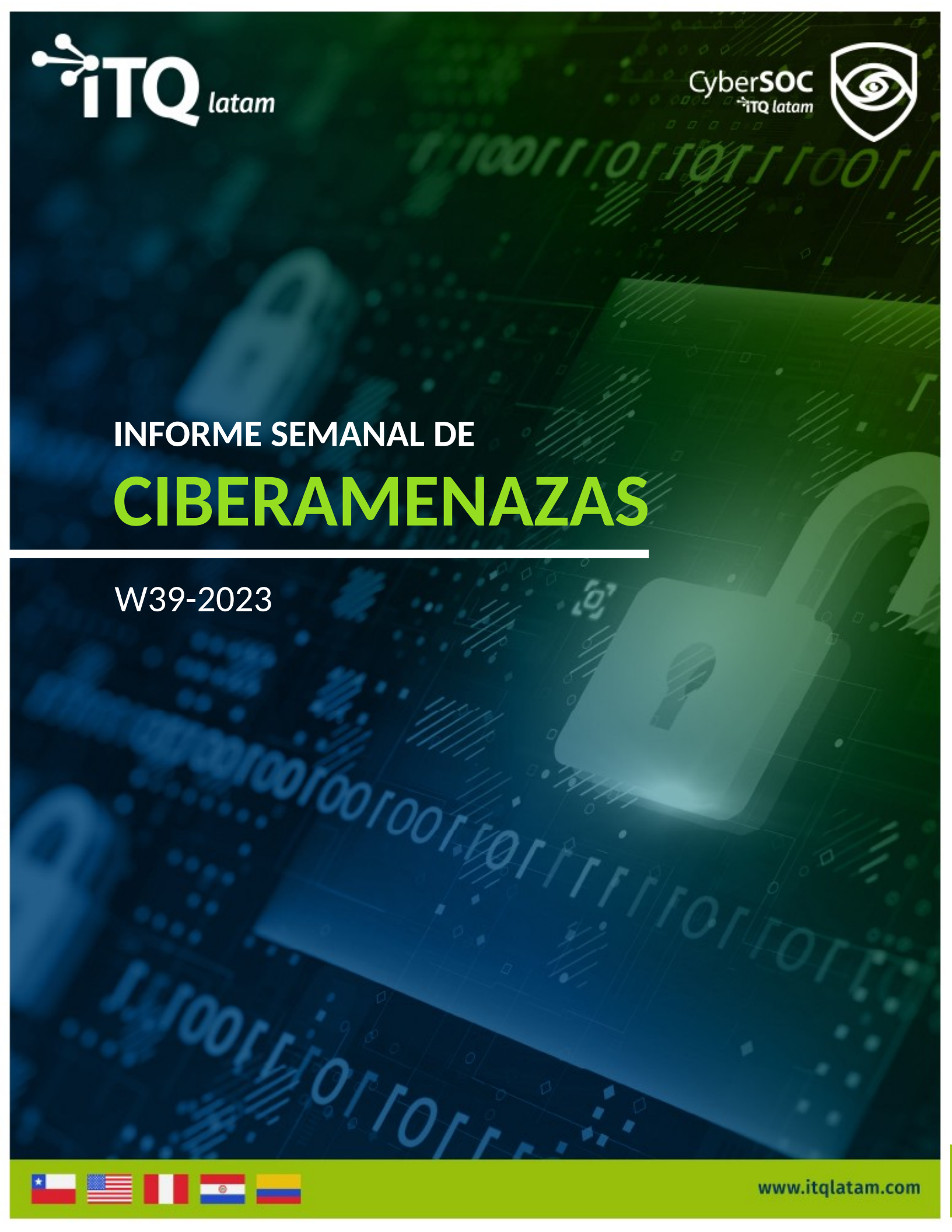
iTQ latam
CyberSOC
iTQ latam
INFORME SEMANAL DE
CIBERAMENAZAS
W39-2023
www.itqlatam.com

Los días cero de Apple y Chrome, parcheados recientemente, explotan en ataques de software espía

Investigadores de seguridad del Citizen Lab y el Threat Analysis Group (TAG) de Google revelaron hoy que se abusó de tres días cero parcheados por Apple el jueves como parte de una cadena de exploits para instalar el software espía Predator de Cytrox.

Entre mayo y septiembre de 2023, los atacantes explotaron los errores (CVE-2023-41991, CVE-2023-41992 y CVE-2023-41993) en ataques utilizando SMS señuelo y mensajes de WhatsApp dirigidos al ex parlamentario egipcio Ahmed Eltantawy después de anunciar planes para unirse a las elecciones presidenciales egipcias de 2024.

https://www.ciberseguridadlatam.com/2023/09/23/los-dias-cero-de-apple-y-chrome-parcheados-recientemente-explotan-en-ataques-de-software-espia/

El gobierno de las Bermudas vincula un ciberataque con los piratas informáticos rusos

El Gobierno del territorio británico de ultramar de las Bermudas ha vinculado un ciberataque que afectó a los sistemas informáticos de todos sus departamentos desde el jueves con piratas informáticos radicados en Rusia.

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

Pizza Hut Australia advierte a 193.000 clientes sobre una violación de datos

Pizza Hut Australia está enviando notificaciones de violación de datos a los clientes, advirtiendo que un ciberataque permitió a los piratas informáticos acceder a su información personal.

La notificación advierte que el pirata informático obtuvo acceso no autorizado a los sistemas de Pizza Hut Australia que almacenan información confidencial de los clientes que realizaron pedidos en línea, así como datos financieros parciales y contraseñas de cuentas cifradas.

https://www.ciberseguridadlatam.com/2023/09/22/pizza-hut-australia-advierte-a-193-000-clientes-sobre-una-violacion-de-datos/

Acumulando polvo y datos: cómo las aspiradoras robóticas pueden espiarte

Desde su aparición como opción para la limpieza del hogar, las aspiradoras robóticas avanzaron rápido y son cada vez más eficientes en aspirar cada esquina sin sufrir golpes. Para evitar los obstáculos, están equipadas con sensores, GPS o incluso cámaras, así como cada vez son más efectivas en aspirar el polvo, también lo son en algo más: recolectar datos personales.

https://www.ciberseguridadlatam.com/2023/09/04/acumulando-polvo-y-datos-como-las-aspiradoras-roboticas-pueden-espiarte/

Industria espacial de EE.UU. bajo amenaza de ciberespionaje extranjero

Los servicios de inteligencia extranjeros podrían usar ataques cibernéticos directos y de cadena de suministro para obtener acceso a la industria espacial de EE. UU., según la inteligencia de EE. UU.

En un aviso conjunto del Centro Nacional de Seguridad y Contrainteligencia de EE. UU., el FBI y la Fuerza Aérea de EE. UU. advirtieron que las entidades de inteligencia extranjeras (FIEs) ven la innovación y los activos relacionados con el espacio de EE. UU. como amenazas potenciales, así como oportunidades valiosas para adquirir tecnologías y experiencia vitales.

https://www.ciberseguridadlatam.com/2023/08/22/industria-espacial-de-ee-uu-bajo-amenaza-de-ciberespionaje-extranjero/

Cómo envian malware o mensajes de phishing a través de teams, esquivando las funciones de seguridad de teams

TeamsPhisher es un software Python3 que fue diseñado para facilitar el envío de mensajes y archivos adjuntos de phishing a usuarios de Microsoft Team cuyas empresas u organizaciones permiten la conexión con terceros. En la mayoría de las circunstancias, no es factible transferir archivos a usuarios de Teams que no forman parte de la empresa. Recientemente, Max Corbridge (@CorbridgeMax) y Tom Ellson (@tde_sec) de JUMPSEC publicaron un medio para eludir esta limitación modificando las solicitudes HTTP realizadas por Teams para cambiar a quién se le envía un mensaje con un archivo adjunto.

https://noticiasseguridad.com/tutoriales/como-envian-malware-o-mensajes-de-phishing-a-traves-de-teams-esquivando-las-funciones-de-seguridad-de-teams/

El Cibercrimen entre los desafíos clave en ciberseguridad para la Industria Aseguradora

Recientemente, se ha publicado el Informe Banana Skins 2023, realizado por PwC en colaboración con el Centro de Estudios para la Innovación Financiera (CSFI), donde se destaca las principales amenazas que enfrenta la industria aseguradora en la actualidad. Estas amenazas se han identificado como el cibercrimen, la regulación y el cambio climático.

La ciberseguridad en la industria aseguradora es un aspecto fundamental dada la creciente dependencia de la tecnología en este sector. La protección de los datos, la confidencialidad, la integridad y la disponibilidad de la información son críticas para garantizar la confianza de los clientes y el funcionamiento eficiente de las aseguradoras. Aquí se presentan algunos aspectos clave sobre la ciberseguridad en esta industria:

https://cybersecuritynews.es/el-cibercrimen-entre-los-desafios-clave-en-ciberseguridad-para-la-industria-aseguradora/

Los propósitos de año nuevo que todo CISO debe tener en cuenta para 2024

Impulsado principalmente por la consecución de nuevos ciberataques, y sus cada vez más disruptivos daños, la ciberseguridad continúa cobrando poco a poco la importancia que verdaderamente tiene dentro de las empresas. Sin embargo, esta situación está provocando que los CISOs se enfrenten a unos desafíos más complejos.

https://cybersecuritynews.es/los-propositos-de-ano-nuevo-que-todo-ciso-debe-tener-en-cuenta-para-2024/

Multa a TikTok de 345 millones de euros por no proteger la privacidad de los menores

La investigación sobre TikTok se centró en la configuración predeterminada de la plataforma, la función conocida como “Sincronización Familiar” y las medidas de verificación de la edad. La DPC descubrió que, por defecto, TikTok configuraba las cuentas de usuarios menores como públicas al registrarse, lo que conllevaba que los videos subidos por los menores se hacían públicos automáticamente, mientras que las opciones de comentarios, la función “Dúo” (que permite publicar un video al lado de otro creador de TikTok) y la herramienta “Stitch” para reutilizar contenido también se encontraban activadas por activadas por defecto.

https://derechodelared.com/multa-a-tiktok-rgpd-datos-ninos/

La Corte Penal Internacional sufre un ciberataque.

La Corte Penal Internacional (CPI) ha declarado este martes que su sistema informático se ha visto comprometido por una actividad “anómala”. Esto puede suponer una brecha en una de las instituciones internacionales de más alto nivel del mundo y en la que se maneja información extremadamente sensible sobre crímenes de guerra.

La CPI es el tribunal permanente para crímenes de guerra con sede en la ciudad holandesa de La Haya, creado en 2002 para juzgar crímenes de guerra y crímenes contra la humanidad. Los fiscales del tribunal llevan a cabo actualmente 17 investigaciones sobre situaciones en Ucrania, Uganda, Venezuela, Afganistán y Filipinas, entre otros países.

https://derechodelared.com/corte-penal-internacional-ciberataque/

INFORME SEMANAL DE

CIBERAMENAZAS

W39-2023