BOLETÍN DE CIBERSEGURIDAD

AGOSTO 2023

ÍNDICE

NOTICIAS INTERNACIONALES

ANONYMOUS LANZA UN CIBERATAQUE CONTRA LA PLANTA NUCLEAR DE FUKUSHIMA

EL GRUPO CONOCIDO COMO 'ANONYMOUS' HA LLEVADO A CABO UN ATAQUE INFORMÁTICO EN LA JORNADA DE HOY CONTRA LA INSTALACIÓN NUCLEAR DE FUKUSHIMA.

Ep. (2023, 18 agosto). «Anonymous» lanza un ciberataque contra la planta nuclear de Fukushima. Diario ABC. https://www.abc.es/sociedad/anonymous-lanza-ciberataque-planta-nuclear-fukushima-20230818191408-nt.html
Tidy, B. J. (2023, 20 junio). MOVEit hack: Gang claims not to have BBC, BA and Boots data. BBC News. https://www.bbc.com/news/technology-65965453

Como forma de protesta en contra del plan gubernamental japonés, respaldado por el Organismo Internacional de Energía Atómica (OIEA), que busca liberar agua tratada residual en el océano.

La firma de seguridad cibernética NNT ha comunicado que en los últimos meses, 'Anonymous' ha incrementado sus ataques en línea, tras la publicación del informe del OIEA en julio, en el cual se aseguraba que las medidas implementadas por el Gobierno de Fumio Kishida cumplen con los estándares internacionales.

Se espera que Kishida inspeccione las instalaciones de descarga y las condiciones de almacenamiento en la central nuclear durante este fin de semana. Además, se tiene programada una reunión ministerial para determinar el inicio de las operaciones. El periódico 'Sankei' ha informado sobre estos acontecimientos. La decisión de liberar el agua tratada ha suscitado preocupación en varios países de la región, incluyendo Corea del Sur, que ha impuesto restricciones a los productos pesqueros provenientes de la zona de Fukushima. A pesar de esto, Corea del Sur ha indicado que espera un impacto mínimo en sus costas.

El agua, que según el OIEA tiene un bajo impacto radiológico en la población y el medio ambiente, ha sido tratada por el Sistema Avanzado de Procesamiento de Líquidos (ALPS) para eliminar la mayoría de las sustancias radiactivas, a excepción del tritio, un isótopo natural del hidrógeno.

Desde el terremoto y tsunami ocurrido en marzo de 2011, que resultó en la fusión de tres núcleos debido a la pérdida de sistemas de refrigeración de emergencia, se ha acumulado una gran cantidad de agua radiactiva en la planta. Esta agua se ha mezclado con precipitaciones y aguas subterráneas.

PREVIENEN DE UNA ESTAFA A TRAVÉS DE CORREO ELECTRÓNICO ALERTANDO DE LA FALTA DE ESPACIO DE ALMACENAMIENTO EN ICLOUD

EL INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE) HA COMUNICADO A TRAVÉS DE SU SITIO WEB QUE SE HAN DESCUBIERTO UNA SERIE DE MENSAJES DE CORREO ELECTRÓNICO FRAUDULENTOS QUE BUSCAN SUPLANTAR LA IDENTIDAD DE ICLOUD CON EL OBJETIVO DE OBTENER INFORMACIÓN PERSONAL Y FINANCIERA

Abc. (2023, 4 agosto). Previenen de una estafa a través de correo electrónico alertando de la falta de espacio de almacenamiento e. . . Diario ABC. https://www.abc.es/tecnologia/incibe-alerta-estafa-traves-correo-electronico-alertando-20230804211106-nt.html

La Oficina de Seguridad del Internauta ha emitido una advertencia en sus redes sociales, indicando que los usuarios deben estar atentos ya que podría tratarse de un caso de "phishing".

La táctica de estafa involucra el envío de un correo electrónico que notifica a los usuarios que su capacidad de almacenamiento ha excedido su límite. Este correo incluye un enlace que aparentemente ofrece 50GB adicionales de almacenamiento de manera gratuita, como parte de un programa de lealtad. No obstante, si el destinatario hace clic en el enlace, será redirigido a un formulario donde se le pedirán datos personales y bancarios con el propósito de robar esta información. El Incibe informa a los usuarios que el remitente del correo electrónico no utiliza una dirección con un dominio asociado a iCloud; en cambio, parece ser generada de manera aleatoria.

El organismo también señala que, al hacer clic en el enlace, la dirección URL no corresponde al sitio web oficial de iCloud, a pesar de comenzar con "https". Además, el logotipo es diferente, ya que elimina la letra 'i' inicial. Además, el correo combina lenguaje formal y coloquial.

Entre los varios asuntos de correo electrónico identificados, se incluyen "RV: iCloud-est lleno"; "Obtén hasta 50 GB adicionales de almacenamiento en la nube"; "Tus fotos y videos serán eliminados, ¡actúa ahora!"; o "Tu cuenta de iCloud ha sido cerrada". Durante el proceso, se solicitan al usuario detalles como su nombre completo, dirección, número de teléfono y correo electrónico. Si se procede a hacer clic en "continuar", se abrirá otra ventana solicitando información bancaria.

Si el usuario ha recibido este correo electrónico, pero no ha proporcionado ningún dato, el Incibe sugiere marcarlo como correo no deseado y eliminarlo de la bandeja de entrada.
En caso de que el usuario ya haya proporcionado información personal o datos de la tarjeta, el Incibe recomienda contactar con la entidad bancaria y reunir evidencia del fraude guardando los correos electrónicos recibidos y capturas de pantalla del sitio web donde se introdujeron los datos. También sugieren monitorear regularmente los movimientos de la cuenta para identificar cargos no autorizados y reportar el incidente a las autoridades competentes.

El Incibe también ha aconsejado realizar una búsqueda de la presencia en línea (egosurfing) para verificar si los datos personales o financieros han sido expuestos. Si es así, se debe solicitar su eliminación mediante el derecho al olvido.

TENDENCIAS Y DESAFÍOS EN CIBERSEGURIDAD Y TECNOLOGÍA: LO ÚLTIMO EN AMENAZAS Y SOLUCIONES

EN MEDIO DEL PANORAMA FINANCIERO, TITLEMAX HA CAUSADO UN GRAN REVUELO EN SU COMUNIDAD DE CLIENTES, QUE CUENTA CON CASI CINCO MILLONES DE MIEMBROS, AL DESCUBRIR ALGUNAS PREOCUPANTES REVELACIONES.

Cyware. (s. f.). Cyber Security News Today | Articles on cyber security, malware attack updates | Cyware. Cyware Labs. https://cyware.com/cyber-dcr/daily-cybersecurity-roundup-august-25-2023-b07b

Resulta que el incidente de febrero también afectó su información de tarjeta de pago y más. Entidades taiwanesas de diferentes sectores están en peligro, ya que un grupo de amenazas supuestamente vinculado a China las está atacando en una nueva campaña de ciberespionaje. En una actualización diferente, prepárese para sorprenderse por la extensa cantidad de víctimas atacadas por la pandilla de ransomware Cl0p. Siga leyendo para obtener estos datos y más.

TitleMax, un prestamista subprime, está advirtiendo a casi cinco millones de clientes que una brecha de datos en febrero no solo robó sus números de Seguro Social y detalles de pasaporte, como se había revelado anteriormente, sino que también comprometió los datos de su tarjeta de pago y códigos de seguridad.

Microsoft advirtió sobre un grupo de hackers que se cree está vinculado a China, conocido como Flax Typhoon, que está atacando activamente a entidades gubernamentales, empresas de tecnología y organizaciones manufactureras en Taiwán como parte de una campaña de ciberespionaje.

Secureworks descubrió que la botnet Smoke Loader está desplegando un nuevo malware llamado Whiffy Recon. Es un malware de escaneo de Wi-Fi que triangula las ubicaciones de los sistemas infectados utilizando puntos de acceso Wi-Fi cercanos y la API de geolocalización de Google.

Según un estudio de Emsisoft, la campaña MOVEit del grupo de ransomware Cl0p ha afectado a casi 1,000 organizaciones y 60 millones de personas, con más del 80% de las entidades afectadas ubicadas en Estados Unidos.

TENDENCIAS Y DESAFÍOS EN CIBERSEGURIDAD Y TECNOLOGÍA: LO ÚLTIMO EN AMENAZAS Y SOLUCIONES

Los actores de amenazas de ransomware están pasando menos tiempo en las redes comprometidas, con un tiempo de permanencia mediano que ha disminuido a cinco días en la primera mitad de 2023, según informó Sophos. También afirmó que los ataques de ransomware representaron el 68.75% de todos los ataques.

Los investigadores descubrieron una nueva cepa de ransomware llamada TZW, que se dirige a individuos y pequeñas empresas y exige rescates más bajos en comparación con otros ransomware. Esta cepa pertenece a la familia de ransomware Adhubllka.

El NIST publicó un borrador de estándares de Criptografía Post-Cuántica (PQC) para uso global, con el objetivo de proteger a las organizaciones de posibles ciberataques habilitados por futuros ordenadores cuánticos.

El HSCC CWG publicó una versión actualizada de la guía Mejores Prácticas de Compartir Información de Ciberseguridad de la Industria de la Salud que tiene como objetivo ayudar a las organizaciones de atención médica a establecer y mantener programas efectivos de intercambio de información sobre amenazas de ciberseguridad.

La plataforma de automatización de ciberseguridad GRC basada en SaaS, Cypago, recaudó $13 millones en financiamiento inicial y $2 millones en financiamiento de deuda de Entrée Capital, Axon Ventures y Jump Capital.

Malwarebytes anunció la adquisición del proveedor de soluciones de privacidad en línea Cyrus, con el objetivo de fortalecer su compromiso con la privacidad y dar a los usuarios más control sobre su información. Los términos del acuerdo no fueron revelados.

BRECHA DE SEGURIDAD EN HOSPITAL DE ILLINOIS: DATOS PERSONALES DE CIENTOS DE MILES COMPROMETIDOS

ESTE COMPLEMENTO ESTÁ DISEÑADO PARA QUE SEA MÁS FÁCIL PARA LOS USUARIOS REGISTRARSE E INICIAR SESIÓN EN SU SITIO WEB.

Cyware. (s. f.-b). Cyber Security News Today | Articles on cyber security, malware attack updates | Cyware. Cyware Labs. https://cyware.com/cyber-dcr/daily-cybersecurity-roundup-august-18-2023-e008

Después de que el grupo de ransomware Royal afirmara que Morris Hospital fue su víctima en mayo, el centro de atención médica ha concluido su investigación y notificado a aproximadamente 250,000 personas sobre la violación de seguridad. APT29, también conocido como Nobelium, ha lanzado una nueva campaña de spear-phishing dirigida a entidades asociadas con la OTAN. ¿Cuál es el delito en línea más dominante? El phishing. Y está en aumento. Lea las estadísticas y más de las últimas 24 horas.

El Hospital y Centros de Atención Médica Morris, Illinois, informaron a 248,943 personas sobre un incidente de ciberseguridad que descubrieron el 4 de abril. La información comprometida incluye números de Seguro Social, números de registros médicos, códigos de diagnóstico y otros datos personales de pacientes y empleados actuales y anteriores.

Los investigadores descubrieron una campaña de spear-phishing en curso llevada a cabo por el grupo de ciberespionaje ruso APT29, dirigida a Ministerios de Relaciones Exteriores en países alineados con la OTAN. La campaña utilizó dos archivos PDF, siendo uno de ellos un vector para el malware Duke.

Los pacientes del Hospital Jefferson Cherry Hill, Nueva Jersey, han sido notificados sobre una posible brecha de datos después de que se extraviara un disco duro de respaldo de una máquina de escaneo DEXA. El disco de respaldo contenía información sensible como números de registros médicos, números de Seguro Social y más. Los investigadores de ESET descubrieron una nueva campaña de ingeniería social dirigida a usuarios del servidor de correo electrónico Zimbra Collaboration, que tiene como objetivo recopilar credenciales de inicio de sesión a través de correos electrónicos de phishing. Está dirigida principalmente a pequeñas y medianas empresas y entidades gubernamentales en Polonia, Ecuador, México, Italia y Rusia.

BRECHA DE SEGURIDAD EN HOSPITAL DE ILLINOIS: DATOS PERSONALES DE CIENTOS DE MILES COMPROMETIDOS

Después de que el grupo de ransomwaEl grupo de amenazas APT de China, Bronze Starlight, está apuntando al sector de los juegos de azar del sudeste asiático, utilizando la usurpación de DLL y ransomware como tácticas de distracción, según advirtió SentinelOne. Están aprovechando fallos en Adobe Creative Cloud, Microsoft Edge y McAfee VirusScan para desplegar beacons de Cobalt Strike.

Según informes, funcionarios de las Escuelas de la Ciudad de Cleveland en Tennessee están abordando un incidente de ransomware que ha afectado a una fracción menor, menos del 5%, de los dispositivos de su sistema. Afortunadamente, no se ha comprometido ningún dispositivo de estudiantes.

Zimperium zLabs encontró 3,300 muestras de aplicaciones públicas que utilizan un método de compresión no compatible para dificultar su análisis. De estas, 71 eran maliciosas y se distribuían fuera de la Play Store. La mayoría de estas muestras están tan dañadas que el sistema operativo Android no puede cargarlas.

Un nuevo informe de Cloudflare señaló un aumento del 35.6% en el uso de enlaces maliciosos como la principal tendencia en ataques de phishing entre mayo de 2022 y mayo de 2023. También encontró que las estafas BEC causaron pérdidas de alrededor de $50 mil millones durante ese período.

Según la Oficina Federal de Policía Criminal de Alemania (BKA), el país registró 136,865 casos de ciberdelitos en 2022, con una pérdida estimada de €203 mil millones ($220 mil millones). También se señaló que, mientras que los ciberdelitos domésticos disminuyeron, los delitos cometidos por actores extranjeros aumentaron un 8%.

La CISA emitió su Plan de Defensa Cibernética RMM para abordar los crecientes riesgos asociados con la explotación de software de Monitoreo y Administración Remota (RMM), que a menudo es el objetivo de actores de amenazas cibernéticas en ataques de ransomware.

NOTICIAS NACIONALES

CAIMÁN MANIPULADO, EL GRUPO QUE HACKEA A CUENTAHABIENTES DE MÉXICO

UN GRUPO DE HACKERS HA ELEGIDO A LOS TITULARES DE CUENTAS BANCARIAS EN MÉXICO COMO SUS OBJETIVOS.

Riquelme, R. (2023, 22 agosto). Caimán manipulado, el grupo que hackea a cuentahabientes de México. El Economista. https://www.eleconomista.com.mx/tecnologia/Caiman-Manipulado-el-grupo-que-hackea-a-cuentahabientes-de-Mexico-20230821-0065.html

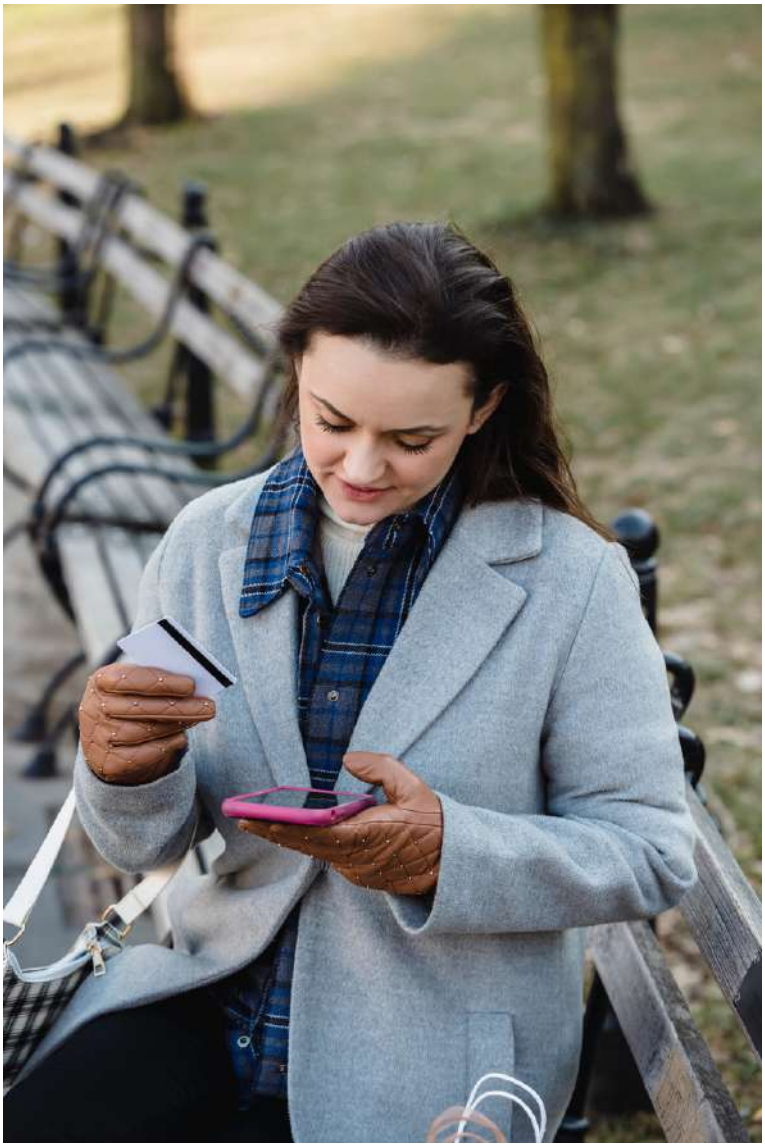
Según un informe de la firma israelí de ciberseguridad Perception Point, el grupo denominado "Caimán Manipulado" ha accedido a las cuentas bancarias de unas 4,000 personas en México.

Este ciberataque está dirigido específicamente a personas y organizaciones con una dirección de Internet (IP) que se encuentra en México, lo que significa que solo afecta a usuarios en ese país.

Perception Point detectó una extensa campaña de phishing dirigida a individuos y organizaciones que son clientes de cinco de los bancos más grandes en México, la cual tuvo lugar a finales de mayo de 2023. El objetivo final de esta campaña de hacking era obtener acceso a las cuentas bancarias de las víctimas. El phishing es una técnica de ingeniería social mediante la cual los ciberatacantes intentan engañar a sus posibles víctimas para obtener acceso o privilegios en un sistema. Según el Estudio sobre el estado global de la ciberseguridad 2023 de la firma estadounidense Infoblox, el 59% de las organizaciones mexicanas informó al menos un ataque de phishing en el último año.

Los atacantes engañaron a sus víctimas mediante correos electrónicos que notificaban la supuesta entrega de un comprobante fiscal digital (CFDI) en un archivo con formato ZIP que aparentaba contener un archivo PDF y otro XML.

CAIMÁN MANIPULADO, EL GRUPO QUE HACKEA A CUENTAHABIENTES DE MÉXICO



Dicho archivo ZIP contenía una dirección URL que ejecutaba un código malicioso. Inicialmente, mostraba un mensaje de error y luego realizaba una solicitud a otra dirección URL. Esta nueva dirección URL descargaba dos archivos que recopilaban información de la computadora o el teléfono de la víctima, como la configuración de idioma y la ubicación de la dirección de Internet (IP).

Si la respuesta provenía de una dirección IP en México, el código ejecutaba el software malicioso. Si provenía de una dirección fuera de México, el código redirigía a otro sitio web y se detenía (práctica conocida como geofencing). El código verificaba si en el dispositivo de la víctima se abría una ventana o aplicación con el nombre de los bancos objetivo y, en caso afirmativo, descargaba dos archivos ejecutables que se encargaban de acceder a la cuenta bancaria para sustraer fondos.

Perception Point afirmó haber accedido a los servidores de Caimán Manipulado, lo que les permitió conocer la cantidad de usuarios infectados, así como sus saldos, la fecha de infección, las transacciones más recientes y, en algunos casos, capturas de pantalla de sus cuentas bancarias. La compañía estimó que había más de 4,000 víctimas en total, con posibles ingresos de hasta 55 millones de dólares (cabe señalar que esta cifra se basa en el saldo en el momento de la infección).

PHISHING AUMENTÓ 10 VECES MÁS EN MÉXICO

EL AUMENTO EN LA CANTIDAD DE MENSAJES FRAUDULENTOS, TANTO EN MÉXICO COMO EN TODA AMÉRICA LATINA

El Economista. (2023, 24 agosto). Phishing aumentó 10 veces más en México. El Economista. https://www.eleconomista.com.mx/finanzaspersonales/Phishing-aumento-10-veces-mas-en-Mexico-20230823-0097.html

se debe principalmente a la normalización de las actividades económicas después de la pandemia, según informó Kaspersky, una empresa especializada en ciberseguridad.

Kaspersky señaló que el phishing ha experimentado un crecimiento notable en México, llegando a aumentar diez veces desde el reinicio de la actividad económica.

La empresa destacó que en el último año, ha registrado un total de 286 millones de bloqueos de intentos de phishing, lo que representa un incremento del 617% en comparación con los doce meses anteriores. Esto equivale a un promedio de 4,000 ataques por minuto en México.

Además, otro tipo de ataque que ha experimentado un aumento significativo en los últimos doce meses en México es el de troyanos bancarios, con un crecimiento del 41%, según el estudio Panorama de Amenazas para América Latina de Kaspersky.

CIBERDELITOS PRENDEN FOCOS ROJOS EN COMBATE AL LAVADO DE DINERO

EL INCREMENTO DE LOS CIBERDELITOS SE HA CONVERTIDO EN UNA PREOCUPACIÓN CRECIENTE, NO SOLO EN MÉXICO SINO EN TODA AMÉRICA LATINA

Saldívar, B. (2023, 25 agosto). Ciberdelitos prenden focos rojos en combate al lavado de dinero. El Economista. https://www.eleconomista.com.mx/economia/Ciberdelitos-prenden-focos-rojos-en-combate-al-lavado-de-dinero-20230824-0147.html

Representa uno de los desafíos principales que deben abordarse en la lucha contra el lavado de dinero, según advirtió Elisa de Anda Madrazo, quien anteriormente ocupó el cargo de vicepresidenta del Grupo de Acción Financiera Internacional (GAFI).

De Anda Madrazo señaló que los ciberdelitos, como el phishing y el ransomware, han aumentado considerablemente, en gran parte debido a la normalización de las actividades económicas después de la pandemia. Estos delitos representan una amenaza importante para la seguridad financiera y la integridad de las personas y las organizaciones.

En particular, destacó que las ganancias obtenidas por los hackers a través de ataques de ransomware han encontrado refugio en el uso de criptomonedas, lo que plantea preocupaciones adicionales para el sistema financiero.

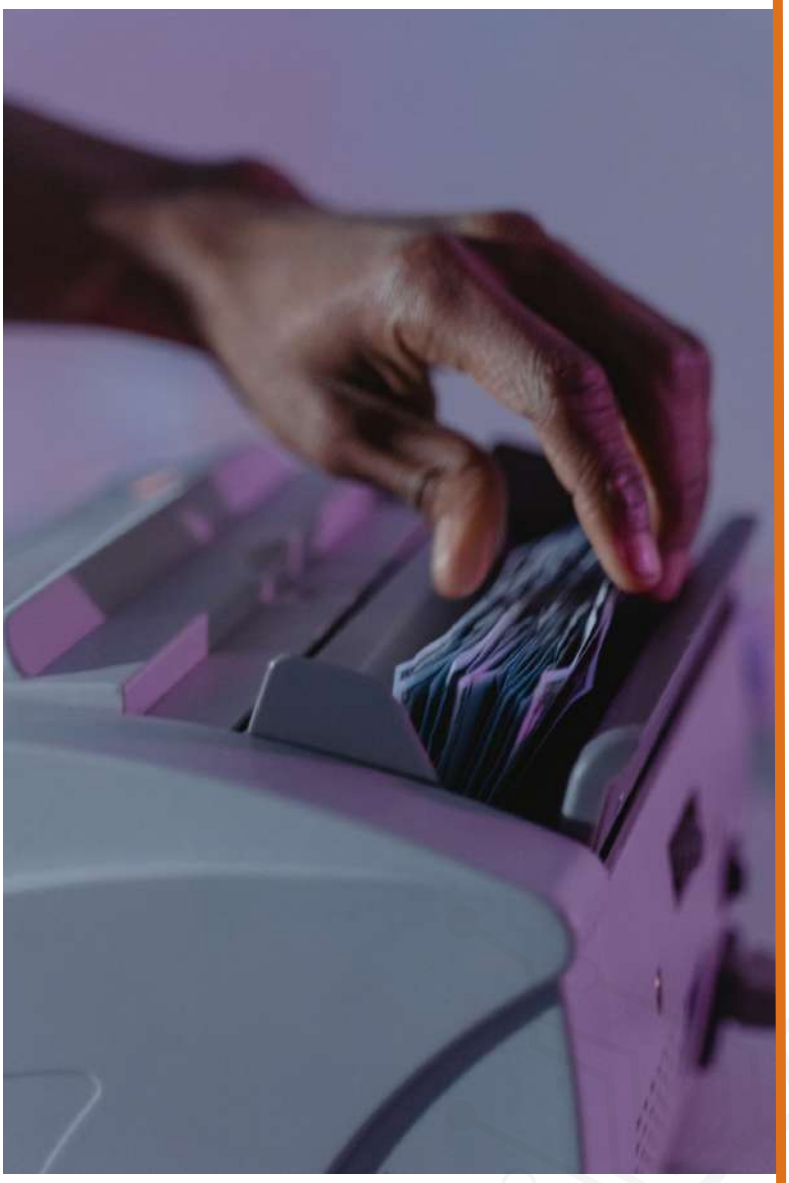
La ex vicepresidenta del GAFI subrayó que estudios indican que aproximadamente uno de cada tres dispositivos electrónicos en los hogares tiene ransomware, lo que subraya la extensión de esta amenaza. De Anda Madrazo instó a estar alerta ante los ciberdelitos, ya que representan uno de los mayores riesgos para los ciudadanos. Además del ransomware, señaló que otros tipos de delitos cibernéticos, como el phishing, hacking y malware, también han ganado relevancia en los últimos años.

CIBERDELITOS PRENDEN FOCOS ROJOS EN COMBATE AL LAVADO DE DINERO

El GAFI es una organización intergubernamental que tiene como objetivo establecer normas y promover la aplicación efectiva de medidas legales y operativas para combatir el lavado de dinero, el financiamiento al terrorismo y otras amenazas relacionadas con la integridad del sistema financiero internacional.

Por su parte, Daniel Quintero Chávez, titular de la Unidad de Inteligencia Financiera (UIF) de la Ciudad de México, señaló que el lavado de dinero presenta desafíos adicionales debido a restricciones legales que deben respetarse. Indicó que el lavado de dinero es una actividad frecuente, aunque a veces no se identifica de inmediato o se confunde con el enriquecimiento ilícito.

Quintero Chávez destacó que, como autoridades, deben respetar la legalidad y el debido proceso, lo que a veces dificulta las investigaciones sobre lavado de dinero. Además, mencionó que algunas fiscalías y funcionarios carecen de capacitación en este campo, lo que a menudo resulta en investigaciones incorrectas.



En México, se estima que en el 2021 se lavaron entre 18,000 y 44,000 millones de dólares, según Global Financial Integrity. Sin embargo, Quintero Chávez sugirió que esta cifra podría ser aún mayor. La UIF federal reportó que entre enero y junio de este año se presentaron 79 denuncias relacionadas con diversos delitos financieros, involucrando a 839 sujetos en total. Estas denuncias incluyeron casos de fraude, defraudación fiscal, delitos contra la salud, delincuencia organizada y operaciones con recursos de procedencia ilícita.

VIOLENCIA DIGITAL EN MÉXICO AFECTA MÁS A MUJERES Y GENERA MAYOR CONSCIENCIA ENTRE ELLAS

EN AUSTIN, TEXAS, AL IGUAL QUE EN LOS ESPACIOS FÍSICOS, SE PRODUCEN EVENTOS EN EL ÁMBITO DIGITAL QUE TIENEN UN IMPACTO SIGNIFICATIVO EN LA VIDA DE LAS PERSONAS.

García, A. K. (2023, 29 agosto). Violencia digital en México afecta más a mujeres y genera mayor consciencia entre ellas. El Economista. https://www.eleconomista.com.mx/arteseideas/Violencia-digital-en-Mexico-afecta-mas-a-mujeres-y-genera-mayor-consciencia-entre-ellas-20230829-0036.html

En México, ocho de cada diez personas mayores de seis años utilizan internet, y en promedio, los usuarios pasan alrededor de cuatro horas y media navegando en plataformas y redes sociales.

El acceso efectivo a la conectividad se ha convertido en un derecho humano fundamental. Internet ofrece la posibilidad de establecer amistades, encontrar parejas, buscar empleo, comunicarse instantáneamente con personas de todo el mundo, obtener información sobre eventos globales, solicitar ayuda en situaciones de emergencia, disfrutar de películas y generar ingresos.

Sin embargo, también en internet se pueden experimentar situaciones de agresión. La violencia digital es una realidad y, de manera similar a lo que ocurre en el mundo físico, refleja estructuras de discriminación hacia ciertos grupos de población, acoso en entornos educativos y desigualdades de género.

En México, uno de cada dos usuarios de internet ha sido víctima de acoso digital o conoce a alguien que lo ha experimentado. Las mujeres y las personas pertenecientes a la comunidad LGBTQ+ son particularmente vulnerables, ya que el 95% y el 75% de las personas de estos grupos, respectivamente, han sufrido agresiones en línea, según una encuesta sobre ciberacoso realizada por Bumble en colaboración con Ipsos.

VIOLENCIA DIGITAL EN MÉXICO AFECTA MÁS A MUJERES Y GENERA MAYOR CONSCIENCIA ENTRE ELLAS

Además, las mujeres son más conscientes de la existencia de la violencia digital en comparación con los hombres. Mientras que el 93% de las mujeres considera que ocurre con frecuencia, solo el 81% de los hombres comparte esta percepción. La encuesta revela que en todos los tipos de agresiones en línea, las mujeres son más conscientes, con la mayor brecha en la categoría de "body shaming" o comentarios humillantes relacionados con la apariencia física, donde el 79% de las mujeres reconoce su existencia en comparación con el 69% de los hombres.

La violencia digital limita el ejercicio del derecho a internet y a una vida libre de violencia. Además, tiene un impacto significativo en la vida diaria de quienes la experimentan, causando ansiedad, estrés y problemas de salud mental. Muchos sobrevivientes han tenido que cambiar sus hábitos de uso de internet, ajustar la configuración de privacidad en sus redes sociales, denunciar agresiones y, en algunos casos, dejar de utilizar las redes sociales por completo o cortar el contacto con amigos y familiares.

Para abordar eficazmente la violencia digital, es esencial que todos los sectores involucrados, incluyendo las autoridades locales y federales, las plataformas en línea, las empresas y la sociedad en general, refuercen y coordinen acciones en áreas como la prevención, el monitoreo, el seguimiento y la aplicación de justicia. Además, es fundamental desarrollar y aplicar regulaciones claras relacionadas con la violencia digital, implementar sistemas de denuncia efectivos y garantizar la accesibilidad para presentar denuncias y obtener información sobre el tema.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: AGOSTO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-3162	08/31/2023	The Stripe Payment Plugin for WooCommerce plugin.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-3162

Descripción: He Stripe Payment Plugin for WooCommerce plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.7.7. This is due to insufficient verification on the user being supplied during a Stripe checkout through the plugin. This allows unauthenticated attackers to log in as users who have orders, who are typically customers.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-4596	08/29/2023	The Forminator plugin for WordPress is vulnerable to arbitrary file uploads.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-3162

Descripción: The Forminator plugin for WordPress is vulnerable to arbitrary file uploads due to file type validation occurring after a file has been uploaded to the server in the upload_post_image() function in versions up to, and including, 1.24.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.

TABLA DE VULNERABILIDADES RELEVANTES: AGOSTO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-23770	08/29/2023	Motorola MBTS Site Controller accepts hard-coded backdoor password.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-23770

Descripción: The Motorola MBTS Site Controller Man Machine Interface (MMI), allowing for service technicians to diagnose and configure the device, accepts a hard-coded backdoor password that cannot be changed or disabled.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-26270	08/27/2023	IBM Security Guardium Data Encryption (IBM Guardium Cloud Key Manager (GCKM) 1.10.3))	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-26270

Descripción: Could allow a remote attacker to execute arbitrary code on the system, caused by an angular template injection flaw. By sending specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 248119.

TABLA DE VULNERABILIDADES RELEVANTES: AGOSTO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2019-13690	08/25/2023	Inappropriate implementation in OS in Google Chrome	CVSS v3.1:9.6[critical]	https://nvd.nist.gov/vuln/detail/CVE-2019-13690

Descripción: On ChromeOS prior to 75.0.3770.80 allowed a remote attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: High).

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-32757	08/25/2023	e-Excellence U-Office Force file uploading function does not restrict upload of file with dangerous type.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-32757

Descripción: On ChromeOS prior to 75.0.3770.80 allowed a remote attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: High).

TABLA DE VULNERABILIDADES RELEVANTES: AGOSTO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2021-32292	08/22/2023	An issue was discovered in json-c through 0.15-20200726.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2021-32292

Descripción: A stack-buffer-overflow exists in the function parseit located in json_parse.c. It allows an attacker to cause code Execution.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-4448	08/20/2023	A vulnerability was found in OpenRapid RapidCMS 1.3.1 and classified as critical.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-4448

Descripción: This issue affects some unknown processing of the file admin/run-movepass.php. The manipulation of the argument password/password2 leads to weak password recovery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 4dff387283060961c362d50105ff8da8ea40bcbe. It is recommended to apply a patch to fix this issue. The identifier VDB-237569 was assigned to this vulnerability.

TABLA DE VULNERABILIDADES RELEVANTES: AGOSTO 2023

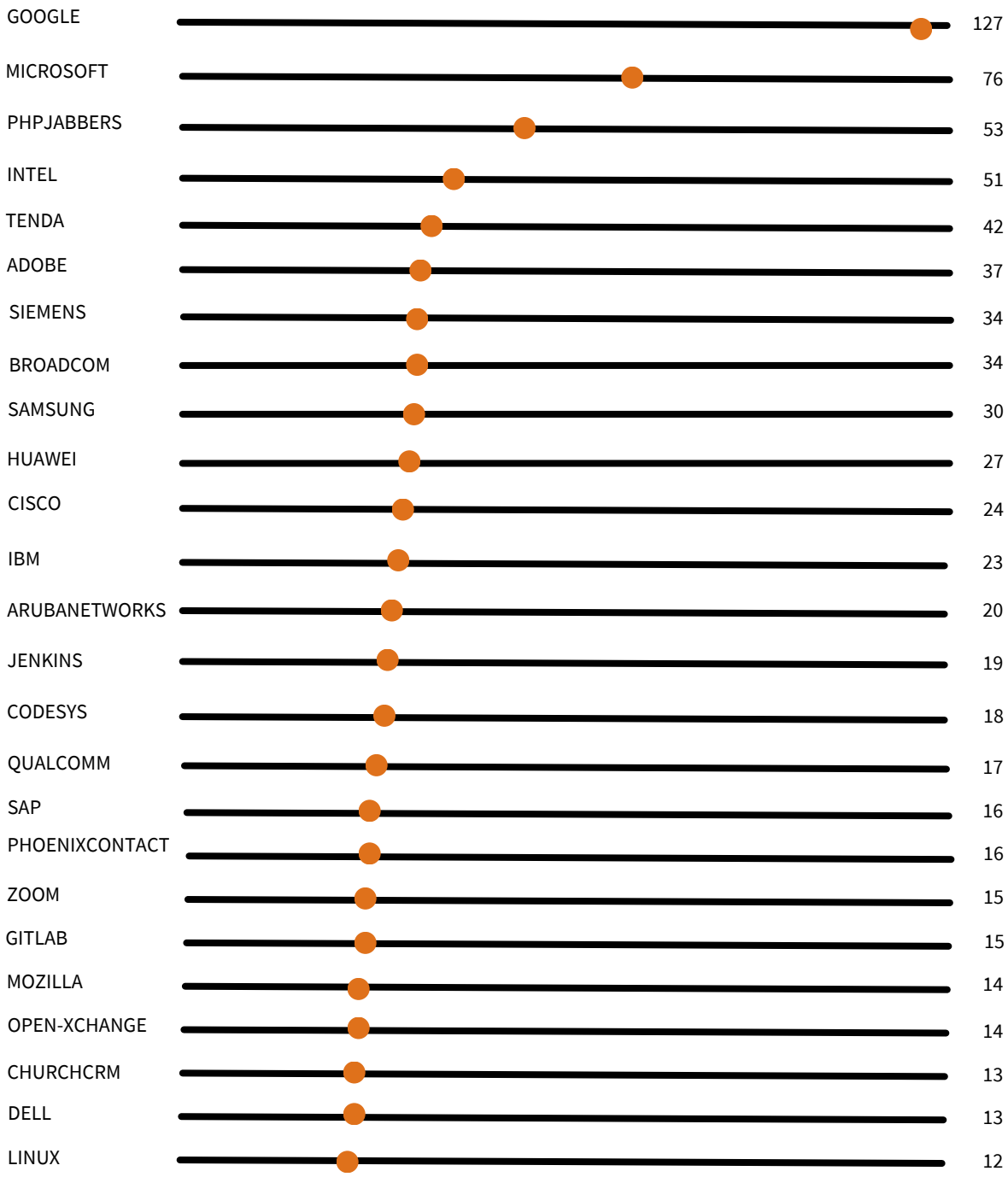
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-2917	08/17/2023	The Rockwell Automation Thinmanager Thinserver is impacted by an improper input validation vulnerability.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-2917

Descripción: Due to an improper input validation, a path traversal vulnerability exists, via the filename field, when the ThinManager processes a certain function. If exploited, an unauthenticated remote attacker can upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. A malicious user could exploit this vulnerability by sending a crafted synchronization protocol message and potentially gain remote code execution abilities.

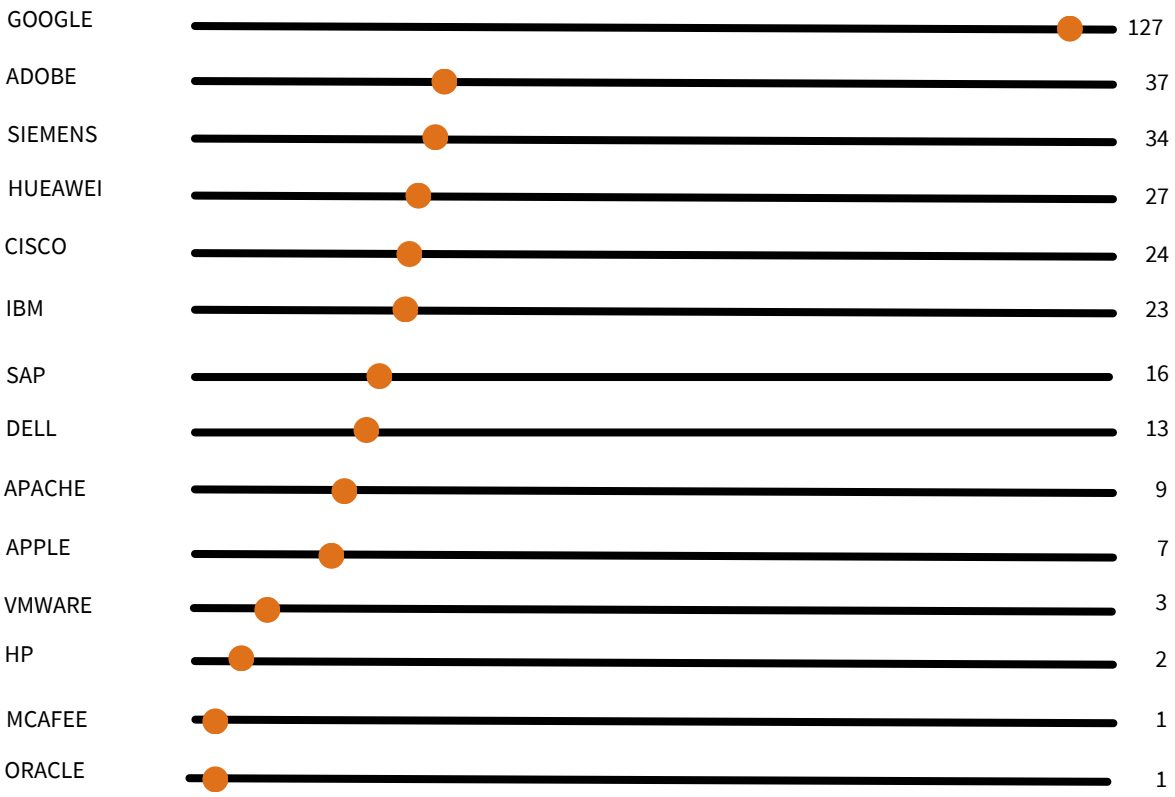
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-32748	08/14/2023	The Linux DVS server component of Mitel MiVoice Connect through 19.3 SP2 (22.24.1500.0)	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-32748

Descripción: Could allow an unauthenticated attacker with internal network access to execute arbitrary scripts due to improper access control.

FABRICANTES CON VULNERABILIDADES RELEVANTES: AGOSTO DE 2023



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: AGOSTO DE 2023



CULTURA DE CIBERSEGURIDAD

ROOTKIT

Un rootkit es un paquete de software malicioso diseñado para permitir el acceso no autorizado a un equipo o a otro software. Los rootkits son difíciles de detectar y pueden ocultar su presencia en un sistema infectado.

Cuando un rootkit se instala en el sistema operativo, este se comporta como un equipo zombi y el hacker puede usar el acceso remoto para ejercer un control absoluto de su dispositivo.

Scranos, un rootkit que roba las contraseñas y los datos de pago almacenados en su navegador. Además, convierte su equipo en una granja de clics para generar ingresos derivados de los vídeos y suscriptores de YouTube a escondidas.

¿CÓMO EVITARLO?

- Realizar respaldos de la información o activos de la empresa y generar copias de seguridad de tus datos en múltiples fuentes.
- No instalar o abrir archivos adjuntos de correo electrónico de remitentes desconocidos o de fuentes no oficiales.
- Actualizar constantemente el software utilizado por la empresa, y realice periódicamente análisis completos de la infraestructura.

¿CÓMO DETECTARLO?

- Análisis del volcado de memoria: Cuando un equipo Windows se bloquea, genera un archivo llamado volcado de memoria o volcado de bloqueo. Un especialista puede examinar este archivo para identificar el origen del bloqueo y ver si fue causado por un rootkit.
- Realizar escaneos peridicos mediante el antivirus para detectar archivos sospechosos.

¿CÓMO CONTENERLO?

Análisis de firmas: La firma de un software es el conjunto de números que sirve como su representación y se puede analizar su equipo con una base de datos de firmas de rootkits conocidos para comprobar si se encuentra alguna de ellas.

¿CÓMO SOLUCIONARLO/REMEDIARLO?

- Ejecutar un software de eliminación de rootkits.
- Realizar un análisis al inició del sistema operativo.
- Reinstalar el sistema operativo en sistemas de almacenamiento sanitizados.

¿CÓMO DETECTARLO?

Es recomendable realizar campañas de concientización respecto al uso correcto de las herraemintas de trabajo, así como el uso de politicas de contraseñas robustas. Cabe destacar que el uso de un AV o EDR ayuda a proteger los equipos de malware y se recomienda hacer uso de este para la protección de la empresa.

REFERENCIAS

REFERENCIAS

- https://www.abc.es/sociedad/anonymous-lanza-ciberataque-planta-nuclear-fukushima-20230818191408-nt.html
- https://www.abc.es/tecnologia/incibe-alerta-estafa-traves-correo-electronico-alertando-20230804211106-nt.html
- https://cyware.com/cyber-dcr/daily-cybersecurity-roundup-august-25-2023-b07b
- https://cyware.com/cyber-dcr/daily-cybersecurity-roundup-august-18-2023-e008
- https://telefonicatech.com/actualidad/bytehide-gana-la-startup-cloud-competition-proyecto-ciberseguridad-en-cloud
- https://telefonicatech.com/actualidad/1600-cest-good-tech-times-optimiza-tu-gasto-en-la-nube-con-aws-by-acens
- https://www.eleconomista.com.mx/tags/ciberseguridad
- https://esemanal.mx/2023/06/mexico-avanza-hacia-una-ley-de-ciberseguridad/
- https://www.redseguridad.com/actualidad/cibercrimen/rootkit-definicion-tipos-y-proteccion-ante-este-malware_20210712.html
- https://www.bitdefender.es/consumer/support/answer/14411/
- https://www.kaspersky.com/resource-center/definitions/what-is-rootkit

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 55 6178 9397

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300