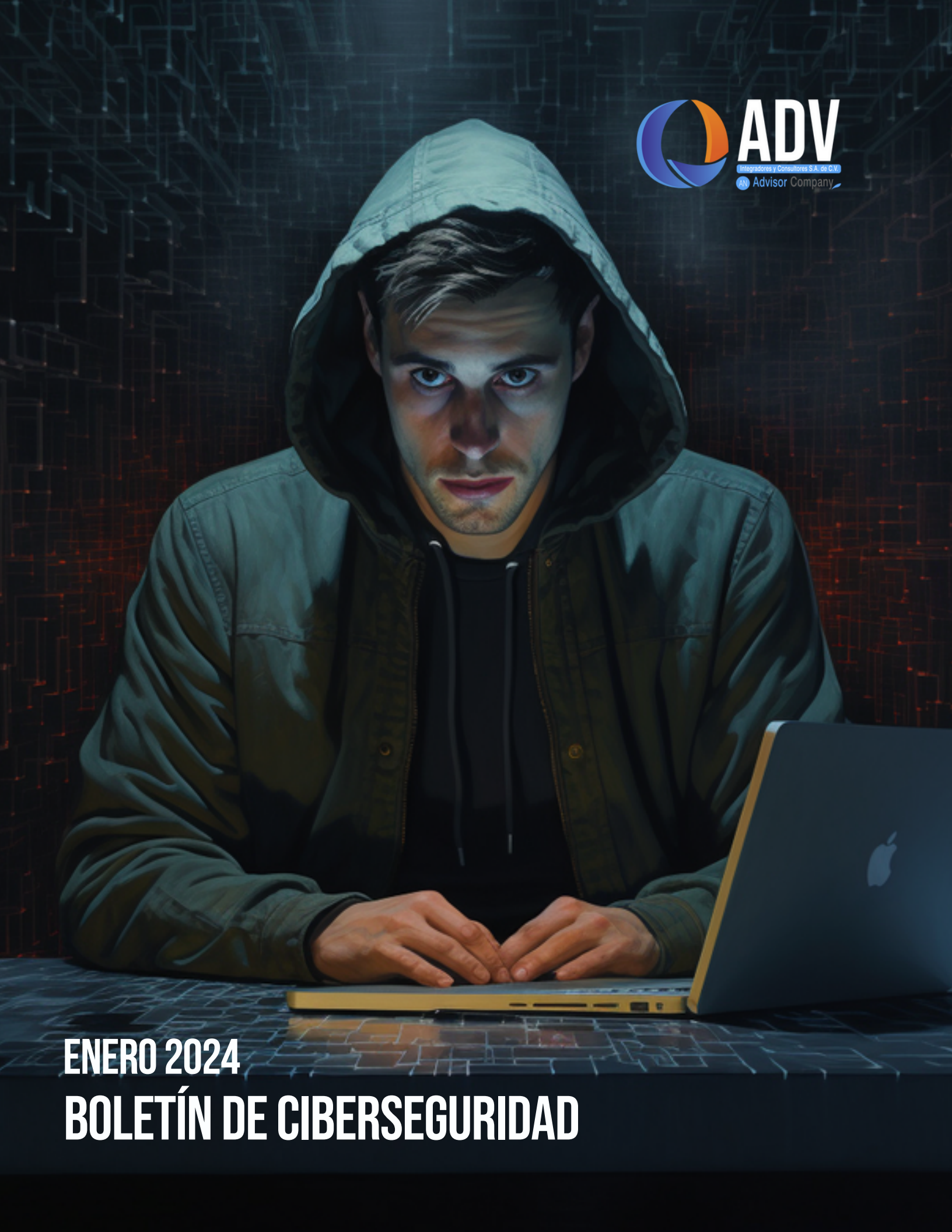


ADV
Integradores y Consultores S.A. de C.V.
Advisor Company

ENERO 2024

BOLETÍN DE CIBERSEGURIDAD

ÍNDICE

NOTICIAS INTERNACIONALES 3

Los investigadores descubren cómo una vulnerabilidad de Outlook podría filtrar sus contraseñas NTLM 4

El NCSC advierte de que la amenaza mundial del ransomware aumentará con la IA 6

La cuenta X de Mandiant fue pirateada mediante un ataque de fuerza bruta a la contraseña 9

Schneider Electric confirma el acceso a datos en un ataque de ransomware 11

NOTICIAS NACIONALES 14

Extracción de datos personales de periodistas fue a través de la cuenta de un exempleado: Gobierno federal 15

Ciberseguridad en crisis: México enfrenta escasez crítica de expertos 18

VULNERAVILIDADES RELEVANTES 20

Tabla de vulnerabilidades relevantes: Diciembre 2023 21

Fabricantes y sus vulnerabilidades relevantes: Diciembre2023 26

Empresas Multinacionales y sus vulnerabilidades: Diciembre 2023 26

CULTURA DE CIBERSEGURIDAD 27

Incident Response. 28

REFERENCIAS 29

NOTICIAS INTERNACIONALES

LOS INVESTIGADORES DESCUBREN CÓMO UNA VULNERABILIDAD DE OUTLOOK PODRÍA FILTRAR SUS CONTRASEÑAS NTLM

UNA VULNERABILIDAD DE SEGURIDAD EN MICROSOFT OUTLOOK, YA CORREGIDA, PODRÍA SER APROVECHADA POR ACTORES MALINTENCIONADOS

Una vulnerabilidad de seguridad en Microsoft Outlook, ya corregida, podría ser aprovechada por actores malintencionados para acceder a contraseñas hash NT LAN Manager (NTLM) v2 al abrir un archivo especialmente diseñado.

Este problema, identificado como CVE-2023-35636 (puntuación CVSS: 6.5), fue abordado por el gigante tecnológico como parte de sus actualizaciones del "Patch Tuesday" de diciembre de 2023.

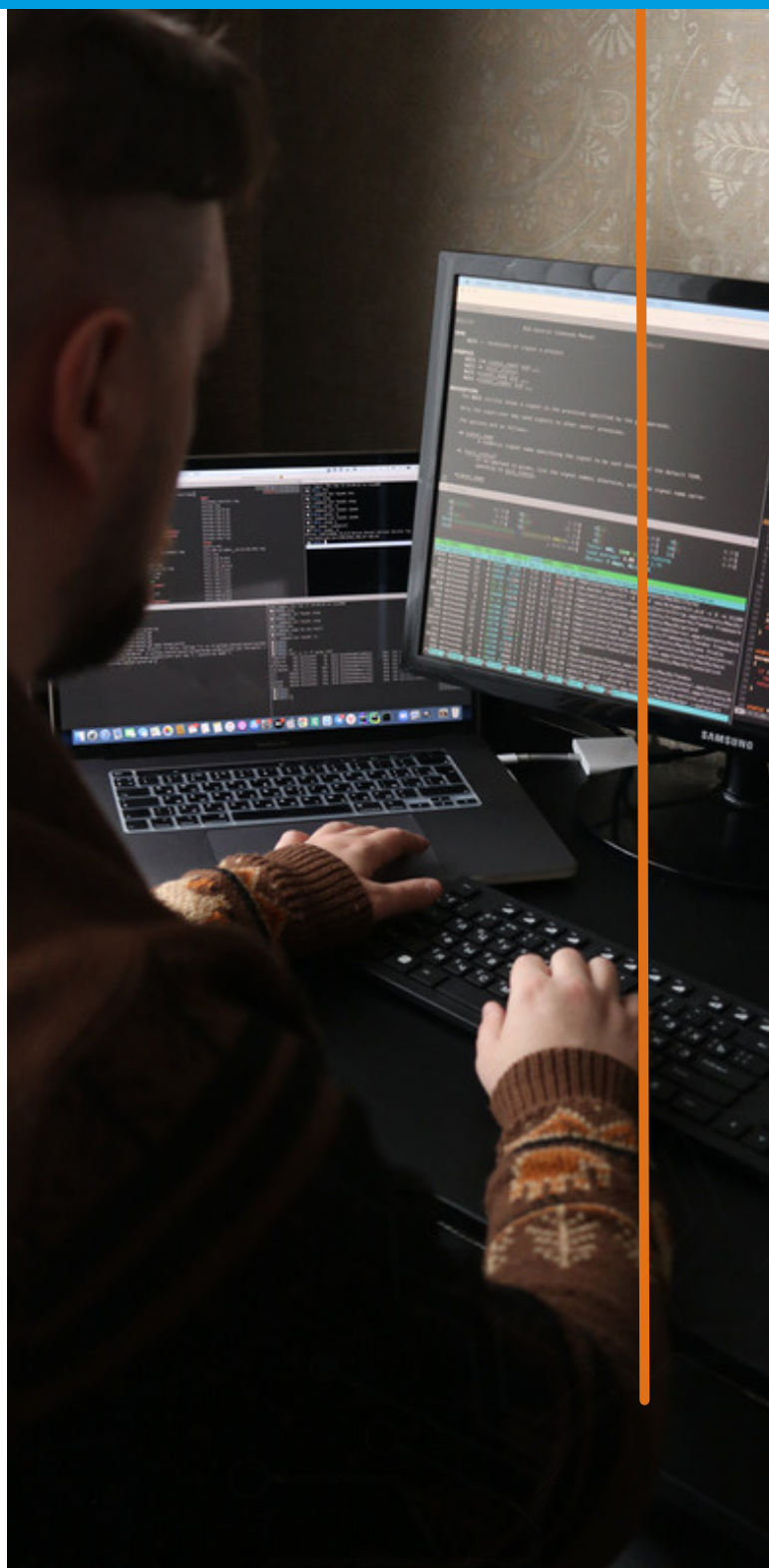
En un escenario de ataque por correo electrónico, un atacante podría explotar la vulnerabilidad al enviar el archivo especialmente diseñado al usuario y convencerlo de abrir el archivo, según un aviso publicado por Microsoft el mes pasado.

En un escenario de ataque basado en web, un atacante podría alojar un sitio web (o aprovechar un sitio comprometido que acepta o aloja contenido proporcionado por el usuario) que contenga un archivo especialmente diseñado para explotar la vulnerabilidad.

En otras palabras, el adversario tendría que persuadir a los usuarios para que hagan clic en un enlace, ya sea incrustado en un correo electrónico de phishing o enviado a través de un mensaje instantáneo, y luego engañarlos para que abran el archivo en cuestión.

El CVE-2023-35636 se origina en la función de intercambio de calendarios en la aplicación de correo electrónico Outlook, donde se crea un mensaje de correo electrónico malicioso insertando dos encabezados, "Content-Class" y "x-sharing-config-url", con valores manipulados para exponer el hash NTLM de la víctima durante la autenticación.

Dolev Taler, investigador de seguridad de Varonis, a quien se le atribuye el descubrimiento y reporte del error,

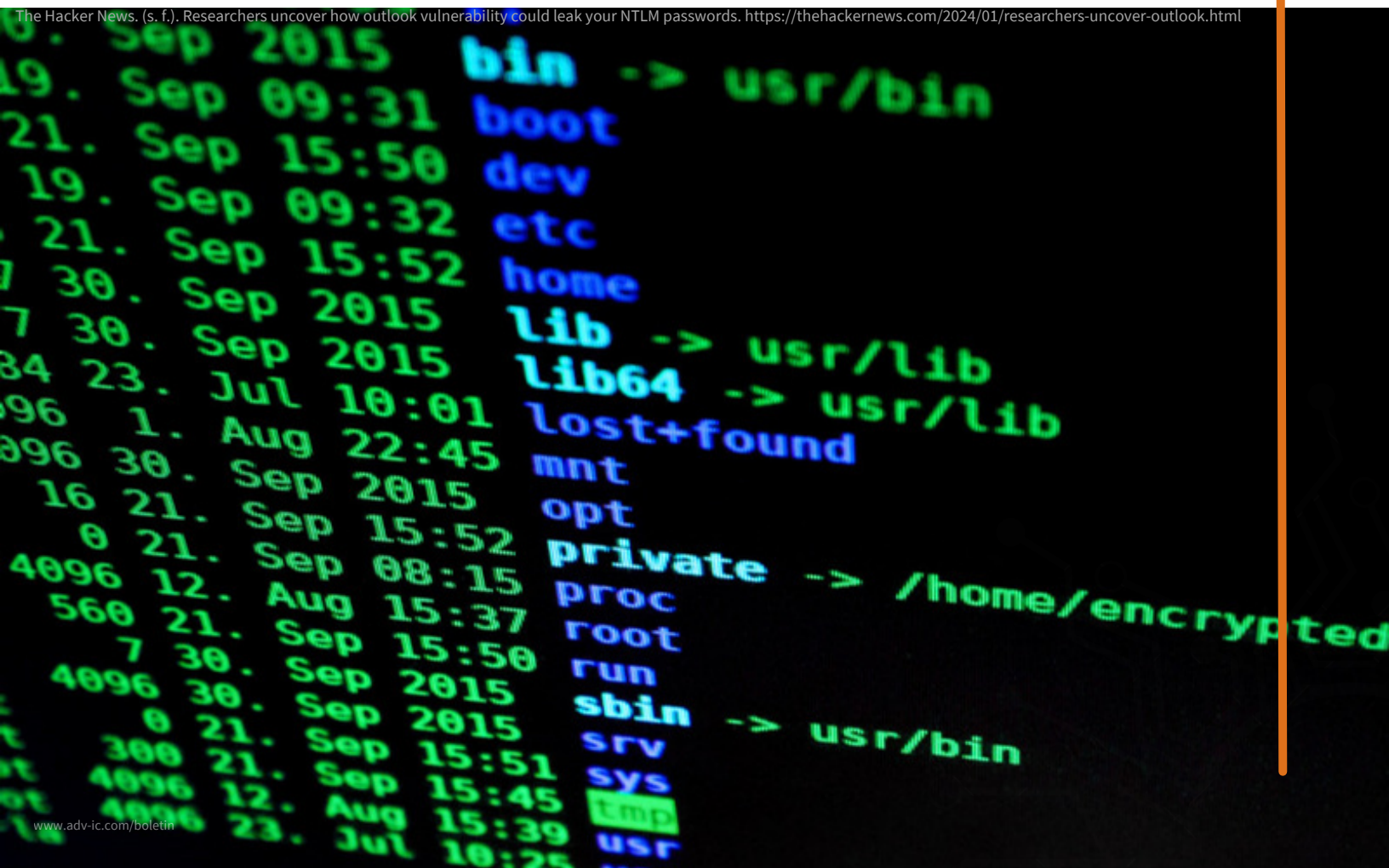


mencionó que los hashes NTLM podrían filtrarse aprovechando Windows Performance Analyzer (WPA) y Windows File Explorer. Sin embargo, estos dos métodos de ataque permanecen sin parchear.

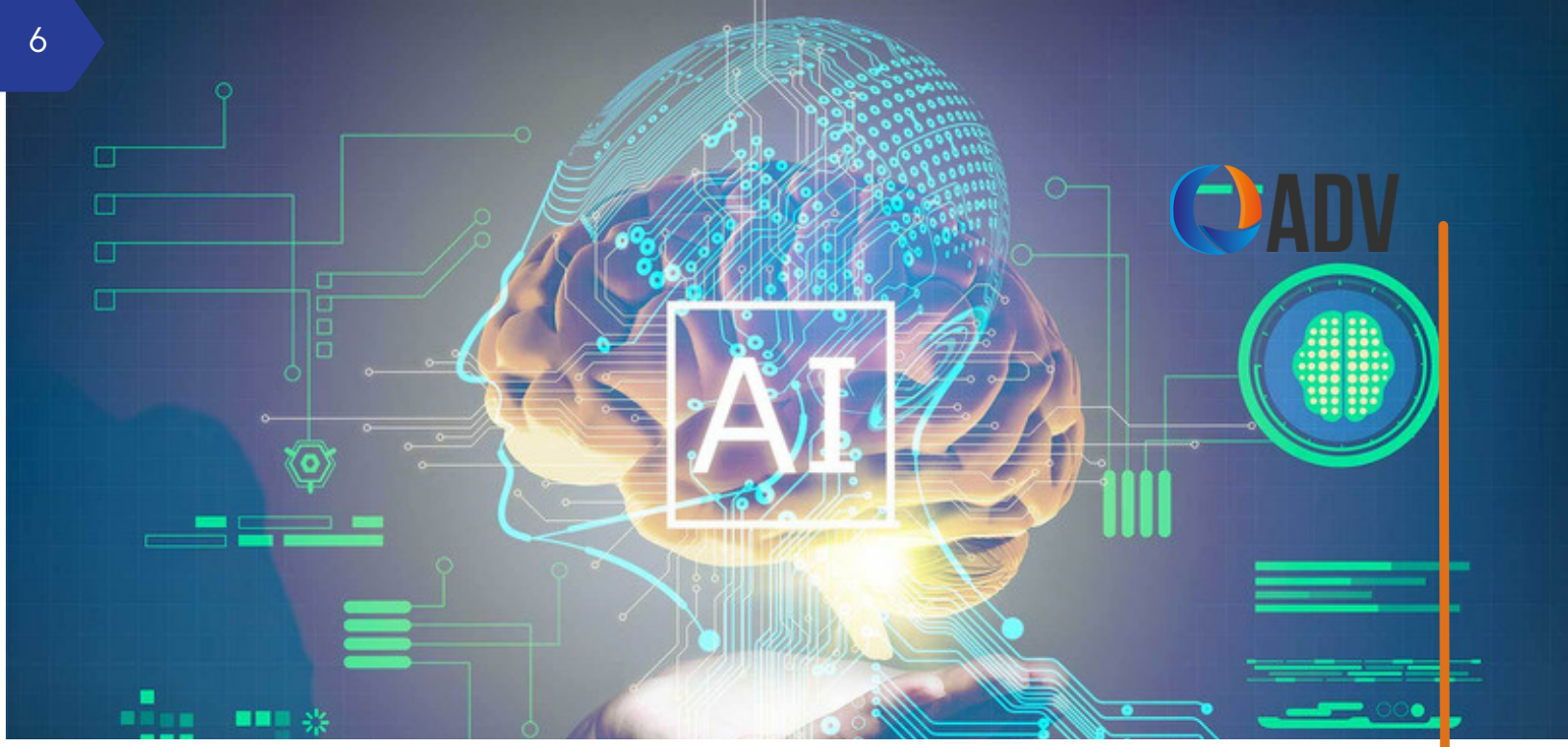
"Lo interesante de esto es que WPA intenta autenticarse usando NTLM v2 a través de la web abierta", dijo Taler. "Por lo general, NTLM v2 debería usarse al intentar autenticarse contra servicios basados en direcciones IP internas. Sin embargo, cuando el hash NTLM v2 pasa a través de Internet abierto, es vulnerable a ataques de relé y fuerza bruta sin conexión".

La revelación se produce cuando Check Point reveló un caso de "autenticación forzada" que podría ser aprovechado para filtrar los tokens NTLM de un usuario de Windows al engañar a la víctima para que abra un archivo malicioso de Microsoft Access.

En octubre de 2023, Microsoft anunció planes para discontinuar NTLM en Windows 11 a favor de Kerberos para mejorar la seguridad, ya que NTLM no admite métodos criptográficos y es susceptible a ataques de relé.



The Hacker News. (s. f.). Researchers uncover how outlook vulnerability could leak your NTLM passwords. https://thehackernews.com/2024/01/researchers-uncover-outlook.html



EL NCSC ADVIERTE DE QUE LA AMENAZA MUNDIAL DEL RANSOMWARE AUMENTARÁ CON LA IA

UNA NUEVA EVALUACIÓN SE CENTRA EN CÓMO LA INTELIGENCIA ARTIFICIAL (IA) AFECTARÁ LA EFICACIA DE LAS OPERACIONES CIBERNÉTICAS

Una nueva evaluación se centra en cómo la inteligencia artificial (IA) afectará la eficacia de las operaciones cibernéticas y las implicaciones para las amenazas cibernéticas en los próximos dos años.

Según un informe publicado hoy por el Centro Nacional de Seguridad Cibernética (NCSC) del GCHQ, se espera que la inteligencia artificial aumente la amenaza global de ransomware en los próximos dos años.

El informe de evaluación a corto plazo del impacto de la IA en la amenaza cibernética, publicado por el NCSC, concluye que la IA ya se está utilizando en actividades cibernéticas maliciosas y casi con certeza aumentará el volumen e impacto de los ciberataques, incluido el ransomware, a corto plazo.

Entre otras conclusiones, el informe sugiere que al reducir la barrera de entrada para los ciberdelincuentes novatos, los hackers a sueldo y los hacktivistas, la IA permite que actores de amenazas relativamente inexpertos lleven a cabo operaciones de acceso y recopilación de información de manera más efectiva. Este mayor acceso, combinado con la mejor focalización de víctimas que permite la IA, contribuirá a la amenaza global de ransomware en los próximos dos años.

El ransomware sigue siendo la amenaza cibernética más aguda para las organizaciones y empresas del Reino Unido, con los ciberdelincuentes adaptando sus modelos de negocio para ganar eficiencia y maximizar beneficios.

Para hacer frente a esta amenaza mejorada, el Gobierno ha invertido £2.6 mil millones en su Estrategia de Ciberseguridad para mejorar la resistencia del Reino Unido, con el NCSC y la industria privada adoptando el uso de la IA para mejorar la resistencia de la ciberseguridad mediante una mejor detección de amenazas y un diseño de seguridad.

EL NCSC ADVIERTE DE QUE LA AMENAZA MUNDIAL DEL RANSOMWARE AUMENTARÁ CON LA IA

En el Reino Unido, el sector de la IA ya emplea a 50,000 personas y contribuye con £3.7 mil millones a la economía, con el gobierno comprometido a garantizar que la economía nacional y el mercado laboral evolucionen con la tecnología, según lo establecido en las cinco prioridades del Primer Ministro.

Lindy Cameron, CEO del NCSC, comentó: "Debemos asegurarnos de aprovechar la tecnología de la IA por su vasto potencial y gestionar sus riesgos, incluyendo sus implicaciones en la amenaza cibernética".

El análisis de la NCA sugiere que los ciberdelincuentes ya han comenzado a desarrollar la IA generativa criminal (GenAI) y ofrecer 'GenAI-como-servicio', poniendo una capacidad mejorada a disposición de cualquiera dispuesto a pagar. Sin embargo, como deja claro el nuevo informe del NCSC, la efectividad de los modelos GenAI estará limitada tanto por la cantidad como por la calidad de los datos con los que se entrenen.

La creciente commoditización de la capacidad habilitada por la IA refleja advertencias de un informe publicado conjuntamente por las dos agencias en septiembre de 2023, que describía la profesionalización del ecosistema de ransomware y un cambio hacia el modelo de "ransomware-como-servicio".

Según la NCA, es poco probable que en 2024 otro método de cibercrimen reemplace al ransomware debido a las recompensas financieras y su modelo de negocio establecido.

James Babbage, Director General de Amenazas en la Agencia Nacional del Crimen, dijo: "El ransomware sigue siendo una amenaza para la seguridad nacional. Como muestra este informe, la amenaza es probable que aumente en los próximos años debido a los avances en la IA y la explotación de esta tecnología por parte de los ciberdelincuentes".

EL NCSC ADVIERTE DE QUE LA AMENAZA MUNDIAL DEL RANSOMWARE AUMENTARÁ CON LA IA

Global ransomware threat expected to rise with AI, NCSC warns. (s. f.). https://www.ncsc.gov.uk/news/global-ransomware-threat-expected-to-rise-with-ai

"Los servicios de IA reducen las barreras de entrada, aumentando el número de ciberdelincuentes, y mejorarán su capacidad al mejorar la escala, velocidad y efectividad de los métodos de ataque existentes. El fraude y el abuso sexual infantil también son particularmente propensos a ser afectados".

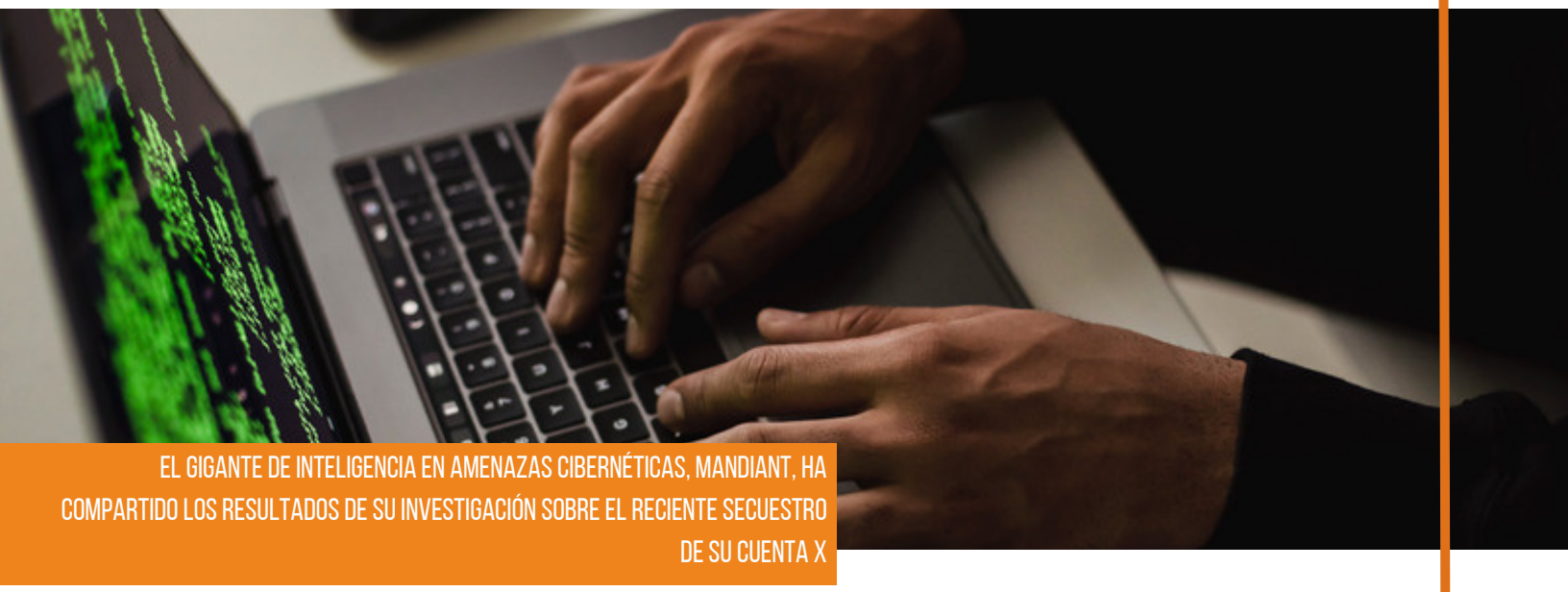
La preparación efectiva es fundamental para prevenir los ataques de ransomware. Implementar el consejo del NCSC, como las medidas protectoras simples descritas en su guía de ransomware, ayudará a las organizaciones del Reino Unido a reducir la probabilidad de infección.

La mayoría de los incidentes de ransomware suelen resultar de ciberdelincuentes que explotan una ciberhigiene deficiente, en lugar de técnicas de ataque sofisticadas. Las "10 Medidas para la Ciberseguridad" y "Consejos Principales para Mantenerse Seguro en Línea" del NCSC describen cómo las organizaciones y las personas pueden protegerse en el ciberespacio.

El informe de impacto a corto plazo de la IA en la amenaza cibernética detalla más formas en las que la IA afectará la eficacia de las operaciones cibernéticas y la amenaza cibernética en los próximos dos años, incluyendo la ingeniería social y el malware. Puedes leer el informe completo aquí.

Abordar los desafíos de asegurar la tecnología futura es una prioridad clave para el NCSC, que publicó sus "Directrices para el Desarrollo Seguro de Sistemas de IA" en noviembre con el respaldo de otros 17 países. CYBERUK 2024, que se llevará a cabo en Birmingham del 13 al 15 de mayo, profundizará en estos temas con su enfoque en "Tecnología Futura, Amenaza Futura, Preparados para el Futuro". Se emitirá un programa completo en los próximos días.

LA CUENTA X DE MANDIANT FUE PIRATEADA MEDIANTE UN ATAQUE DE FUERZA BRUTA A LA CONTRASEÑA



EL GIGANTE DE INTELIGENCIA EN AMENAZAS CIBERNÉTICAS, MANDIANT, HA COMPARTIDO LOS RESULTADOS DE SU INVESTIGACIÓN SOBRE EL RECIENTE SECUESTRO DE SU CUENTA X

El gigante de inteligencia en amenazas cibernéticas, Mandiant, ha compartido los resultados de su investigación sobre el reciente secuestro de su cuenta X, tras una ola de ataques a cuentas X relacionados con criptomonedas.

El 3 de enero de 2024, la cuenta X (anteriormente Twitter) de Mandiant, una subsidiaria de Google Cloud, fue tomada y comenzó a enviar enlaces a una página de phishing de drenaje de criptomonedas a sus 123,500 seguidores.

La firma recuperó la cuenta al día siguiente y lo anunció en redes sociales con el siguiente mensaje: "Como probablemente notaron, ayer Mandiant perdió el control de esta cuenta X, que tenía 2FA habilitado. Actualmente, no hay indicios de actividad maliciosa más allá de la cuenta X afectada, que está de nuevo bajo nuestro control. Compartiremos los resultados de nuestra investigación una vez concluida".

El 11 de enero, la empresa publicó el resultado de la investigación, que determinó que el secuestro probablemente fue resultado de un ataque de fuerza bruta a la contraseña y se limitó a la cuenta principal de la empresa, @Mandiant.

La investigación no encontró "evidencia de actividad aliciosa en, o compromiso de, ningún sistema de Mandiant o Google Cloud que llevara al compromiso de esta cuenta".

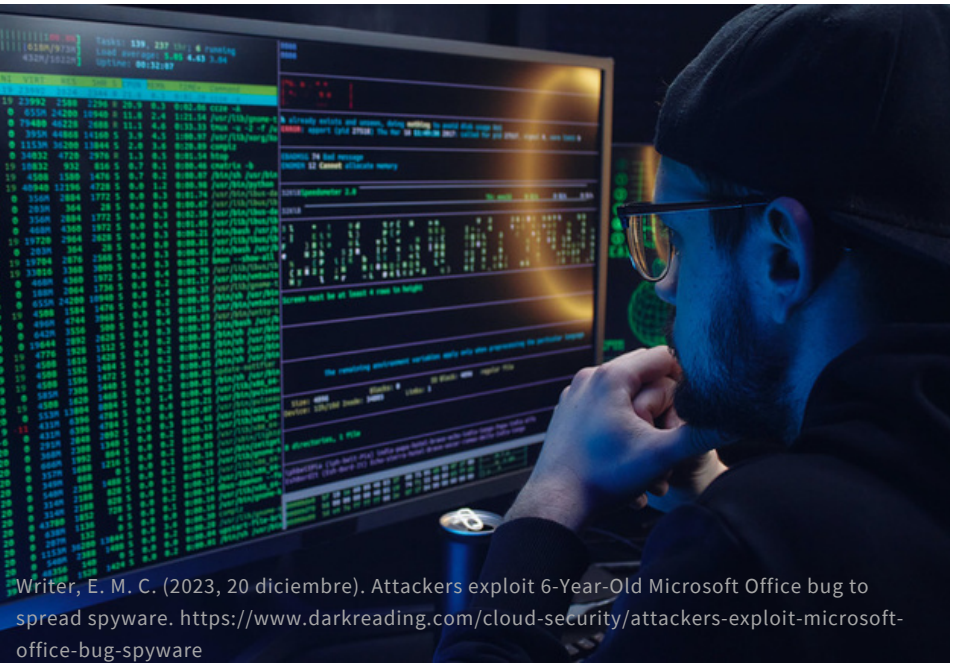
Mandiant Culpa a los Cambios en la 2FA de X.

En su comunicado, Mandiant señaló a las malconfiguraciones en la autenticación de dos factores (2FA) de su cuenta, por las cuales la empresa asumió parte de la responsabilidad, pero también culpó en parte a X.

"Normalmente, la 2FA habría mitigado esto, pero debido a algunas transiciones en el equipo y un cambio en la política de 2FA de X, no estábamos adecuadamente protegidos. Hemos realizado cambios en nuestro proceso para asegurarnos de que esto no vuelva a suceder", dijo el mensaje en redes sociales de la empresa.
Aunque el proveedor de ciberseguridad no especificó a qué cambios se refería, recientemente la 2FA se convirtió en una función exclusiva para los suscriptores Premium de X.

Antes, todos los usuarios podían habilitar la 2FA para una mayor seguridad, pero ahora solo los que pagan por el servicio de suscripción pueden acceder a elementos de esta función.

LA CUENTA X DE MANDIANT FUE PIRATEADA MEDIANTE UN ATAQUE DE FUERZA BRUTA A LA CONTRASEÑA



Writer, E. M. C. (2023, 20 diciembre). Attackers exploit 6-Year-Old Microsoft Office bug to spread spyware. https://www.darkreading.com/cloud-security/attackers-exploit-microsoft-office-bug-spyware

Específicamente, el método de mensajes de texto/SMS de la 2FA fue desactivado para los usuarios no suscriptores de Twitter Blue en febrero de 2023. Los métodos de la aplicación de autenticación y la clave de seguridad siguen estando disponibles.

Esta decisión generó considerable controversia entre la base de usuarios, ya que la 2FA se considera una medida de seguridad crucial y limitar su disponibilidad plantea preocupaciones sobre posibles vulnerabilidades.

La cuenta @Mandiant no tiene una marca de verificación dorada en X, lo que podría significar que la empresa no se ha suscrito al plan premium de la red social.

Mandiant Identifica a Actores de Amenazas de CLINKSINK detrás del Hackeo.

Mandiant ha identificado 35 identificaciones asociadas a un grupo de Drainer-as-a-Service (DaaS) que utiliza el drainer de billetera cripto CLINKSINK, un tipo de malware que aprovecha vulnerabilidades en contratos inteligentes o errores de usuario para robar fondos.

CLINKSINK se centra específicamente en las billeteras Solana (SOL).

Estos estafadores digitales utilizan cuentas X y Discord secuestradas para compartir páginas de phishing temáticas de criptomonedas, haciéndose pasar por Phantom, DappRadar y BONK con temas falsos de distribución de tokens.

Utilizando estas cuentas comprometidas, atraen a sus víctimas con promesas de tokens gratuitos, desplegando páginas de phishing convincentes disfrazadas como plataformas de criptomonedas populares.

En lugar de enriquecer a sus objetivos, están drenando fondos directamente a sus propios bolsillos, conservando el 20% para ellos y dejando el resto para las figuras sombrías que dirigen el servicio de drenaje.

Mandiant estima que este plan malicioso ha drenado al menos $900,000 de entusiastas de criptomonedas desprevenidos.

Las mismas 35 identificaciones afiliadas han utilizado CLINKSINK desde diciembre de 2023 para robar fondos y tokens de usuarios de Solana en diferentes campañas.

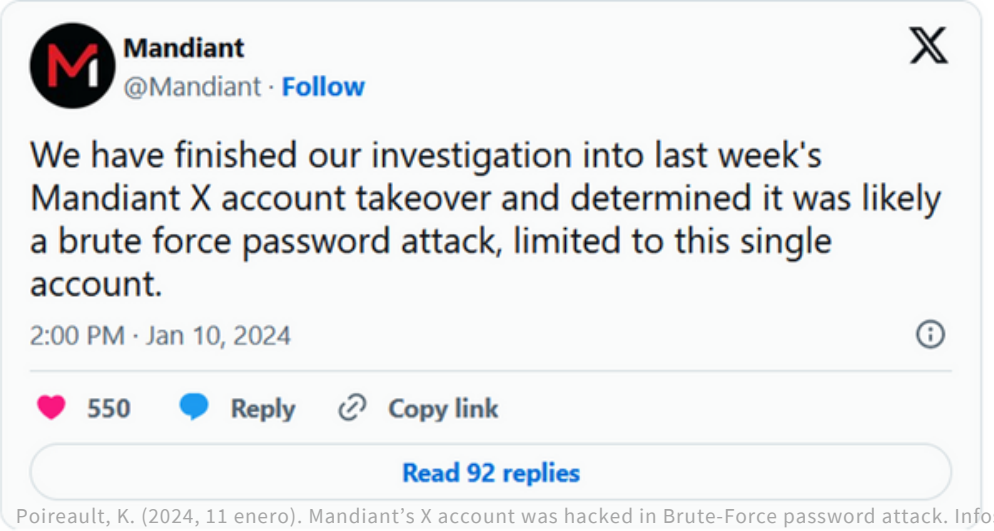
Una Ola de Secuestros de Cuentas X Relacionados con Criptomonedas.

LA CUENTA X DE MANDIANT FUE PIRATEADA MEDIANTE UN ATAQUE DE FUERZA BRUTA A LA CONTRASEÑA

Varias empresas, incluyendo Netgear, Hyundai y Certik, también han tenido recientemente sus cuentas de redes sociales X secuestradas y utilizadas para estafas de criptomonedas por actores de amenazas.

El 10 de enero, la cuenta X de la Comisión de Valores y Bolsa de los Estados Unidos, @SECGov, fue comprometida y publicó un anuncio falso sobre la aprobación de fondos cotizados en bolsa de Bitcoin (ETF) en bolsas de valores, lo que llevó a un breve aumento en los precios de Bitcoin.

El equipo de seguridad de X posteriormente dijo que el secuestro se debió al robo de un número de teléfono asociado con la cuenta @SECGov en un ataque de cambio de SIM. X también señaló que la cuenta de la SEC no tenía la autenticación de dos factores (2FA) habilitada en el momento del hackeo.



Poireault, K. (2024, 11 enero). Mandiant's X account was hacked in Brute-Force password attack. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/mandiant-x-account-brute-force/

SCHNEIDER ELECTRIC CONFIRMA EL ACCESO A DATOS EN UN ATAQUE DE RANSOMWARE

La empresa de energía Schneider Electric ha revelado que ha sido víctima de un ataque de ransomware, lo que resultó en el acceso a datos de su división de Negocios Sostenibles.

Se informa que el grupo de ransomware Cactus ha reclamado la responsabilidad del ataque, supuestamente robando terabytes de datos corporativos en el proceso. La compañía afirmó que el incidente ocurrió el 17 de enero de 2024, con su equipo de respuesta a incidentes trabajando para responder y contener el ataque.

Schneider ha informado a los clientes afectados sobre la violación. Entre los clientes de su brazo de consultoría empresarial Negocios Sostenibles se encuentran grandes marcas como Hilton, Pepsico y Walmart.

Actualmente, no está claro qué información se accedió en el incidente.

Schneider declaró: "La investigación en curso muestra que se ha accedido a datos. A medida que esté disponible más información, la división de Negocios Sostenibles de Schneider Electric continuará el diálogo directamente con sus clientes afectados y seguirá proporcionando información y asistencia según sea relevante".

Como resultado del ataque, se han desconectado varios sistemas específicos de la división, incluido Resource Advisor.

En la actualización del 29 de enero, Schneider dijo que su equipo global de respuesta a incidentes está tomando medidas de remedio para restaurar de manera segura sus sistemas. La empresa espera que el acceso a sus plataformas comerciales se reanude en los próximos dos días hábiles.

El gigante energético confirmó que ninguna otra entidad dentro del grupo Schneider Electric se ha visto afectada, ya que su Negocio Sostenible es una entidad autónoma que opera en una infraestructura de red aislada.

La investigación sobre el incidente continúa, con Schneider trabajando con empresas de ciberseguridad y "autoridades pertinentes" para obtener un análisis detallado.

Amenazas a Infraestructuras Críticas

Stephen Robinson, Analista Sénior de Inteligencia de Amenazas en WithSecure, señaló que Schneider fue víctima de la campaña de ransomware MOVEit de LockBit en 2023, y es preocupante que la empresa haya sido comprometida nuevamente tan pronto.

"Las empresas de energía tienen grandes cantidades de información personal que no solo tiene valor en la web oscura, sino que también es una excelente palanca para los ciberatacantes al exigir un rescate", afirmó.

SCHNEIDER ELECTRIC CONFIRMA EL ACCESO A DATOS EN UN ATAQUE DE RANSOMWARE

Darren Williams, CEO y Fundador de BlackFog, señaló que este incidente, que posiblemente involucra el robo de datos de grandes empresas, podría tener un impacto de gran alcance.

"En particular, el sector energético es un objetivo principal debido a sus recompensas potencialmente lucrativas, si tiene éxito, y el caos máximo causado por su amplio alcance público. Naturalmente, con clientes de alto perfil como Hilton y PepsiCo, Schneider Electric encaja en el perfil", dijo Williams.

Empresas de energía prominentes afectadas por ataques de ransomware en 2023 incluyeron a Tata Power, Suncor Energy y Energy One.

En diciembre de 2023, datos de SecurityScorecard revelaron que el 90% de las mayores empresas de energía del mundo habían sufrido una violación de datos en la cadena de suministro en los últimos 12 meses.

A principios de enero, dos importantes proveedores de agua, Southern Water en el Reino Unido y la subsidiaria norteamericana de Veolia Water, revelaron que habían sido víctimas de ataques de ransomware que llevaron al acceso a datos personales.

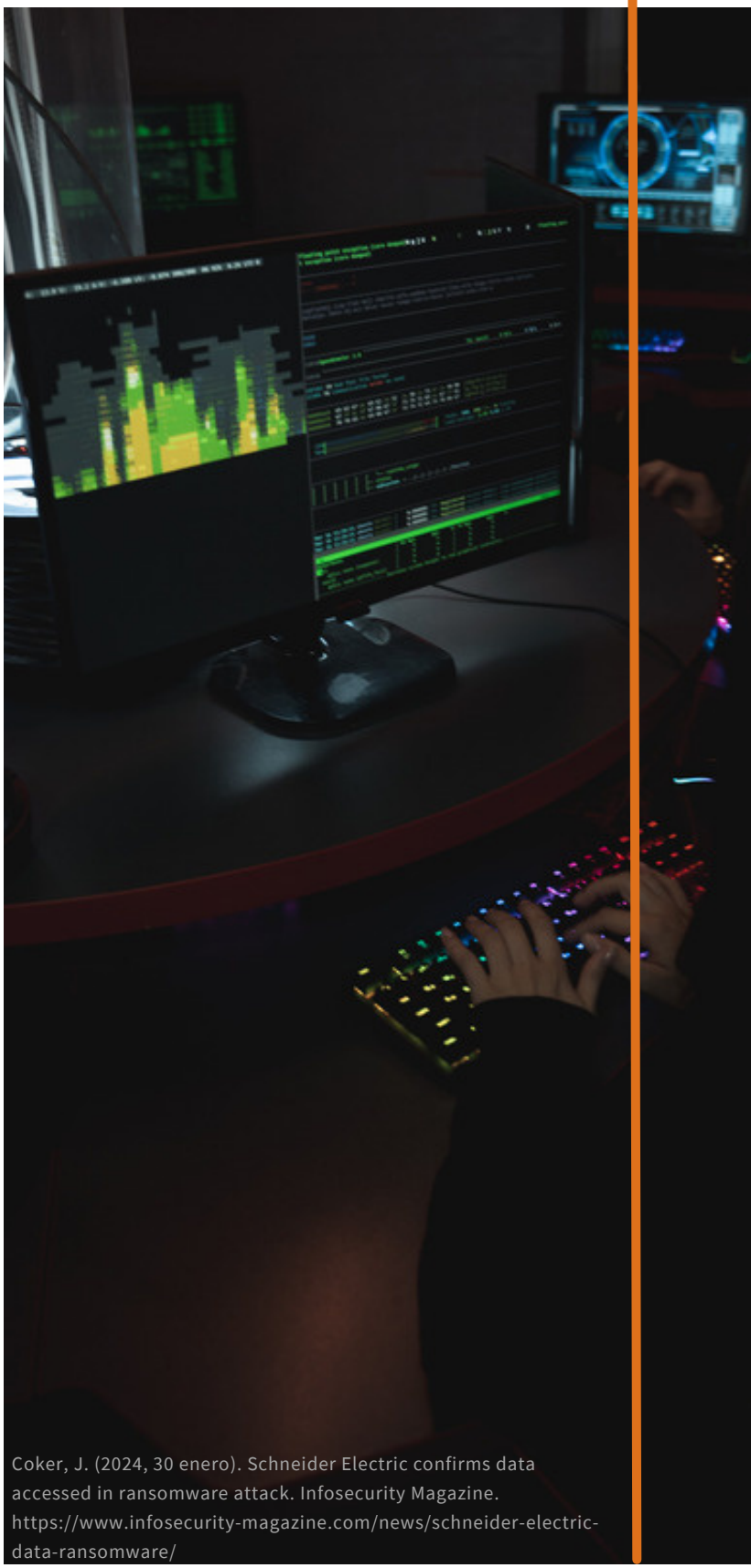
Cactus Group Cada Vez Más Activo

Robinson señaló que el grupo Cactus, que afirmó haber comprometido a Schneider, ha estado cada vez más activo en los últimos meses.

"Son un grupo de extorsión multipunto que apareció por primera vez en marzo de 2023, y sus TTP (técnicas, tácticas y procedimientos) siguen el libro de jugadas estándar de ransomware, haciendo uso de herramientas y métodos conocidos", explicó.

"Durante varios de sus ataques iniciales en 2023, Cactus ganó acceso a las redes de las víctimas a través de puertas de enlace VPN vulnerables, a menudo instancias de VPN Fortinet", agregó Robinson.

Actualización del 1 de febrero: Schneider ha publicado una declaración confirmando que el acceso a las plataformas comerciales de la división de Negocios Sostenibles se reabrió el 31 de enero de 2024.



Coker, J. (2024, 30 enero). Schneider Electric confirms data accessed in ransomware attack. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/schneider-electric-data-ransomware/

NOTICIAS NACIONALES

EXTRACCIÓN DE DATOS PERSONALES DE PERIODISTAS FUE A TRAVÉS DE LA CUENTA DE UN EXEMPLEADO: GOBIERNO FEDERAL

LAS AUTORIDADES FEDERALES DETALLARON QUE SE PRODUJO EL ROBO DE DATOS PERSONALES DE 263 PERIODISTAS, DE UN TOTAL DE 309 REGISTRADOS EN LA BASE DE DATOS DE PRESIDENCIA

El Economista. (2024, 30 enero). Extracción de datos personales de periodistas fue a través de la cuenta de un exempleado: Gobierno Federal. El Economista. https://www.eleconomista.com.mx/politica/Extraccion-de-datos-personales-de-periodistas-fue-a-traves-de-la-cuenta-de-un-exempleado-Gobierno-federal-20240129-0108.html

El presidente de México, Andrés Manuel López Obrador, anunció este lunes que su gobierno está investigando el robo de datos personales de cientos de periodistas acreditados en la Presidencia, atribuyendo la "filtración" a sus adversarios políticos.

En su rueda de prensa matutina, el mandatario expresó la necesidad de determinar qué sucedió y quién perpetró el hackeo, comprometiéndose a proporcionar apoyo a todos los afectados.

Más tarde, el gobierno federal aclaró que no se trató de una filtración, sino de una sustracción parcial de datos que afectó a 263 periodistas de los 309 registrados en la base de datos. La obtención de datos no se llevó a cabo mediante un hackeo informático, sino utilizando una cuenta legítima.

Emiliano Calderón, coordinador de estrategia digital de la Presidencia, explicó en una conferencia de prensa que se utilizó una cuenta de usuario no activa para extraer ilegalmente los documentos, identificando que el acceso se realizó desde direcciones IP registradas en España.

Entre los documentos divulgados se encuentran 186 credenciales del Instituto Nacional Electoral (INE), 63 pasaportes, 10 documentos migratorios, una licencia de conducir estadounidense, dos currículums, otro pasaporte con información ilegible y cuatro fotografías sin datos ni identificación.

Las autoridades federales indicaron que el paquete de documentos data de 2022 y fue extraído de un servidor de "preproducción" utilizado para tareas previas al traslado al sistema de producción final de las acreditaciones de periodistas que cubren las conferencias matutinas del presidente.

El gobierno presentará denuncias penales contra los responsables del robo informático, según la secretaria de Gobernación, Luisa María Alcalde, quien también ofreció un mecanismo de protección administrado por su despacho para periodistas afectados que se sientan amenazados o en riesgo.

EXTRACCIÓN DE DATOS PERSONALES DE PERIODISTAS FUE A TRAVÉS DE LA CUENTA DE UN EXEMPLEADO: GOBIERNO FEDERAL

La Sociedad Interamericana de Prensa (SIP) expresó su alarma por la filtración de datos y pidió una investigación oportuna para determinar responsabilidades.

Más tarde, el gobierno federal aclaró que no se trató de una filtración, sino de una sustracción parcial de datos que afectó a 263 periodistas de los 309 registrados en la base de datos. La obtención de datos no se llevó a cabo mediante un hackeo informático, sino utilizando una cuenta legítima.

Emiliano Calderón, coordinador de estrategia digital de la Presidencia, explicó en una conferencia de prensa que se utilizó una cuenta de usuario no activa para extraer ilegalmente los documentos, identificando que el acceso se realizó desde direcciones IP registradas en España.

Entre los documentos divulgados se encuentran 186 credenciales del Instituto Nacional Electoral (INE), 63 pasaportes, 10 documentos migratorios, una licencia de conducir estadounidense, dos currículums, otro pasaporte con información ilegible y cuatro fotografías sin datos ni identificación.

Las autoridades federales indicaron que el paquete de documentos data de 2022 y fue extraído de un servidor de "preproducción" utilizado para tareas previas al traslado al sistema de producción final de las acreditaciones de periodistas que cubren las conferencias matutinas del presidente.

El gobierno presentará denuncias penales contra los responsables del robo informático, según la secretaria de Gobernación, Luisa María Alcalde, quien también ofreció un mecanismo de protección administrado por su despacho para periodistas afectados que se sientan amenazados o en riesgo.

EXTRACCIÓN DE DATOS PERSONALES DE PERIODISTAS FUE A TRAVÉS DE LA CUENTA DE UN EXEMPLEADO: GOBIERNO FEDERAL

El Economista. (2024, 30 enero). Extracción de datos personales de periodistas fue a través de la cuenta de un exempleado: Gobierno Federal. El Economista. https://www.eleconomista.com.mx/politica/Extraccion-de-datos-personales-de-periodistas-fue-a-traves-de-la-cuenta-de-un-exempleado-Gobierno-federal-20240129-0108.html

La Sociedad Interamericana de Prensa (SIP) expresó su alarma por la filtración de datos y pidió una investigación oportuna para determinar responsabilidades.

López Obrador mencionó la entrega de un informe al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai), organismo que él ha criticado y anunciado su intención de eliminar mediante una reforma constitucional.

El presidente considera este incidente como "guerra sucia" y "espionaje", culpando una vez más a sus adversarios a pocos meses de las elecciones presidenciales del 2 de junio. Reconoció una falla en la seguridad pero insistió en atribuir la responsabilidad a sus opositores, alegando que tienen recursos para contratar a delincuentes especializados.

La divulgación de estos datos busca, según López Obrador, sembrar la idea de que su gobierno censura y actúa como dictador.

El viernes, Víctor Ruiz, fundador de la firma de seguridad cibernética Silikn, denunció en redes sociales la "filtración" de los nombres y datos personales de los periodistas. México es considerado uno de los países más peligrosos para ejercer el periodismo, con al menos 43 periodistas asesinados desde que López Obrador asumió la presidencia en diciembre de 2018, según la ONG Article 19.

CIBERSEGURIDAD EN CRISIS: MÉXICO ENFRENTA ESCASEZ CRÍTICA DE EXPERTOS

En la actualidad, México enfrenta una aguda escasez de profesionales en ciberseguridad, con más de 1.6 millones de puestos de trabajo vacantes en este campo. Aunque las organizaciones están cada vez más conscientes de la importancia de abordar esta problemática, la formación de especialistas en ciberseguridad presenta un rezago significativo.

EN LA ACTUALIDAD, MÉXICO ENFRENTA UNA AGUDA ESCASEZ DE PROFESIONALES EN CIBERSEGURIDAD

VICROR RUIZ (INFOBAE)

El sector de la ciberseguridad se ve afectado por esta escasez de talento, generando un impacto directo en la seguridad de las organizaciones que deben enfrentar una creciente carga de trabajo debido a la evolución constante de los ciberataques. La falta de profesionales capacitados para hacer frente a estas amenazas plantea un riesgo significativo, y es imperativo que las organizaciones desarrollen soluciones para cerrar esta brecha de talento.

En este contexto, la recapacitación emerge como una solución poderosa para construir equipos de seguridad sólidos, cerrar la brecha de talento en ciberseguridad y fortalecer la conciencia de seguridad en toda la organización. Desde ataques de phishing y ransomware hasta amenazas internas y vulnerabilidades de día cero, el panorama de amenazas en ciberseguridad es vasto y en constante evolución. Se espera que el costo global del delito cibernético supere los 68 mil millones de pesos para finales de 2024, lo que subraya la urgencia de contar con una fuerza laboral bien capacitada para protegerse eficazmente contra estas amenazas.

Actualmente, más de 1.6 millones de puestos de trabajo en ciberseguridad en México están sin cubrir, y el 65.2% de los líderes empresariales informan brechas de capacitación y habilidades en sus organizaciones, según un análisis de SILIKN. La brecha de talento en ciberseguridad se convierte así en un riesgo crítico para la seguridad, ya que las organizaciones enfrentan el desafío no solo de encontrar y retener talento, sino también de fortalecer la postura general de ciberseguridad de sus negocios.

La recapacitación se presenta como una solución integral y estratégica para abordar esta brecha de talento en ciberseguridad. Algunos elementos clave a considerar incluyen la identificación de talento potencial entre los

empleados actuales, la personalización de programas de formación, el fomento de certificaciones y la provisión de tutoría y aprendizaje. Este enfoque multifacético permite a las organizaciones cerrar la brecha de talento, fomentar la lealtad y retención de empleados, y construir equipos de seguridad cibernética multifacéticos y capacitados.

Un caso de estudio relevante es la Federal Cyber Reskilling Academy en los Estados Unidos, que se implementó en 2019 para abordar la escasez de empleados federales con habilidades en ciberseguridad. Este programa de recapacitación se diseñó para identificar y capacitar a empleados actuales interesados en adquirir nuevas habilidades en ciberseguridad, proporcionándoles la formación necesaria para desempeñar roles en este ámbito dentro del gobierno.

Ruiz, V. (2024, 15 enero). Ciberseguridad en crisis: México enfrenta escasez crítica de expertos. infobae. https://www.infobae.com/mexico/2024/01/15/ciberseguridad-en-crisis-mexico-enfrenta-escasez-critica-de-expertos/

En conclusión, cerrar la brecha de talento en ciberseguridad mediante la recapacitación es esencial para abordar los desafíos actuales y futuros en seguridad cibernética. Las organizaciones necesitan adoptar un enfoque estratégico y proactivo para fortalecer su fuerza laboral en ciberseguridad, y la recapacitación se presenta como una herramienta efectiva y rentable para lograrlo.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: ENERO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-50356	01/31/2024	SSL connections to NOVELL and Synology LDAP server are vulnerable to a man-in-the-middle attack due to improper certificate validation in AREAL Topkapi Vision (Server).	CVSS v3.1:9.1[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-50356

Descripción: This allows a remote unauthenticated attacker to gather sensitive information and prevent valid users from login.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-0960	01/27/2024	A vulnerability was found in flink-extended ai-flow 0.3.1. It has been declared as critical.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2024-0960

Descripción: Affected by this vulnerability is the function cloudpickle.loads of the file \ai_flow\cli\commands\workflow_command.py. The manipulation leads to deserialization. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-252205 was assigned to this vulnerability.

TABLA DE VULNERABILIDADES RELEVANTES: ENERO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-20253	01/26/2024	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device.	CVSS v3.1:10[critical]	https://nvd.nist.gov/vuln/detail/CVE-2024-20253

Descripción: This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-0402	01/25/2024	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1	CVSS v3.1:9.9 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2024-0402

Descripción: Which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace.

TABLA DE VULNERABILIDADES RELEVANTES: ENERO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-23622	01/25/2024	A stack-based buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2024-23622

Descripción: A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution with SYSTEM privileges.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-35837	01/23/2024	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-35837

Descripción: Authentication for web interface is completed via an unauthenticated WiFi AP. The administrative password for the web interface has a default password, equal to the registration ID of the device. This same registration ID is used as the WiFi SSID name. No routine is in place to force a change to this password on first use or bring its default state to the attention of the user. Once authenticated, an attacker can reconfigure the device or upload new firmware, both of which can lead to Denial of Service, code execution, or Escalation of Privileges.

TABLA DE VULNERABILIDADES RELEVANTES: ENERO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-45790	01/22/2024	The Omron FINS protocol has an authenticated feature to prevent access to memory regions.	CVSS v3.1:9.1[critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-45790

Descripción: Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-22317	01/18/2024	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.24 and 12.0.1.0 through 12.0.11.0	CVSS v3.1:9.1[critical]	https://nvd.nist.gov/vuln/detail/CVE-2024-22317

Descripción: Could allow a remote attacker to obtain sensitive information or cause a denial of service due to improper restriction of excessive authentication attempts. IBM X-Force ID: 279143.

TABLA DE VULNERABILIDADES RELEVANTES: ENERO 2024

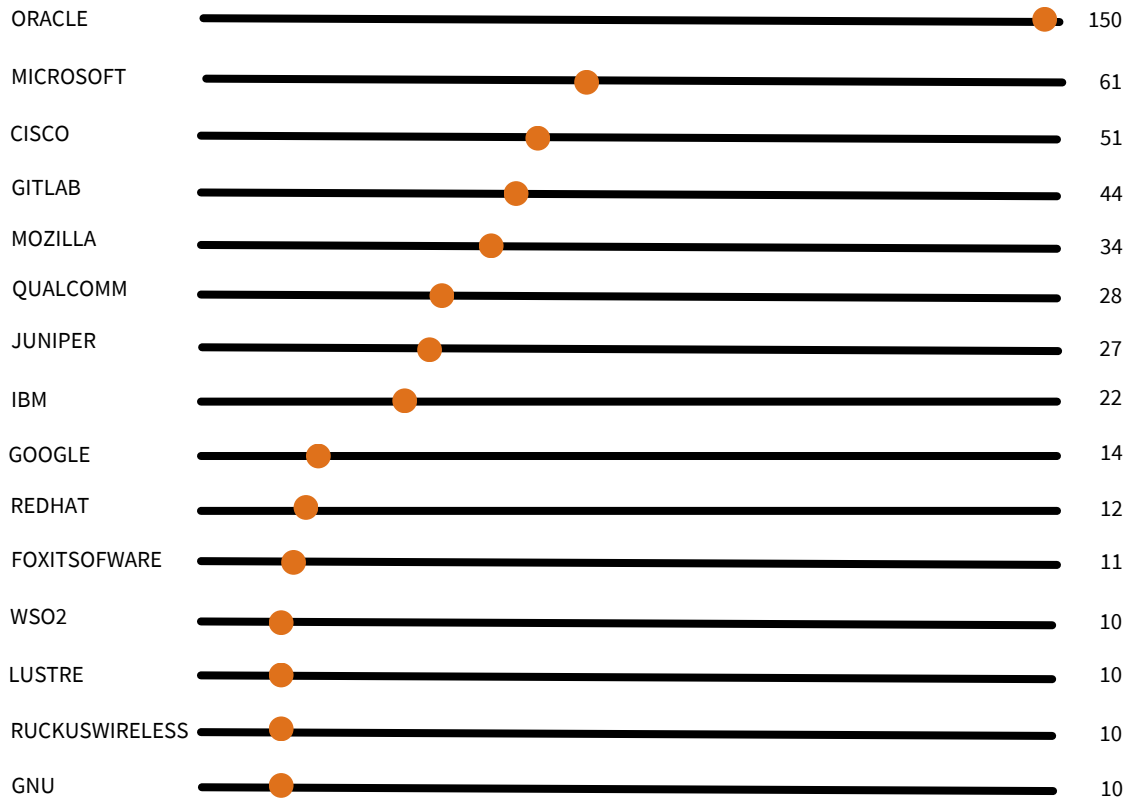
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-20272	01/17/2024	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2024-20272

Descripción: This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root.

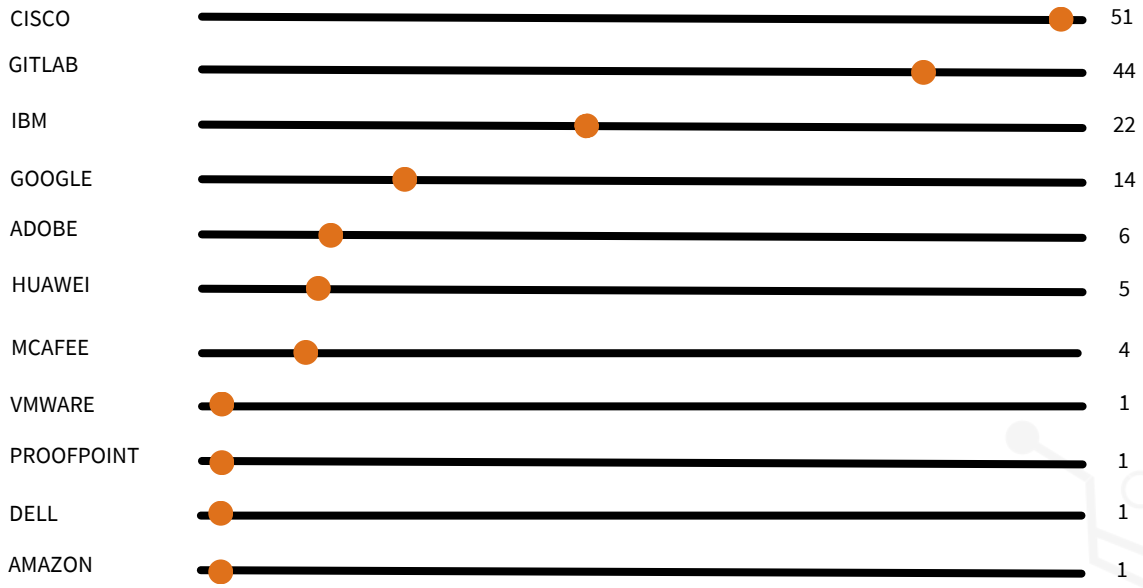
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-0485	01/13/2024	A vulnerability, which was classified as critical, was found in code-projects Fighting Cock Information System 1.0.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2024-0485

Descripción: Affected is an unknown function of the file admin/pages/tables/add_con.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250590 is the identifier assigned to this vulnerability.

FABRICANTES CON VULNERABILIDADES RELEVANTES: ENERO DE 2024



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: ENERO DE 2024



CULTURA DE CIBERSEGURIDAD

LECCIONES CLAVE DE ATAQUES A LA NUBE ENTRE 2020 Y 2022

Se ha realizado un análisis de seis importantes incidentes de ciberataques en la nube ocurridos entre 2020 y 2022, revelando que muchos de estos ataques podrían haberse evitado con una detección y respuesta más rápidas.

Los investigadores señalan que los ataques en la nube están volviéndose más avanzados en volumen y en el uso de herramientas automatizadas por parte de los atacantes. Entre las lecciones aprendidas, se destaca que los atacantes están construyendo herramientas automatizadas para explorar, encontrar y explotar vulnerabilidades, además de acceder a sistemas mediante credenciales filtradas y vulnerabilidades comunes.

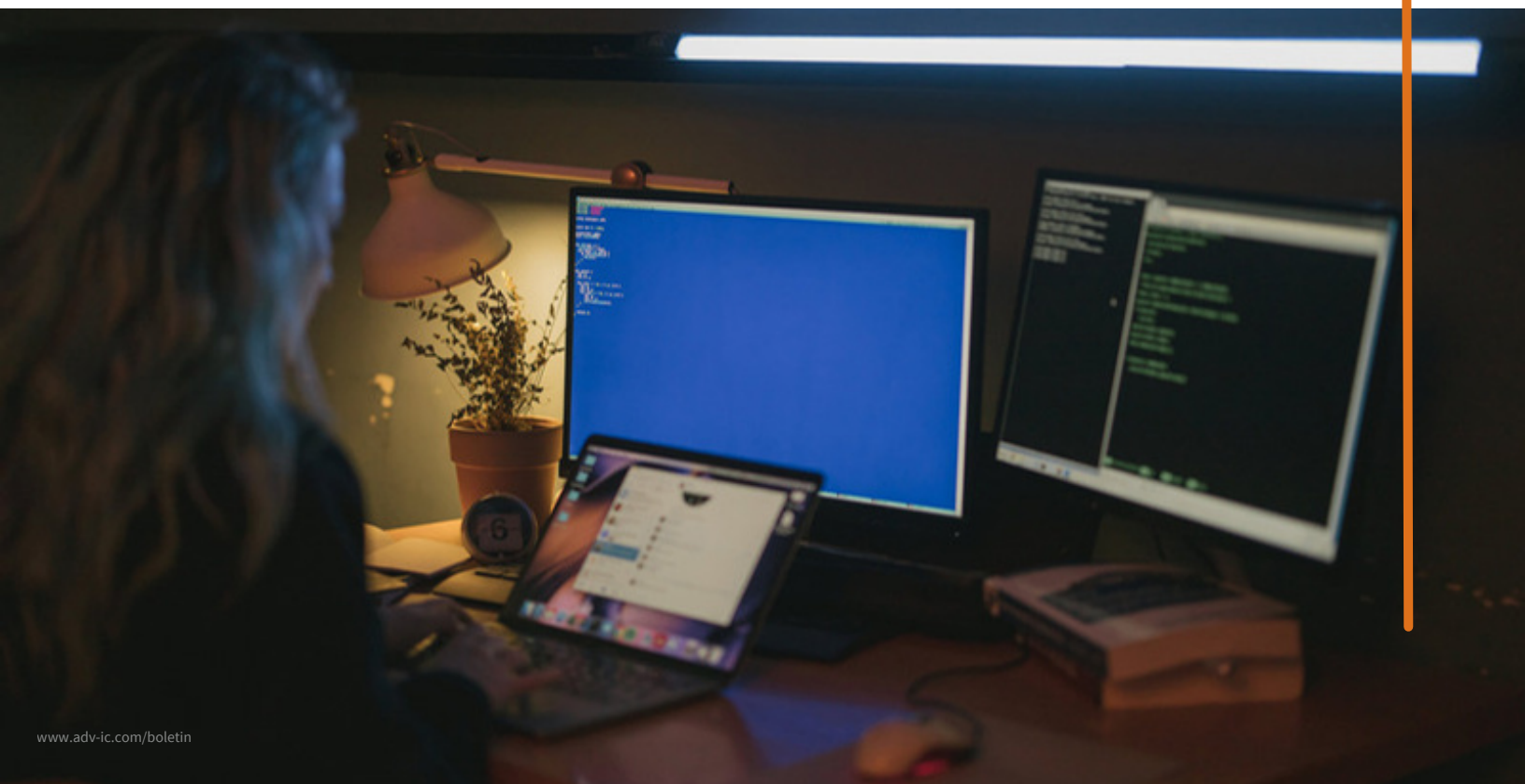
Algunos de los incidentes analizados incluyen un ataque a PyTorch, donde un atacante utilizó el repositorio de código PyPI para descargar una dependencia comprometida, y un ataque a Alibaba - Shanghai Police, donde una configuración incorrecta dejó un servidor en la nube abierto durante más de un año, resultando en el robo de 23TB de datos personales chinos.

En resumen, la realidad de los ciberataques en la nube destaca la importancia de una respuesta proactiva y robusta. Para mitigar estos riesgos, es crucial implementar prácticas efectivas de detección y respuesta.

Recomendamos enfocarse en la detección temprana mediante herramientas avanzadas y un monitoreo constante. La prevención activa, como la actualización regular de sistemas y el fortalecimiento de contraseñas, es clave para evitar vulnerabilidades explotables.

En caso de un incidente, contar con un plan de respuesta sólido es esencial: aislar rápidamente la amenaza, evaluar el alcance y trabajar en una solución. Para organizaciones que buscan una defensa integral, nuestro Servicio de Operaciones de Seguridad (SOC, por sus siglas en inglés) ofrece monitoreo continuo, análisis de amenazas y respuesta coordinada para mantener su entorno seguro y protegido contra las crecientes amenazas cibernéticas.

En la era digital, la seguridad proactiva es la clave para salvaguardar la integridad de su empresa y los datos críticos.



REFERENCIAS

REFERENCIAS

- Raywood, D. (2013, 9 de noviembre). What We Can Learn From Major Cloud Cyberattacks. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/what-we-can-learn-from-major-cloud-cyberattacks
- Ruiz, V. (2024, 15 enero). Ciberseguridad en crisis: México enfrenta escasez crítica de expertos. infobae. https://www.infobae.com/mexico/2024/01/15/ciberseguridad-en-crisis-mexico-enfrenta-escasez-critica-de-expertos/
- El Economista. (2024, 30 enero). Extracción de datos personales de periodistas fue a través de la cuenta de un exempleado: Gobierno Federal. El Economista. https://www.eleconomista.com.mx/politica/Extraccion-de-datos-personales-de-periodistas-fue-a-traves-de-la-cuenta-de-un-exempleado-Gobierno-federal-20240129-0108.html

ZERU Cybersecurity Services

Security Operation Center - SOC by

+52 81 2011 8604

contacto@adv-ic.com

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

ADV Integradores y consultores S.A de C.V | adv_consultores | adv_ic | ADV Integradores y Consultores | adv-ic.mx | ADV.Integradores