



# BOLETÍN DE CIBERSEGURIDAD ABRIL 2024

# ÍNDICE



## **NOTICIAS INTERNACIONALES**

	<b>3</b>
Los hackers están utilizando la vulnerabilidad de Magento para extraer información de pago de los sitios web de comercio electrónico.	4
Un astuto skimmer de tarjetas de crédito se camufla como un aparentemente inofensivo rastreador de Facebook.	5
La pandilla de ransomware Akira ha logrado extorsionar la considerable suma de 42 millones de dólares, y ahora ha ampliado su enfoque para atacar servidores Linux.	7
La Corporación MITRE ha sido comprometida por piratas informáticos respaldados por estados, quienes están aprovechando las vulnerabilidades en el software de Ivanti.	9
Los paquetes falsos de npm están siendo utilizados como una táctica para engañar a los desarrolladores de software, llevándolos a instalar malware.	11

## **NOTICIAS NACIONALES**

	<b>13</b>
¿Está México transformándose en el sitio de experimentación para el desarrollo del ransomware en el futuro?	14
Fortinet: a la vanguardia de la ciberseguridad en México.	17
México se enfrenta a una dura realidad: es el país más atacado en términos de ciberseguridad.	18

## **VULNERABILIDADES RELEVANTES**

	<b>19</b>
Tabla de vulnerabilidades relevantes: Abril 2024	20
Fabricantes y sus vulnerabilidades relevantes: Abril2024	25
Empresas Multinacionales y sus vulnerabilidades: Abril 2024	25

## **CULTURA DE CIBERSEGURIDAD**

	<b>26</b>
Ingeniería social	27

## **REFERENCIAS**

29



A light gray silhouette of a world map, showing the continents of North America, South America, Europe, Africa, Asia, and Australia, centered in the background.

# **NOTICIAS INTERNACIONALES**

# LOS HACKERS ESTÁN UTILIZANDO LA VULNERABILIDAD DE MAGENTO PARA EXTRAER INFORMACIÓN DE PAGO DE LOS SITIOS WEB DE COMERCIO ELECTRÓNICO.



Este ataque aprovecha la CVE-2024-20720 (CVSS score: 9.1), la cual ha sido descrita por Adobe como una instancia de "neutralización inadecuada de elementos especiales", abriendo la posibilidad de ejecución de código arbitrario.

La empresa abordó esta vulnerabilidad como parte de las actualizaciones de seguridad publicadas el 13 de febrero de 2024.

Según Sansec, se encontró una "plantilla de diseño ingeniosamente diseñada en la base de datos", la cual se utiliza para inyectar automáticamente código malicioso con el fin de ejecutar comandos arbitrarios.

"Los atacantes están combinando el analizador de diseño de Magento con el paquete beberlei/assert (instalado por defecto) para ejecutar comandos del sistema", informó la compañía.

Debido a que el bloque de diseño está asociado al carrito de pago, este comando se ejecuta cada vez que se solicita <tienda>/checkout/cart. El comando en cuestión es sed, que se utiliza para insertar un código de puerta trasera de ejecución, responsable de introducir un skimmer de pagos de Stripe para capturar y filtrar información financiera hacia otra tienda Magento comprometida.

Este desarrollo surge en un momento en que el gobierno ruso ha acusado a seis individuos de utilizar malware skimmer para sustraer información de pagos y tarjetas de crédito de tiendas de comercio electrónico extranjeras, al menos desde finales de 2017. Los sospechosos incluyen a Denis Priymachenko, Alexander Aseyev, Alexander Basov, Dmitry Kolpakov, Vladislav Patyuk y Anton Tolmachev. Según informes de Recorded Future News, los arrestos tuvieron lugar hace un año, según documentos judiciales.

La Fiscalía General de la Federación de Rusia declaró: "Como resultado, los miembros del grupo de piratas informáticos obtuvieron ilegalmente información sobre casi 160.000 tarjetas de pago de ciudadanos extranjeros y las vendieron a través de sitios web ocultos".

**LOS PERPETRADORES DE AMENAZAS HAN SIDO IDENTIFICADOS EXPLOTANDO UNA VULNERABILIDAD CRÍTICA EN MAGENTO PARA IMPLANTAR UNA PUERTA TRASERA PERSISTENTE EN LOS SITIOS WEB DE COMERCIO ELECTRÓNICO.**



# UN ASTUTO SKIMMER DE TARJETAS DE CRÉDITO SE CAMUFLA COMO UN APARENTEMENTE INOFENSIVO RASTREADOR DE FACEBOOK.

Según Sucuri, el malware se inserta en sitios web a través de herramientas que permiten código personalizado, como los complementos de WordPress como Simple Custom CSS y JS, o la sección "Miscellaneous Scripts" del panel de administración de Magento.

"Los editores de scripts personalizados son populares entre los actores maliciosos porque permiten la inclusión de JavaScript externo de terceros (y malicioso) y pueden fácilmente disfrazarse como benignos utilizando convenciones de nomenclatura que coinciden con scripts populares como Google Analytics o bibliotecas como JQuery", explicó el investigador de seguridad Matt Morrow.

El falso script de seguimiento Meta Pixel identificado por la empresa de seguridad web contiene elementos similares a su contraparte legítima, pero una inspección más detallada revela la inclusión de código JavaScript que reemplaza las referencias al dominio "connect.facebook[.]net" por "b-connected[.]com".

A pesar de que "connect.facebook[.]net" es un dominio legítimo asociado a la funcionalidad de seguimiento de píxeles, el dominio de reemplazo, "b-connected[.]com", se utiliza para cargar un script malicioso adicional ("fbevents.js"). Este script monitorea si el usuario está en una página de pago y, si es así, despliega una superposición fraudulenta para recopilar los datos de la tarjeta de crédito de la víctima.

Los investigadores de ciberseguridad han descubierto un skimmer de tarjetas de crédito oculto dentro de un script de seguimiento falso de Meta Pixel, en un intento de eludir la detección.

Para mitigar estos riesgos, se recomienda mantener actualizados los sitios web, revisar periódicamente las cuentas de administrador para asegurarse de que todas sean legítimas y actualizar las contraseñas con regularidad.

Esto es especialmente crítico ya que los actores de amenazas suelen aprovechar contraseñas débiles y vulnerabilidades en los complementos de WordPress para obtener acceso privilegiado



LOS INVESTIGADORES DE CIBERSEGURIDAD HAN DESCUBIERTO UN SKIMMER DE TARJETAS DE CRÉDITO OCULTO DENTRO DE UN SCRIPT DE SEGUIMIENTO FALSO DE META PIXEL, EN UN INTENTO DE ELUDIR LA DETECCIÓN.



## UN ASTUTO SKIMMER DE TARJETAS DE CRÉDITO SE CAMUFLA COMO UN APARENTEMENTE INOFENSIVO RASTREADOR DE FACEBOOK.



a un sitio objetivo y agregar usuarios administradores maliciosos. Estos usuarios luego se utilizan para llevar a cabo diversas actividades, como la instalación de complementos y puertas traseras adicionales.

"Debido a que los ladrones de tarjetas de crédito a menudo están programados para activarse en palabras clave como 'pagar' o 'una página', es posible que no sean detectados hasta que se cargue la página de pago", explicó Morrow.

"Dado que la mayoría de las páginas de pago se generan dinámicamente en función de los datos de las cookies y otras variables que se pasan a la página, estos scripts pueden eludir los escáneres públicos. La única manera de identificar el malware es verificar el origen de la página o monitorear el tráfico de la red. Estos scripts funcionan silenciosamente en segundo plano."

Este desarrollo se produce mientras Sucuri también revela que los sitios creados con WordPress y Magento son el objetivo de otro malware conocido como Magento Shoplift. Variantes anteriores de Magento Shoplift se han detectado en el entorno en vivo desde septiembre de 2023.

La cadena de ataque se inicia con la inserción de un fragmento de JavaScript ofuscado en un archivo JavaScript legítimo. Este fragmento es responsable de cargar un segundo script desde jqueurystatics[.]com a través de WebSocket Secure (WSS). Este segundo script está diseñado para facilitar el robo de datos, incluidos los datos de tarjetas de crédito, y se camufla como un script de Google Analytics.

"WordPress también se ha consolidado como una importante plataforma en el comercio electrónico, gracias a la popularidad de WooCommerce y otros complementos que permiten convertir fácilmente un sitio de WordPress en una tienda en línea completa", señaló la investigadora Puja Srivastava.

"Sin embargo, esta popularidad también hace que las tiendas de WordPress sean un objetivo principal para los atacantes, quienes están adaptando su malware de comercio electrónico MageCart para dirigirse a una variedad más amplia de plataformas de gestión de contenido (CMS)".



# LA PANDILLA DE RANSOMWARE AKIRA HA LOGRADO EXTORSIONAR LA CONSIDERABLE SUMA DE 42 MILLONES DE DÓLARES, Y AHORA HA AMPLIADO SU ENFOQUE PARA ATACAR SERVIDORES LINUX.



LOS PERPETRADORES DE AMENAZAS DETRÁS DEL GRUPO DE RANSOMWARE AKIRA HAN OBTENIDO ALREDEDOR DE 42 MILLONES DE DÓLARES EN GANANCIAS ILÍCITAS DESPUÉS DE COMPROMETER LAS REDES DE MÁS DE 250 VÍCTIMAS HASTA EL 1 DE ENERO DE 2024.

Según un comunicado conjunto de las agencias de ciberseguridad de los Países Bajos y EE. UU., junto con el Centro Europeo de Ciberdelincuencia (EC3) de Europol, desde marzo de 2023, el ransomware Akira ha impactado a diversas empresas y entidades de infraestructura crítica en América del Norte, Europa y Australia.

En abril de 2023, tras dirigirse inicialmente a sistemas Windows, los actores de amenazas de Akira lanzaron una variante dirigida a máquinas virtuales VMware ESXi basadas en Linux.

Se ha observado que el grupo emplea una variante C++ del ransomware en las etapas iniciales, antes de cambiar a un código basado en Rust desde agosto de 2023. Es importante destacar que este actor del crimen cibernético es completamente distinto de la familia de ransomware Akira que estuvo activa en 2017.

El acceso inicial a las redes objetivo se logra mediante la explotación de vulnerabilidades conocidas en dispositivos Cisco, como CVE-2020-3259 y CVE-2023-20269.

Otros vectores de ataque incluyen el uso de Protocolo de Escritorio Remoto (RDP), phishing, credenciales válidas y servicios de red privada virtual (VPN) que carecen de protecciones de autenticación multifactor (MFA).

También se ha identificado que los actores detrás de Akira utilizan diversas tácticas para establecer la persistencia en los sistemas comprometidos, como la creación de una nueva cuenta de dominio y eludir la detección mediante el abuso del controlador Zemana AntiMalware para finalizar procesos relacionados con el antivirus, en lo que se conoce como un ataque Bring Your Own Vulnerable Driver (BYOVD).

Para facilitar la escalada de privilegios, los atacantes confían en herramientas de extracción de credenciales como Mimikatz y LaZagne, mientras que utilizan Windows RDP para moverse lateralmente dentro de la red de la víctima. La exfiltración de datos se realiza a través de herramientas como FileZilla, WinRAR, WinSCP y RClone.

Según un análisis de Trend Micro publicado en octubre de 2023, el ransomware Akira cifra los sistemas específicos utilizando un algoritmo de cifrado híbrido que combina Chacha20 y RSA. Además, el binario de ransomware Akira incluye una función que impide la recuperación del sistema al eliminar instantáneas del sistema afectado.

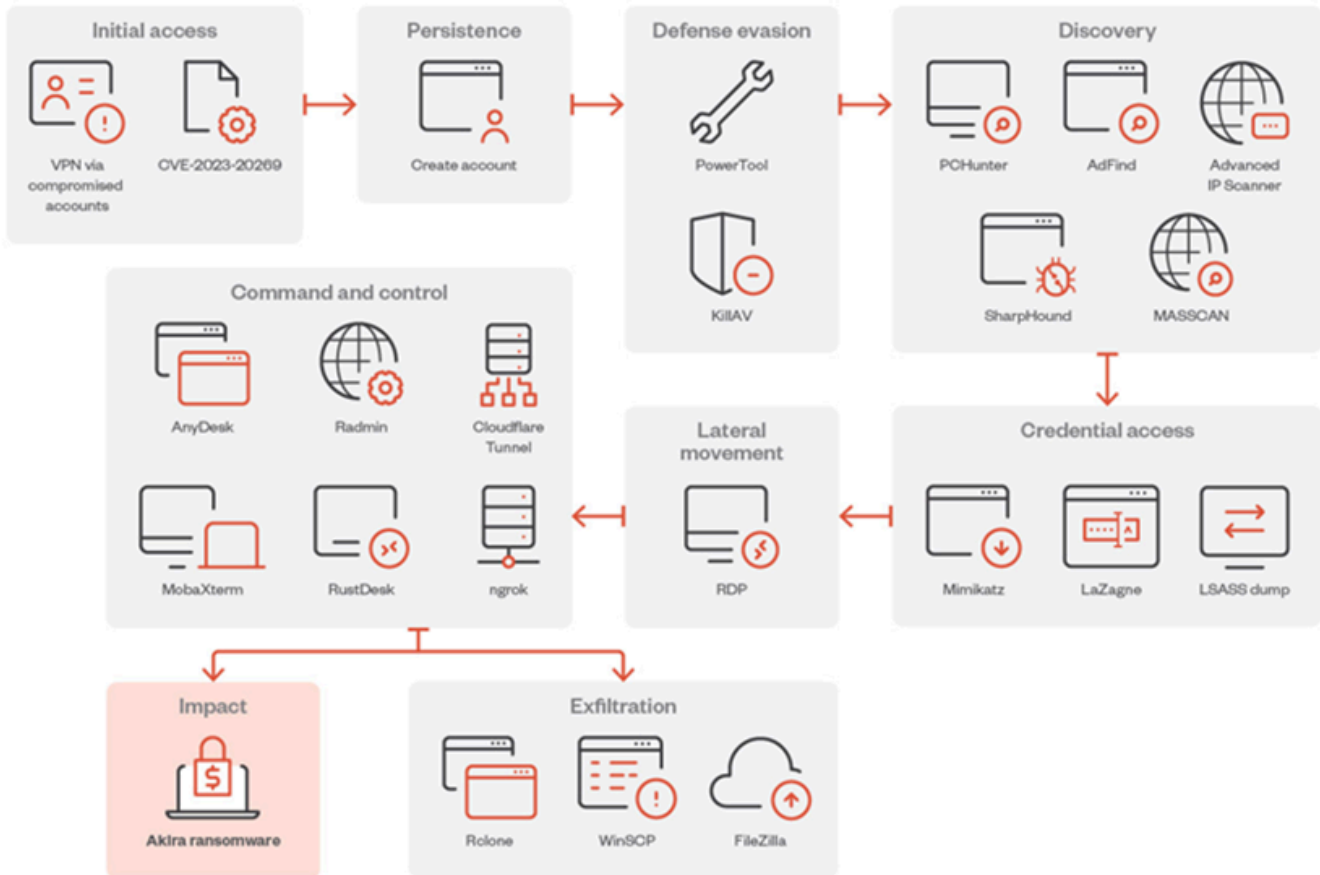
En algunos casos, el grupo también ha desplegado dos variantes diferentes de ransomware, una dirigida a sistemas Windows y otra a sistemas ESXi (Akira\_v2), como parte del mismo evento de compromiso.

## LA PANDILLA DE RANSOMWARE AKIRA HA LOGRADO EXTORSIONAR LA CONSIDERABLE SUMA DE 42 MILLONES DE DÓLARES, Y AHORA HA AMPLIADO SU ENFOQUE PARA ATACAR SERVIDORES LINUX.



Los datos de blockchain y el análisis del código fuente sugieren que el grupo de ransomware Akira podría estar relacionado con la banda de ransomware Conti, que ha dejado de operar. Avast lanzó un descifrador para Akira en julio pasado, aunque es probable que las vulnerabilidades hayan sido corregidas desde entonces.

La mutación de Akira para apuntar a entornos empresariales Linux también sigue movimientos similares de otras familias de ransomware establecidas como LockBit, Cl0p, Royal, Monti y RTM Locker.



©2023 TREND MICRO

La pandilla de ransomware Akira ha logrado extorsionar la considerable suma de 42 millones de dólares, y ahora ha ampliado su enfoque para atacar servidores Linux.



# LA CORPORACIÓN MITRE HA SIDO COMPROMETIDA POR PIRATAS INFORMÁTICOS RESPALDADOS POR ESTADOS, QUIENES ESTÁN APROVECHANDO LAS VULNERABILIDADES EN EL SOFTWARE DE IVANTI.



HACK TOOL V2.364

```

transform.rotation = Quaternion.Slerp(transform.rotation, Quater
}
public float deltaRotation;
public float deltaLimit;
public float deltaReduce;
float previousRotation;
float currentRotation;

#if UNITY_EDITOR
void FixedUpdate()
{
    if (Input.GetMouseButtonDown(0))
    {
        deltaRotation = 0f;
        previousRotation = angleBetweenPoints(transform.position,
    }
    else if (Input.GetMouseButton(0))
    {
        currentRotation = angleBetweenPoints(transform.position,
        deltaRotation = Mathf.DeltaAngle(currentRotation, previous
        if (Mathf.Abs(deltaRotation) > deltaLimit)
    }

```

MITRE Corporation ha revelado que fue objeto de un ciberataque perpetrado por un estado-nación, el cual aprovechó dos vulnerabilidades de día cero en los dispositivos Ivanti Connect Secure a partir de enero de 2024.

Este incidente condujo a la comprometida de su entorno de virtualización, investigación y experimentación en red (NERVE), una red no clasificada utilizada para investigación y desarrollo de prototipos.

El adversario, aún no identificado, llevó a cabo un reconocimiento de las redes de MITRE, explotando una de sus redes privadas virtuales (VPN) mediante el aprovechamiento de dos vulnerabilidades de día cero en Ivanti Connect Secure, y logrando eludir la autenticación multifactor al secuestrar sesiones, según lo expresado por Lex Crumpton, un investigador especializado en operaciones cibernéticas defensivas de la organización sin fines de lucro, durante la semana pasada.

El ataque implicó la explotación de dos vulnerabilidades específicas: CVE-2023-46805 (CVSS score: 8.2) y CVE-2024-21887 (CVSS score: 9.1), que los actores de amenazas utilizaron para eludir la autenticación y ejecutar comandos arbitrarios en el sistema infectado.

Una vez que obtuvieron acceso inicial, los atacantes se movieron lateralmente y comprometieron la infraestructura VMware de MITRE utilizando una cuenta de administrador comprometida. Esto les permitió desplegar puertas traseras y shells web para lograr persistencia y recolectar credenciales.

"NERVE es una red colaborativa no clasificada que proporciona recursos de almacenamiento, computación y redes", declaró MITRE. "Según nuestra investigación hasta la fecha, no hay indicios de que la red empresarial central de MITRE o los sistemas de los socios se hayan visto afectados por este incidente".

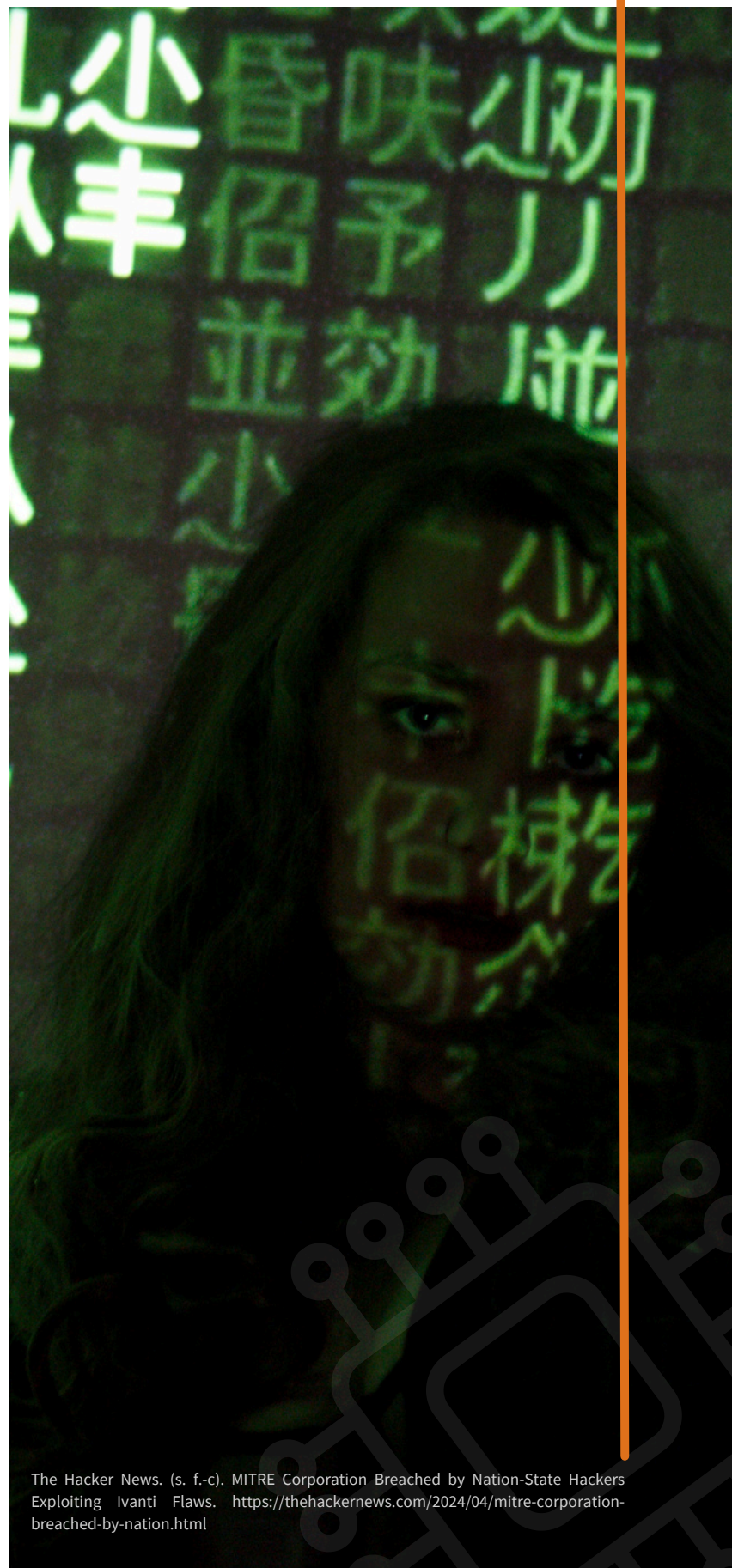
LA CORPORACIÓN MITRE HA SIDO COMPROMETIDA POR PIRATAS INFORMÁTICOS RESPALDADOS POR ESTADOS, QUIENES ESTÁN APROVECHANDO LAS VULNERABILIDADES EN EL SOFTWARE DE IVANTI.



La explotación inicial de estas vulnerabilidades ha sido atribuida a un grupo identificado por la empresa de ciberseguridad Volexity como UTA0178, un actor estatal probablemente vinculado a China. Desde entonces, varios otros grupos de hackers con conexiones con China han seguido explotando estas vulnerabilidades, según Mandiant.

"Este tipo de ciberataques pueden afectar a cualquier organización, incluso aquellas que se esfuerzan por mantener los más altos estándares de ciberseguridad", declaró Jason Providakes, presidente y director ejecutivo de MITRE.

"Estamos compartiendo esta información sobre el incidente de manera oportuna porque estamos comprometidos con el interés público y defendemos las mejores prácticas que promueven la seguridad empresarial. Asimismo, estamos trabajando para implementar medidas que mejoren la postura de ciberdefensa de la industria en general".



The Hacker News. (s. f.-c). MITRE Corporation Breached by Nation-State Hackers Exploiting Ivanti Flaws. <https://thehackernews.com/2024/04/mitre-corporation-breached-by-nation.html>

# LOS PAQUETES FALSOS DE NPM ESTÁN SIENDO UTILIZADOS COMO UNA TÁCTICA PARA ENGAÑAR A LOS DESARROLLADORES DE SOFTWARE, LLEVÁNDOLOS A INSTALAR MALWARE.

Una campaña de ingeniería social en curso está dirigida a desarrolladores de software mediante el uso de paquetes npm falsos que se presentan como una oportunidad de trabajo. Estos paquetes contienen una puerta trasera de Python, diseñada para engañar a los desarrolladores y hacer que descarguen y ejecuten el software malicioso.

La empresa de ciberseguridad Securonix ha estado monitoreando esta actividad, conocida como DEV#POPPER, y la ha relacionado con actores de amenazas norcoreanos.

"Durante estas entrevistas fraudulentas, se le solicita a los desarrolladores que realicen tareas que implican la descarga y ejecución de software de fuentes que parecen legítimas, como GitHub", explicaron los investigadores de seguridad Den Iuzvyk, Tim Peck y Oleg Kolesnikov. "Este software contiene una carga útil maliciosa de Node JS que, una vez ejecutada, compromete el sistema del desarrollador".

Los detalles de esta campaña emergieron inicialmente a finales de noviembre de 2023, cuando la Unidad 42 de Palo Alto Networks describió un conjunto de actividades denominado "Entrevista Contagiosa". En esta táctica, los actores de amenazas se hacen pasar por empleadores con el objetivo de atraer a los desarrolladores de software para que instalen malware como BeaverTail e InvisibleFerret durante el proceso de entrevista.

Posteriormente, a principios de febrero, la empresa de seguridad de la cadena de suministro de software Phylum descubrió un conjunto de paquetes maliciosos en el registro npm que entregaban las mismas familias de malware, comprometiendo así información confidencial de los sistemas de desarrollo.

Es importante señalar que "Contagious Interview" se distingue de "Operation Dream Job" (también conocido como DeathNote o NukeSped). La Unidad 42 explicó a The Hacker News que la primera está enfocada en dirigirse a desarrolladores, principalmente a través de identidades falsas en portales de empleo independientes, y que las siguientes etapas involucran el uso de herramientas de desarrollo y paquetes npm que conducen a BeaverTail e InvisibleFerret.

**MITRE CORPORATION HA REVELADO QUE FUE OBJETO DE UN CIBERATAQUE PERPETRADO POR UN ESTADO-NACIÓN, EL CUAL APROVECHÓ DOS VULNERABILIDADES DE DÍA CERO EN LOS DISPOSITIVOS IVANTI CONNECT SECURE A PARTIR DE ENERO DE 2024.**



**UPLOADING VIRUS ...**



**PROGRESS ... 65%**

## LOS PAQUETES FALSOS DE NPM ESTÁN SIENDO UTILIZADOS COMO UNA TÁCTICA PARA ENGAÑAR A LOS DESARROLLADORES DE SOFTWARE, LLEVÁNDOLOS A INSTALAR MALWARE.



Por otro lado, "Operation Dream Job", vinculada al Grupo Lazarus de Corea del Norte, es una campaña de larga duración que utiliza ofertas de trabajo falsas para distribuir malware a profesionales en sectores como el aeroespacial, las criptomonedas y la defensa.


La cadena de ataque identificada por Securonix comienza con un archivo ZIP alojado en GitHub, probablemente enviado al objetivo como parte de la entrevista. Dentro de este archivo se encuentra un módulo npm aparentemente benigno que aloja un archivo JavaScript malicioso, codificado como BeaverTail, que actúa como un ladrón de información y un cargador para una puerta trasera de Python llamada InvisibleFerret, que se descarga desde un servidor remoto.

El implante, además de recopilar información del sistema, tiene la capacidad de ejecutar comandos, enumerar y extraer archivos, y registrar el portapapeles y las pulsaciones de teclas.

Este desarrollo es un indicio de que los actores de amenazas norcoreanos continúan perfeccionando una serie de herramientas para su arsenal de ataques cibernéticos. Constantemente actualizan sus técnicas con capacidades mejoradas para ocultar sus acciones y mezclarse con los sistemas y redes anfitriones, además de desviar datos y convertir los compromisos en ganancias financieras.

"Es crucial mantener una mentalidad centrada en la seguridad cuando se enfrenta a ataques que utilizan ingeniería social, especialmente en situaciones intensas y estresantes como las entrevistas de trabajo", comentaron los investigadores de Securonix.

"Los atacantes detrás de las campañas DEV#POPPER se aprovechan de esto, sabiendo que la persona al otro lado está muy distraída y en un estado mucho más vulnerable".

A light grey silhouette map of Mexico, showing the outline of the country and its islands, including the Baja Peninsula and the Yucatán Peninsula.

# NOTICIAS NACIONALES

LOS GRUPOS DELICTIVOS EXPERTOS EN RANSOMWARE ESTÁN REALIZANDO ENSAYOS EN NACIONES EN VÍAS DE DESARROLLO COMO MÉXICO ANTES DE LLEVAR A CABO SUS ATAQUES CONTRA OBJETIVOS EN ESTADOS UNIDOS, EUROPA O ASIA.

## ¿ESTÁ MÉXICO TRANSFORMÁNDOSE EN EL SITIO DE EXPERIMENTACIÓN PARA EL DESARROLLO DEL RANSOMWARE EN EL FUTURO?

Recientemente, hemos presenciado un marcado incremento en los ataques de ransomware dirigidos a organizaciones de diversos sectores en distintas regiones del planeta. Este tipo de software malicioso involucra a un atacante que encripta archivos o restringe el acceso a un sistema informático, exigiendo un rescate a cambio de su liberación o descifrado.

En los últimos años, ha habido un considerable aumento de casos de ransomware en México. Para finales de 2023, el país se ubicó como el segundo en Latinoamérica en cuanto a detecciones únicas de este tipo de malware, representando el 25.8% de la distribución regional. Durante el primer trimestre de 2024, se confirmó que el ransomware sigue siendo un desafío significativo en México, impactando una variedad de sectores, tanto públicos como privados.

En los últimos años, los ataques de ransomware han causado pérdidas económicas considerables en el país. Por ejemplo, en 2023 se registró que el costo promedio para recuperarse de un ataque de ransomware ascendió a 2.3 millones de dólares.

De acuerdo con un estudio llevado a cabo por la unidad de investigación de SILIKN, México se sitúa en el puesto número 14 a nivel mundial como objetivo de ataques de ransomware. Los sectores más perjudicados por estos ataques son el gobierno y la industria. Además, el grupo cibercriminal más activo en el país en cuanto a ransomware ha sido LockBit 3.0, con un total de 28 ataques documentados.

## ¿ESTÁ MÉXICO TRANSFORMÁNDOSE EN EL SITIO DE EXPERIMENTACIÓN PARA EL DESARROLLO DEL RANSOMWARE EN EL FUTURO?

Entre las estadísticas relevantes relacionadas con el ransomware recopiladas en el año 2023, destacan los siguientes datos:

- Durante el año 2023, un 88% de las organizaciones mexicanas experimentaron impactos causados por ransomware.
- De estos ataques, el 72% resultaron en la encriptación de datos.
- Solo el 19% de las organizaciones afectadas lograron recuperar parte de sus datos cifrados.
- El 45% de las organizaciones optaron por pagar el rescate exigido.
- Aquellas organizaciones mexicanas que pagaron el rescate lograron recuperar en promedio el 28% de sus datos.
- El costo promedio para recuperarse de un ataque de ransomware en México durante 2023 fue de 2.3 millones de dólares.
- El 98% de las organizaciones en México informaron que los ataques de ransomware afectaron su capacidad operativa.
- El 96% de estas organizaciones reportaron pérdidas en negocios, clientes o ingresos debido a los ataques de ransomware.
- En promedio, las organizaciones mexicanas tardaron seis meses en recuperarse por completo de estos ataques.

En el contexto actual, ha surgido una preocupación importante: ¿Está México convirtiéndose en el campo de pruebas para el ransomware del futuro? Según la unidad de investigación de SILIKN, grupos delictivos especializados en ransomware están llevando a cabo pruebas en países en desarrollo como México antes de ejecutar sus ataques contra blancos en Estados Unidos, Europa o Asia. Esto se debe a que han identificado en México, y en América Latina en general, una falta de conciencia sobre ciberseguridad, sistemas desactualizados sin parches de seguridad, tecnologías obsoletas y sin soporte del fabricante, así como diversas vulnerabilidades globales que no se han abordado de manera oportuna ni efectiva. Además, también observan una respuesta débil por parte de los usuarios frente a los ataques de phishing.

Un aspecto importante a destacar es que los países en desarrollo están siendo seleccionados como objetivos principales para estas pruebas debido a su rápida adopción de la digitalización y su infraestructura de seguridad relativamente más débil. Por esta razón, grupos como LockBit 3.0, Trigona, 8Base, Rhysida, Medusa, Raworld, Akira y Noescape, entre otros, están utilizando estas regiones como terrenos de pruebas. Una vez que logran infiltrarse con éxito en empresas y gobiernos de América Latina, expanden sus operaciones hacia objetivos en países desarrollados.



## ¿ESTÁ MÉXICO TRANSFORMÁNDOSE EN EL SITIO DE EXPERIMENTACIÓN PARA EL DESARROLLO DEL RANSOMWARE EN EL FUTURO?



Un ejemplo ilustrativo de esto es el descubrimiento de nuevas variantes del ransomware SEXi, que afectó a principios de abril de 2024 a IxMetro Powerhost, un proveedor chileno de centros de datos y servicios de hosting, y se sospecha que también impactó a la empresa mexicana Coppel a mediados del mismo mes. Además, se estima que este avanzado malware no solo causó una interrupción temporal en los servicios, sino que también eliminó datos financieros de una empresa tributaria en Colombia y de una agencia gubernamental en Argentina.

En la búsqueda de soluciones, la lucha contra el ransomware parece ser un desafío perpetuo. Sin embargo, los criminales informáticos muestran una creciente preocupación por las operaciones encubiertas realizadas por agencias de aplicación de la ley como el FBI, Interpol y Europol, que recientemente han logrado desmantelar grupos delictivos notables como Blackcat o Hive. Estas acciones han dejado claro que es posible arrestar a los ciberdelincuentes, lo que ha generado un temor entre ellos de ser capturados y perder sus ganancias ilícitas. Aunque este efecto aún es limitado, sirve como un disuasivo contra las actividades de ransomware.

Además de México, otros países de América Latina deben intensificar sus esfuerzos para mejorar sus medidas de ciberseguridad y así reducir los efectos perjudiciales causados por los grupos de ciberdelincuentes. Esta tarea debe considerarse una prioridad, ya que de lo contrario, corren el riesgo de seguir siendo naciones constantemente vulnerables a los ataques cibernéticos.





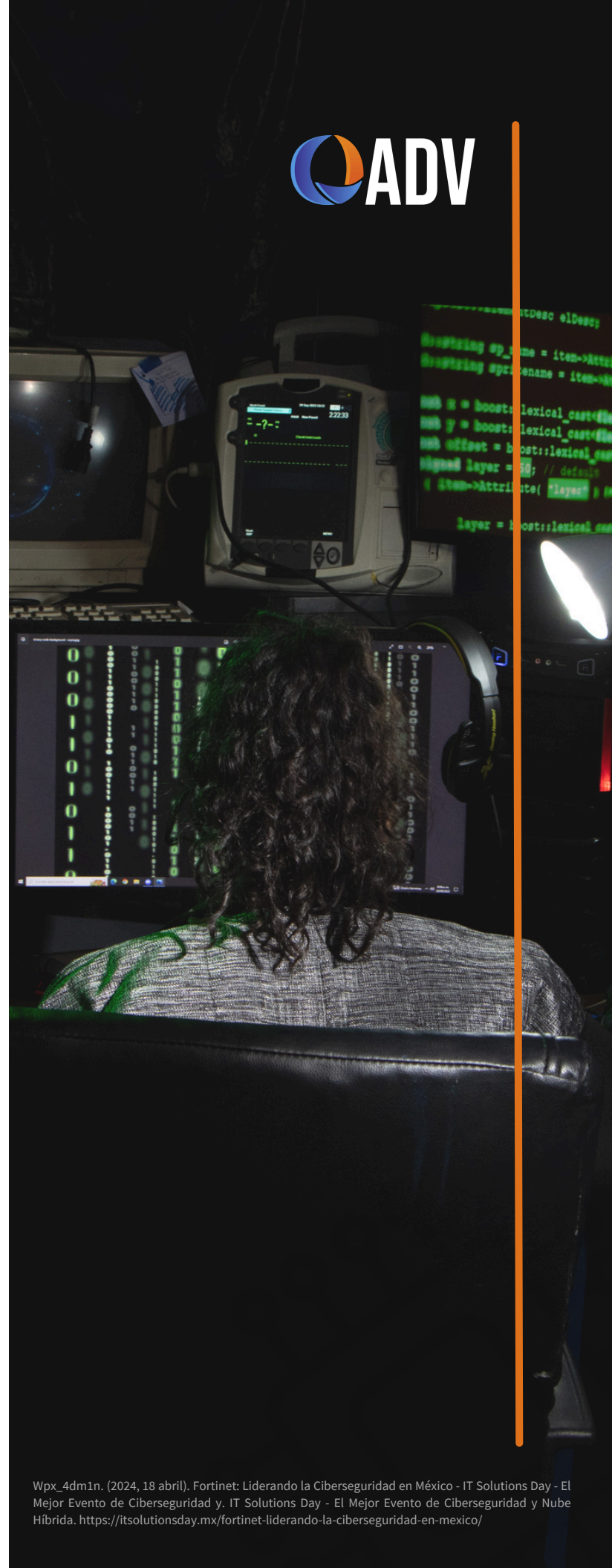
# FORTINET: A LA VANGUARDIA DE LA CIBERSEGURIDAD EN MÉXICO.

Fortinet lidera el panorama de la ciberseguridad en México, ofreciendo soluciones robustas y confiables en un entorno digital cada vez más complejo y amenazante. En un país que ha experimentado un notable aumento en los ciberataques en los últimos años, la presencia de Fortinet se destaca como una aliada indispensable para las organizaciones mexicanas.

La economía digitalmente avanzada de México enfrenta desafíos únicos en materia de ciberseguridad, y Fortinet ha demostrado ser un socio confiable en esta área. A través de su participación constante en eventos como el IT Solutions Day, Fortinet se compromete a compartir las últimas soluciones y estrategias en ciberseguridad con los líderes tecnológicos de México.

Para los CISOs, que tienen la responsabilidad de garantizar la seguridad de la información en sus organizaciones, Fortinet ofrece más que simples productos: proporciona una verdadera asociación. Con una amplia cartera que abarca desde la seguridad integral hasta la inteligencia de amenazas y el soporte y capacitación continuos a través de la Fortinet Security Academy, Fortinet se destaca como un aliado indispensable para enfrentar los desafíos de seguridad cibernética.

Además, Fortinet ha contribuido significativamente al panorama de la ciberseguridad en México a través de iniciativas como la colaboración con instituciones educativas para fomentar el talento local en ciberseguridad y su participación activa en foros y conferencias de seguridad. Su compromiso con la educación y la difusión de las mejores prácticas de seguridad ha elevado el estándar de ciberseguridad en el país.





## MÉXICO SE ENFRENTA A UNA DURA REALIDAD: ES EL PAÍS MÁS ATACADO EN TÉRMINOS DE CIBERSEGURIDAD.

México enfrenta una situación preocupante, siendo el país con el mayor número de ciberataques, según el "Cyberthreat Defense Report 2024" elaborado por CyberEdge Group. El informe revela que el 97% de las empresas mexicanas fueron afectadas al menos una vez durante el año pasado. A nivel mundial, el porcentaje de empresas atacadas exitosamente se redujo del 84.7% al 81.5%, lo que indica una disminución generalizada. Esto se atribuye principalmente al regreso a las oficinas, que reduce el riesgo de empresas por ataques en modalidad de teletrabajo, así como a una mayor adopción de herramientas de protección y capacitación de empleados.

Sin embargo, en el caso de México, aunque se está volviendo a las oficinas, la adopción de herramientas de protección y capacitación no parece estar aumentando al mismo ritmo que la actividad de los ciberatacantes. Esto ha resultado en un aumento en la frecuencia y gravedad de los ataques. Manuel Rivera de NEKT Group, empresa en ciberseguridad, señala que la situación en México es alarmante debido a esta brecha entre la defensa cibernética y la actividad de los ciberdelincuentes.

Después de México, los países más afectados por los ciberataques contra empresas son Sudáfrica, Colombia, España y Brasil, según el informe. Esta tendencia resalta la importancia urgente de fortalecer las medidas de ciberseguridad en México y en todo el mundo para proteger a las empresas contra las crecientes amenazas cibernéticas.

Entre las principales industrias analizadas, las instituciones financieras experimentaron la mayor frecuencia de ataques exitosos, seguidas por firmas de telecomunicaciones y tecnología, mientras que la manufactura y el comercio minorista fueron menos afectados.

Para el año 2024, el documento muestra que el porcentaje de encuestados que creen que un ataque exitoso pueda ocurrir pasó del 71.8 al 66.7 por ciento a nivel mundial. En el caso de México, aunque el 97% de los encuestados reportaron haber sido atacados exitosamente el año pasado, solo el 62.5% cree que esto sucederá de nuevo en 2024.

Según los especialistas, hay esperanza para México, ya que es uno de los países donde más empresas han incluido expertos en ciberseguridad en sus consejos de administración, con un 88%, en comparación con el 62% a nivel global. Sin embargo, es necesario que el conocimiento del consejo de administración se difunda y permee en toda la organización para traducirlo en una menor tasa de éxito para los atacantes.

A large, light gray warning sign graphic consisting of a triangle with a thick border and a large exclamation mark in the center. The text is overlaid on the exclamation mark.

**VULNERABILIDADES  
RELEVANTES**

# TABLA DE VULNERABILIDADES RELEVANTES:

## ABRIL 2024



Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-3342	04/27/2024	Fallas de seguridad en productos WordPress	CVSS v3.1: 9.9 [critico]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-3342">https://nvd.nist.gov/vuln/detail/CVE-2024-3342</a>

**Descripción:** El complemento Timetable and Event Schedule by MotoPress para WordPress es vulnerable a la inyección SQL a través del atributo 'events' del shortcode 'mp-timetable' en todas las versiones hasta la 2.4.11 inclusive debido a un escape insuficiente en el parámetro proporcionado por el usuario, y falta de preparación suficiente en la consulta SQL existente. Esto hace posible que los atacantes autenticados, con acceso de nivel de colaborador y superior, agreguen consultas SQL adicionales a consultas ya existentes que pueden usarse para extraer información confidencial de la base de datos.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-39367	17/04/2024	Fallas de seguridad en productos HTTP	CVSS v3.1: 9.1 [critico]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-39367">https://nvd.nist.gov/vuln/detail/CVE-2023-39367</a>

**Descripción:** Existe una vulnerabilidad de inyección de comandos del sistema operativo en la funcionalidad mac2name de la interfaz web de Peplink Smart Reader v1.2.0 (en QEMU). Una solicitud HTTP especialmente diseñada puede provocar la ejecución de un comando arbitrario. Un atacante puede realizar una solicitud HTTP autenticada para desencadenar esta vulnerabilidad.

## TABLA DE VULNERABILIDADES RELEVANTES: ABRIL 2024



Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21082	16/04/2024	Fallas de seguridad en productos Oracle	CVSS v3.1: 9.8 [critico]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-21082">https://nvd.nist.gov/vuln/detail/CVE-2024-21082</a>

**Descripción:** Vulnerabilidad en el producto Oracle BI Publisher de Oracle Analytics (componente: Servicios XML). Las versiones compatibles que se ven afectadas son 7.0.0.0.0 y 12.2.1.4.0. Una vulnerabilidad fácilmente explotable permite que un atacante no autenticado con acceso a la red a través de HTTP comprometa Oracle BI Publisher. Los ataques exitosos a esta vulnerabilidad pueden resultar en la adquisición de Oracle BI Publisher. CVSS 3.1 Puntuación base 9,8 (impactos en la confidencialidad, la integridad y la disponibilidad). Vector CVSS: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-20758	10/04/2024	Fallas de seguridad en productos Adobe	CVSS v3.1: 9.0 [critico]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-20758">https://nvd.nist.gov/vuln/detail/CVE-2024-20758</a>

**Descripción:** Las versiones 2.4.6-p4, 2.4.5-p6, 2.4.4-p7, 2.4.7-beta3 y anteriores de Adobe Commerce se ven afectadas por una vulnerabilidad de validación de entrada incorrecta que podría provocar la ejecución de código arbitrario en el contexto del usuario actual. . La explotación de este problema no requiere la interacción del usuario, pero la complejidad del ataque es alta.

## TABLA DE VULNERABILIDADES RELEVANTES: ABRIL 2024



Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-29990	09/04/2024	Fallas de seguridad en productos Microsoft Azure	CVSS v3.1: 9.0 [critico]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-29990">https://nvd.nist.gov/vuln/detail/CVE-2024-29990</a>

**Descripción:** Vulnerabilidad de elevación de privilegios del contenedor confidencial del servicio Microsoft Azure Kubernetes

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21894	04/04/2024	Fallas de seguridad en productos Ivanti	CVSS v3.1: 9.8 [Critico]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-21894">https://nvd.nist.gov/vuln/detail/CVE-2024-21894</a>

**Descripción:** na vulnerabilidad de desbordamiento de montón en el componente IPSec de Ivanti Connect Secure (9.x, 22.x) e Ivanti Policy Secure permite que un usuario malintencionado no autenticado envíe solicitudes especialmente diseñadas para bloquear el servicio, provocando así un ataque DoS. En determinadas condiciones, esto puede conducir a la ejecución de código arbitrario.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21473	01/04/2024	Fallas de seguridad en productos Qualcomm	CVSS v3.1: 9.8 [Crítico]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-21473">https://nvd.nist.gov/vuln/detail/CVE-2024-21473</a>

**Descripción:** Corrupción de la memoria al redirigir el archivo de registro a cualquier ubicación de archivo con cualquier nombre de archivo.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-4185	30/04/2024	Fallas de seguridad en productos WordPress	CVSS v3.1: 8.1 [Alto]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-4185">https://nvd.nist.gov/vuln/detail/CVE-2024-4185</a>

**Descripción:** El complemento Customer Email Verification para WooCommerce para WordPress es vulnerable a la verificación de correo electrónico y a la omisión de autenticación en todas las versiones hasta la 2.7.4 inclusive mediante el uso de un código de activación insuficientemente aleatorio. Esto hace posible que los atacantes no autenticados omitan la verificación por correo electrónico, y si están marcadas las opciones "Iniciar sesión con el usuario automáticamente después de verificar la cuenta" y "Verificar cuenta para los usuarios actuales", entonces potencialmente hace posible que los atacantes eludan autenticación para otros usuarios.

## TABLA DE VULNERABILIDADES RELEVANTES: ABRIL 2024



Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-48655	28/04/2024	Fallas de seguridad en productos Linux	CVSS v3.1: 7.8 [Alto]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-48655">https://nvd.nist.gov/vuln/detail/CVE-2022-48655</a>

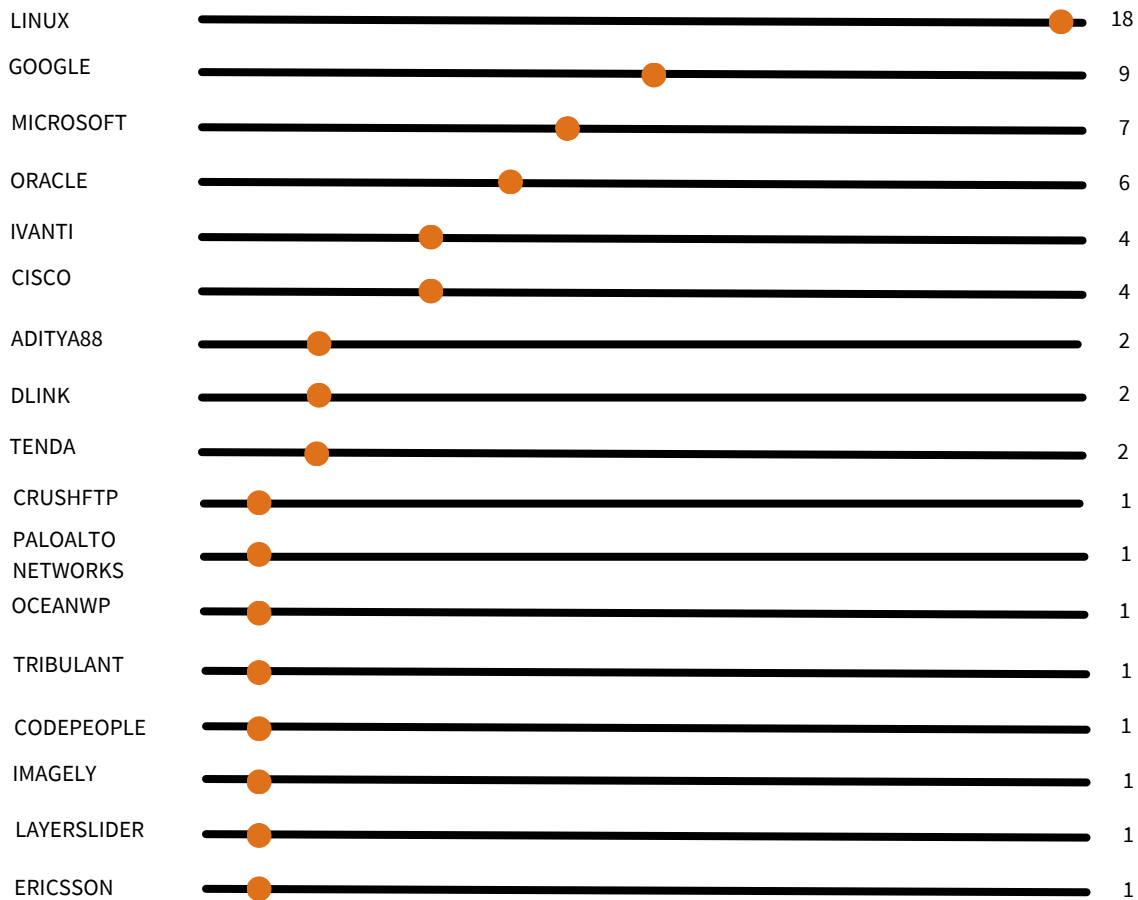
**Descripción:** En el kernel de Linux, se ha resuelto la siguiente vulnerabilidad: firmware: arm\_scmi: Refuerza los accesos a los dominios de reinicio. El acceso a los descriptores de dominios de reinicio por el índice ante las solicitudes de los controladores SCMI a través de la interfaz de operaciones de reinicio de SCMI puede conducir potencialmente a violaciones fuera de límites. si el controlador SCMI se comporta mal. Agregue una verificación de coherencia interna antes de que se acceda a dichos descriptores de dominio.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21445	24/04/2024	Fallas de seguridad en productos Cisco	CVSS v3.1: 8.6 [Alto]	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-20353">https://nvd.nist.gov/vuln/detail/CVE-2024-20353</a>

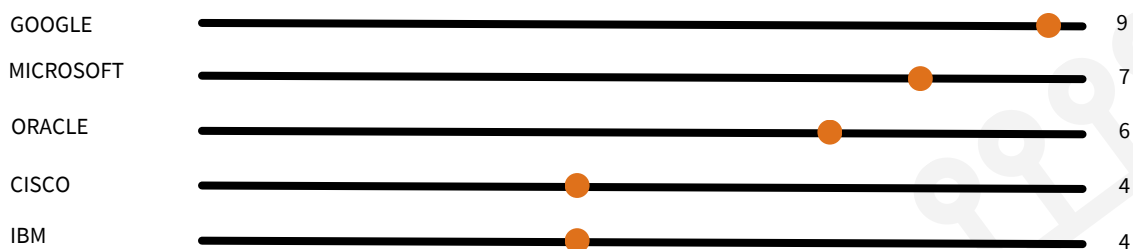
**Descripción:** Una vulnerabilidad en los servidores web de administración y VPN para el software Cisco Adaptive Security Appliance (ASA) y el software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado provoque que el dispositivo se recargue inesperadamente, lo que resultaría en una denegación de servicio (DoS). ) condición. Esta vulnerabilidad se debe a una comprobación de errores incompleta al analizar un encabezado HTTP. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada a un servidor web específico en un dispositivo. Un exploit exitoso podría permitir al atacante provocar una condición DoS cuando el dispositivo se recarga.



## FABRICANTES CON VULNERABILIDADES RELEVANTES: ABRIL DE 2024



## EMPRESAS MULTINACIONALES CON VULNERABILIDADES: ABRIL DE 2024



A large, light gray graphic of a padlock is centered on the page. The padlock is shown in an open position, with the shackle at the top. It is surrounded by a circular frame with four small circles at the top, bottom, left, and right positions, resembling a network or a globe.

**CULTURA DE  
CIBERSEGURIDAD**

# INGENIERÍA SOCIAL



La ingeniería social es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de valor. Los ataques pueden ocurrir en línea, en persona y a través de otras interacciones.

## ¿CÓMO Y POR QUÉ FUNCIONA LA INGENIERÍA SOCIAL?

Manipulan las emociones e instintos de las víctimas de formas que se ha demostrado que llevan a las personas a tomar medidas que no son las más convenientes para sus intereses.

La mayoría de los ataques de ingeniería social emplean una o más de las siguientes tácticas:

- Hacerse pasar por una marca de confianza
- Hacerse pasar por una agencia gubernamental o una figura de autoridad
- Inducir miedo o sensación de urgencia
- Apelando a la codicia
- Apelar a la amabilidad la curiosidad

## TIPOS DE ATAQUES DE INGENIERÍA SOCIAL

### PHISHING

Los ataques de phishing son mensajes digitales o de voz que intentan manipular a los destinatarios para compartir información confidencial, descargar software malicioso, transferir dinero o activos a personas equivocadas o tomar otras medidas perjudiciales. Los estafadores elaboran mensajes de phishing para que parezcan o suenen como si procedieran de una organización o persona de confianza o creíble, a veces incluso una persona que el destinatario conoce personalmente.

Hay muchos tipos de fraude por phishing:

- Los correos electrónicos masivos de phishing
- El spear phishing
- La suplantación de identidad por voz, o vishing
- El phishing por SMS, o smishing
- La suplantación de identidad en los motores de búsqueda
- Angler phishing es phishing a través de cuentas falsas de redes sociales

## BAITING

El baiting atrae (sin doble sentido) a las víctimas para que, consciente o inconscientemente, faciliten información confidencial o descarguen código malicioso, tentándolas con una oferta valiosa o incluso un objeto de valor.

## TAILGATING

En el tailgating -también llamado "piggybacking"- una persona no autorizada sigue de cerca a una persona autorizada hasta un área que contiene información sensible o activos valiosos.

## PRETEXTAR

Al pretextar, el actor de la amenaza crea una situación falsa para la víctima y se hace pasar por la persona adecuada para resolverla. Muy a menudo (e irónicamente) el estafador afirma que la víctima ha sido afectada por una violación de seguridad, y luego ofrece arreglar cosas si la víctima proporcionará información importante de la cuenta o control sobre el ordenador o dispositivo de la víctima.

## QUID PRO QUO

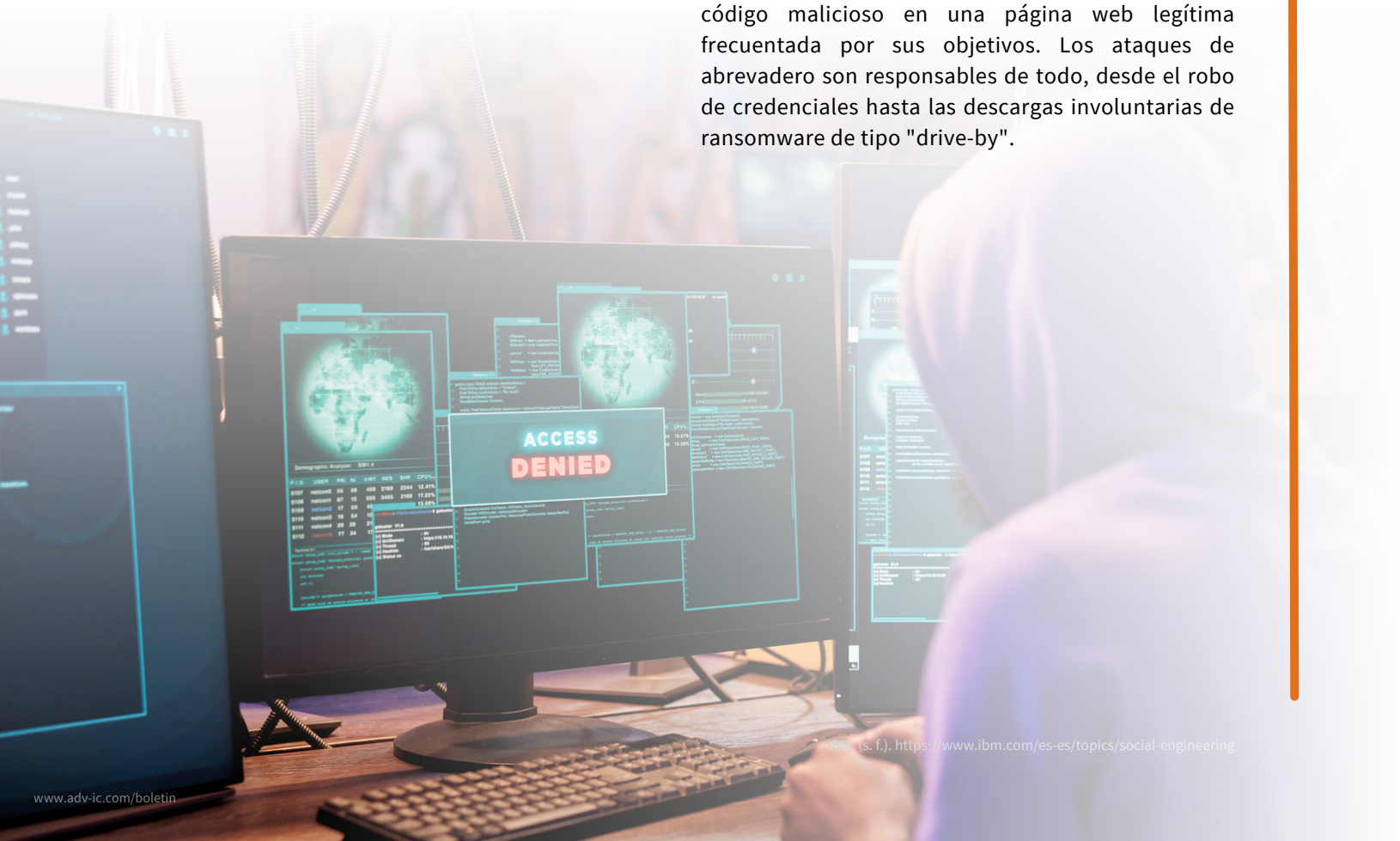
En una estafa quid pro quo, los piratas informáticos cuelgan un bien o servicio deseable a cambio de la información confidencial de la víctima. Ganar concursos falsos o recompensas de fidelidad aparentemente inocentes («gracias por su pago, tenemos un regalo para usted») son ejemplos de tácticas quid pro quo.

## SCAREWARE

También considerado una forma de malware, el scareware es un software que utiliza el miedo para manipular a las personas para que compartan información confidencial o descarguen malware. El scareware suele adoptar la forma de un falso aviso de las fuerzas de seguridad acusando al usuario de un delito, o de un falso mensaje de soporte técnico advirtiéndole de la presencia de malware en su dispositivo.

## ATAQUE DE ABREVADERO

Derivado de la frase "alguien envenenó el abrevadero": los piratas informáticos inyectan código malicioso en una página web legítima frecuentada por sus objetivos. Los ataques de abrevadero son responsables de todo, desde el robo de credenciales hasta las descargas involuntarias de ransomware de tipo "drive-by".





## REFERENCIAS



- IBM. (s. f.). <https://www.ibm.com/es-es/topics/social-engineering>
- Impreso. (2024, 30 abril). México, el país más atacado. Diario de Yucatán. <https://www.yucatan.com.mx/mexico/2024/04/30/mexico-el-pais-mas-atacado.html>
- Wpx\_4dm1n. (2024, 18 abril). Fortinet: Liderando la Ciberseguridad en México - IT Solutions Day - El Mejor Evento de Ciberseguridad y. IT Solutions Day - El Mejor Evento de Ciberseguridad y Nube Híbrida. <https://itsolutionsday.mx/fortinet-liderando-la-ciberseguridad-en-mexico/>
- Ruiz, P. V. (2024, 27 abril). ¿Se está convirtiendo México en el laboratorio de pruebas para el ransomware del futuro? Infobae. <https://www.infobae.com/mexico/2024/04/26/se-esta-convirtiendo-mexico-en-el-laboratorio-de-pruebas-para-el-ransomware-del-futuro/>
- The Hacker News. (s. f.-b). Bogus npm Packages Used to Trick Software Developers into Installing Malware. <https://thehackernews.com/2024/04/bogus-npm-packages-used-to-trick.html>
- The Hacker News. (s. f.-c). MITRE Corporation Breached by Nation-State Hackers Exploiting Ivanti Flaws. <https://thehackernews.com/2024/04/mitre-corporation-breached-by-nation.html>
- The Hacker News. (s. f.-a). Akira ransomware gang extorts \$42 million; now targets Linux servers. <https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html>
- The Hacker News. (s. f.-e). Sneaky Credit Card Skimmer Disguised as Harmless Facebook Tracker. <https://thehackernews.com/2024/04/sneaky-credit-card-skimmer-disguised-as.html>
- The Hacker News. (s. f.). Hackers Exploit Magento Bug to Steal Payment Data from E-commerce Websites. <https://thehackernews.com/2024/04/hackers-exploit-magento-bug-to-steal.html>



ZERU Cybersecurity  
Services

Security Operation Center - SOC by



+52 81 2011 8604



info@adv-ic.com



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



[Visita nuestra página Web](#)



ADV Integradores y consultores S.A de C.V



adv\_consultores



adv\_ic



ADV Integradores y Consultores



[adv-ic.mx](http://adv-ic.mx)



ADV.Integradores