BOLETÍN DE CIBERSEGURIDAD

MAYO 2024

ÍNDICE

NOTICIAS INTERNACIONALES

HACKERS UTILIZAN UNA VULNERABILIDAD EN LA CACHÉ LITESPEED PARA TOMAR EL CONTROL ABSOLUTO DE LOS SITIOS WEB DE WORDPRESS

LOS HACKERS ESTÁN ACTUALMENTE APROVECHANDO UNA VULNERABILIDAD CRÍTICA EN EL COMPLEMENTO LITESPEED CACHE PARA WORDPRESS, PERMITIENDO LA CREACIÓN DE CUENTAS DE ADMINISTRADOR FRAUDULENTAS EN SITIOS WEB VULNERABLES.

Estos hallazgos provienen de WPScan, que ha informado que la vulnerabilidad (CVE-2023-40000, con una puntuación CVSS de 8.3) está siendo explotada para establecer usuarios administradores falsos bajo los nombres "wpsupp-user" y "wp-configuser".

CVE-2023-40000, revelada por Patchstack en febrero de 2024, es una vulnerabilidad de secuencias de comandos entre sitios (XSS) almacenada que podría permitir a un usuario no autenticado aumentar sus privilegios mediante solicitudes HTTP especialmente diseñadas.

La vulnerabilidad fue corregida en octubre de 2023 con la versión 5.7.0.1 del complemento. Es relevante destacar que la última versión disponible es la 6.2.0.1, lanzada el 25 de abril de 2024.

LiteSpeed Cache cuenta con más de 5 millones de instalaciones activas. Las estadísticas muestran que aproximadamente el 16.8% de todos los sitios web aún utilizan versiones anteriores a 5.7, 6.0, 6.1 y 6.2.

Según la información proporcionada por la empresa propiedad de Automattic, el malware suele insertar código JavaScript alojado en dominios como dns.startservicefounds[.]com y api.startservicefounds[.]com en los archivos de WordPress.

La creación de cuentas de administrador en sitios de WordPress puede acarrear consecuencias graves, ya que otorga al atacante control total sobre el sitio web, permitiéndole llevar a cabo acciones arbitrarias que van desde la inserción de malware hasta la instalación de complementos maliciosos.

Para mitigar posibles amenazas, se recomienda a los usuarios que apliquen las últimas correcciones, revisen todos los complementos instalados y eliminen los archivos y carpetas sospechosos.

HACKERS UTILIZAN UNA VULNERABILIDAD EN LA CACHÉ LITESPEED PARA TOMAR EL CONTROL ABSOLUTO DE LOS SITIOS WEB DE WORDPRESS

Según WPScan, se aconseja buscar en la base de datos cadenas sospechosas como 'eval(atob(Strings.fromCharCode' específicamente en la opción litespeed.admin_display.messages.

Este desarrollo surge después de que Sucuri revelara una campaña de estafa de redireccionamiento llamada Mal.Metrica, que utiliza mensajes falsos de verificación CAPTCHA en sitios de WordPress infectados para llevar a los usuarios a sitios fraudulentos e indeseables. Estos sitios están diseñados para descargar software incompleto o para atraer a las víctimas a proporcionar información personal bajo la apariencia de recibir recompensas.

Aunque estos mensajes pueden parecer una simple verificación humana, en realidad son completamente falsos y buscan engañar al usuario para que haga clic en el botón, lo que inicia una redirección a sitios web maliciosos y fraudulentos.

The Hacker News. (n.d.). Hackers exploiting LiteSpeed Cache bug to gain full control of WordPress sites. https://thehackernews.com/2024/05/hackers-exploiting-litespeed-cache-bug.html

PAQUETE MALICIOSO DE PYTHON OCULTA EL MARCO SLIVER C2 DENTRO DEL LOGOTIPO DE UNA BIBLIOTECA FALSA DE SOLICITUDES

Los investigadores de ciberseguridad han descubierto un paquete Python malicioso que se hace pasar por una extensión de la conocida biblioteca Requests. Este paquete, llamado request-darwin-lite, ha sido identificado ocultando una versión en Golang del marco de comando y control (C2) de Sliver dentro de una imagen PNG que representa el logotipo del proyecto.

Antes de ser eliminado del Índice de Paquetes de Python (PyPI), request-darwin-lite fue descargado unas 417 veces.

A simple vista, requests-darwin-lite parecía ser una variante del popular paquete Requests, pero con algunas diferencias significativas. En particular, incluía un binario malicioso en Go empaquetado dentro de una versión alterada del logotipo PNG del proyecto Requests.

Los cambios fueron implementados en el archivo setup.py del paquete, configurándolo para decodificar y ejecutar un comando en Base64 con el objetivo de recopilar el Identificador Único Universal (UUID) del sistema. Sin embargo, esta acción solo se ejecutaba después de verificar que el host comprometido estuviera utilizando Apple macOS.

Este descubrimiento llega poco más de un mes después de que la empresa detectara un paquete fraudulento en npm llamado vue2util, que se hacía pasar por una utilidad auxiliar pero en realidad llevaba a cabo actividades de criptojacking y robaba tokens USDT de las víctimas.

El paquete explotaba el mecanismo de aprobación del contrato ERC20 (USDT), otorgando de manera encubierta aprobación ilimitada a la dirección del contrato del atacante, lo que le permitía drenar efectivamente los tokens USDT de la víctima.

En un giro interesante, la cadena de infección solo avanzaba si el UUID coincidía con un valor específico, lo que sugiere que los autores del paquete estaban buscando atacar una máquina particular para la cual ya tenían el UUID obtenido a través de otro medio.

Esta situación plantea dos posibilidades: o se trata de un ataque altamente dirigido o se trata de un proceso de prueba antes de una campaña más amplia.

ESTA SITUACIÓN PLANTEA DOS POSIBILIDADES: O SE TRATA DE UN ATAQUE ALTAMENTE DIRIGIDO O SE TRATA DE UN PROCESO DE PRUEBA ANTES DE UNA CAMPAÑA MÁS AMPLIA.

PAQUETE MALICIOSO DE PYTHON OCULTA EL MARCO SLIVER C2 DENTRO DEL LOGOTIPO DE UNA BIBLIOTECA FALSA DE SOLICITUDES

Si el UUID coincidía, request-darwin-lite procedía a leer datos de un archivo PNG llamado "requests-sidebar-large.png", que guarda similitudes con el paquete de solicitudes legítimas que incluye un archivo similar llamado "requests-sidebar.png". Sin embargo, la diferencia radicaba en que mientras el logotipo real incrustado en las solicitudes tenía un tamaño de archivo de 300 kB, el contenido dentro de las solicitudes-darwin-lite era aproximadamente de 17 MB.

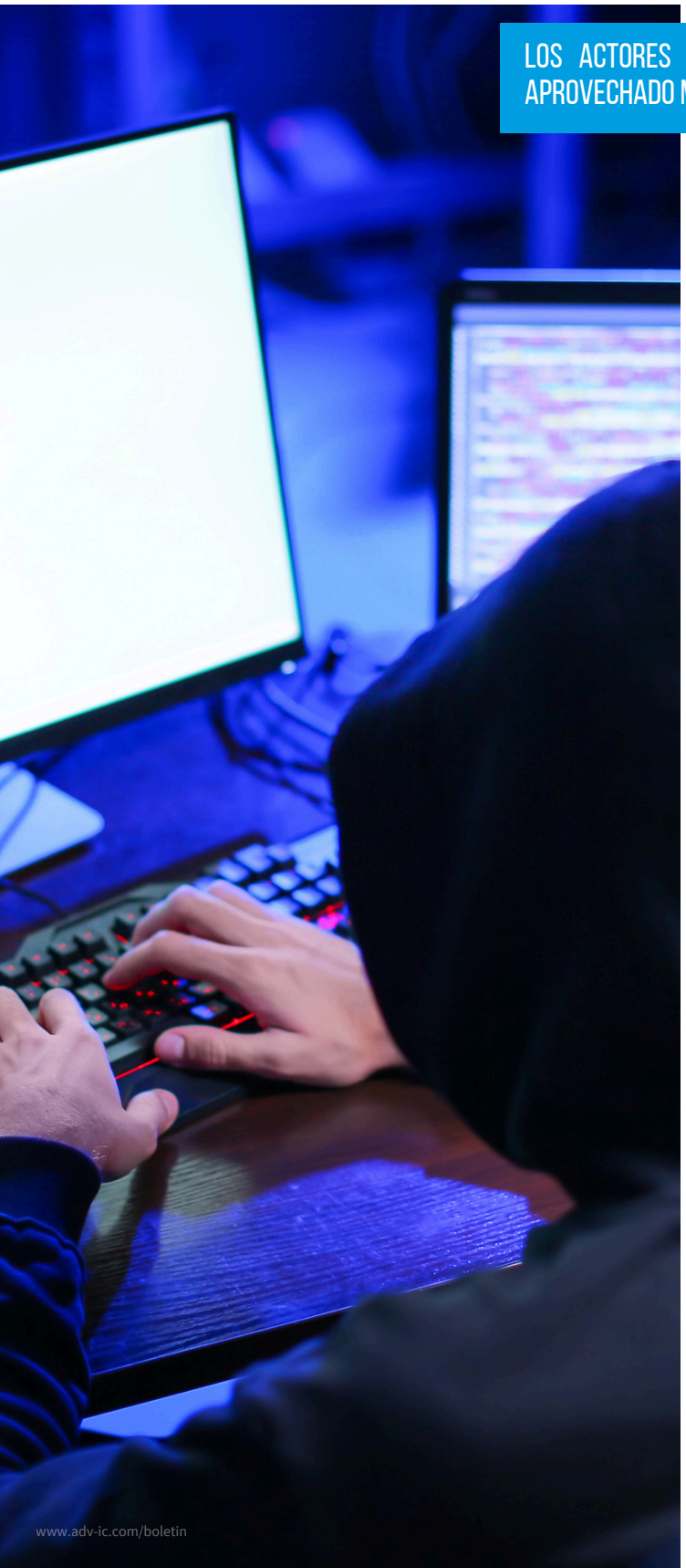
Los datos binarios ocultos en la imagen PNG son de Sliver, un marco C2 basado en Golang, diseñado para ser utilizado por profesionales de la seguridad en operaciones de equipo rojo.

El objetivo exacto del paquete aún no está claro, pero este desarrollo es otra señal de que los ecosistemas de código abierto continúan siendo un objetivo atractivo para la distribución de malware.

Dado que una gran parte del código depende de software de código abierto, la continua entrada de malware en repositorios como npm, PyPI y otros registros de paquetes, junto con episodios recientes como el de XZ Utils, subraya la necesidad de abordar sistemáticamente problemas que podrían "descarrilar grandes porciones de la red".

The Hacker News. (n.d.). Malicious Python package hides Sliver C2 framework in fake requests library logo. https://thehackernews.com/2024/05/malicious-python-package-hides-sliver.html

LOS INVESTIGADORES ESTÁN ALERTANDO SOBRE UNA TÉCNICA DE ATAQUE DDOS (DENEGACIÓN DE SERVICIO DISTRIBUIDO) LLAMADA CATDDOS BOTNET Y DNSBOMB.



LOS ACTORES DE AMENAZAS DETRÁS DE LA BOTNET DE MALWARE CATDDOS HAN APROVECHADO MÁS DE 80 VULNERABILIDADES CONOCIDAS.

Los actores de amenazas detrás de la botnet de malware CatDDoS han aprovechado más de 80 vulnerabilidades conocidas en varios programas durante los últimos tres meses para infiltrarse en dispositivos vulnerables y convertirlos en parte de una botnet para llevar a cabo ataques distribuidos de denegación de servicio (DDoS).

El equipo de QiAnXin XLab comentó: "Las muestras relacionadas con CatDDoS han utilizado una variedad de vulnerabilidades conocidas para propagar muestras. Además, se ha observado que el número máximo de objetivos supera los 300+ por día".

Estas vulnerabilidades afectan a una amplia gama de dispositivos y equipos de red, incluidos enrutadores, equipos de red y otros dispositivos de proveedores como Apache (ActiveMQ, Hadoop, Log4j y RocketMQ), Cacti, Cisco, D-Link, DrayTek, FreePBX, GitLab, Gocloud, Huawei, Jenkins, Linksys, Metabase, NETGEAR, Realtek, Seagate, SonicWall, Tenda, TOTOLINK, TP-Link, ZTE y Zyxel, entre otros.

CatDDoS fue previamente documentado por QiAnXin y NSFOCUS a finales de 2023, siendo descrito como una variante de la botnet Mirai capaz de realizar ataques DDoS utilizando varios métodos, incluyendo UDP, TCP, entre otros.

El malware, que fue detectado por primera vez en agosto de 2023, ha recibido el nombre de CatDDoS debido a las referencias relacionadas con gatos, como "catddos.pirate" y "password_meow", presentes en el código fuente del artefacto y en los nombres de dominio de comando y control (C2).

LOS INVESTIGADORES ESTÁN ALERTANDO SOBRE UNA TÉCNICA DE ATAQUE DDOS (DENEGACIÓN DE SERVICIO DISTRIBUIDO) LLAMADA CATDDOS BOTNET Y DNSBOMB.

Según la información compartida por NSFOCUS en octubre de 2023, la mayoría de los objetivos de ataque del malware se encuentran en China, seguidos por Estados Unidos, Japón, Singapur, Francia, Canadá, Reino Unido, Bulgaria, Alemania, Países Bajos e India.

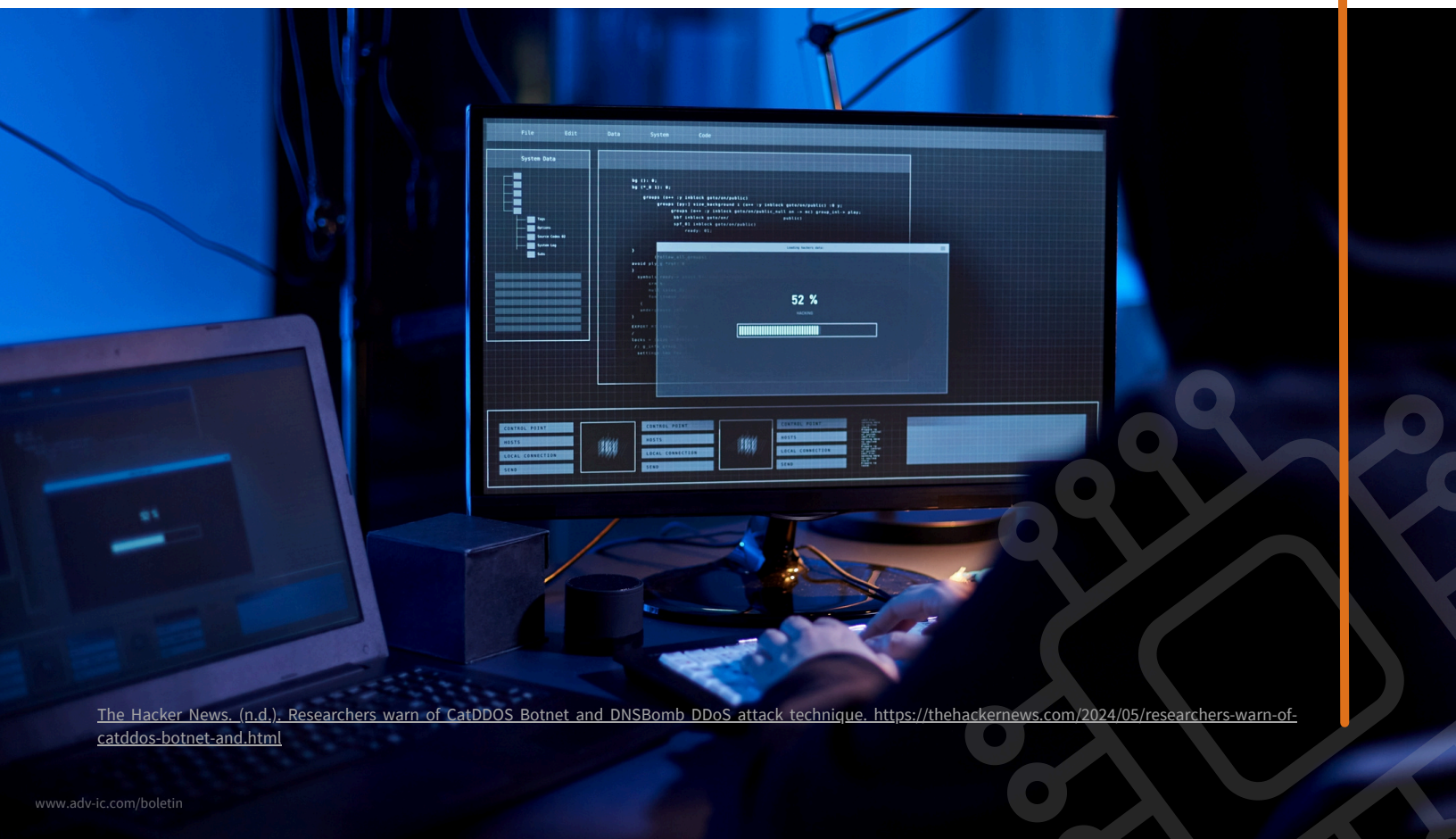
Además de cifrar las comunicaciones con el servidor C2 utilizando el algoritmo ChaCha20, el malware utiliza un dominio OpenNIC para el C2 en un intento de evadir la detección, una técnica que fue previamente adoptada por otra botnet DDoS basada en Mirai llamada Fodcha.

En un giro interesante, CatDDoS comparte el mismo par de clave/nonce para el algoritmo ChaCha20 con otras tres botnets DDoS llamadas hailBot, VapeBot y Woodman.

Según XLab, los ataques se centran principalmente en países como Estados Unidos, Francia, Alemania, Brasil y China, y afectan a una amplia gama de industrias, incluidos proveedores de servicios en la nube, educación, investigación científica, transmisión de información, administración pública, construcción y otras.

Se sospecha que los autores originales del malware cerraron sus operaciones en diciembre de 2023, pero antes de hacerlo pusieron a la venta el código fuente en un grupo dedicado de Telegram.

"Debido a la venta o filtración del código fuente, surgieron nuevas variantes, como RebirthLTD, Komaru, Cecilio Network, etc. después del cierre", explicaron los investigadores. "Aunque las diferentes variantes pueden ser administradas por diferentes grupos, hay poca variación en el código, diseño de comunicación, cadenas, métodos de descifrado, etc."



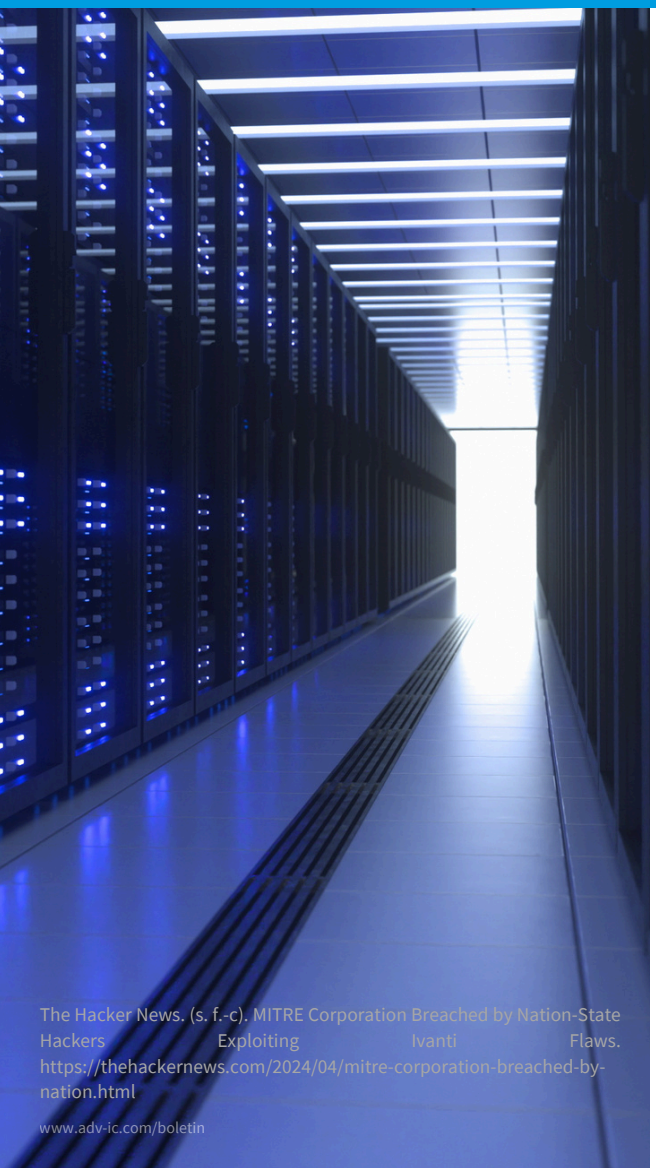
The Hacker News. (n.d.). Researchers warn of CatDDOS Botnet and DNSBomb DDoS attack technique. https://thehackernews.com/2024/05/researchers-warn-of-catddos-botnet-and.html

ALERTA DE CIBERESPIONAJE: LILACSQUID APUNTA A LOS SECTORES DE TI, ENERGÍA Y FARMACIA.

Según el investigador de Cisco Talos, Asheer Malhotra, en un nuevo informe técnico publicado recientemente, la campaña tiene como objetivo establecer un acceso prolongado a organizaciones víctimas comprometidas para permitir a LilacSquid exfiltrar datos de interés a servidores controlados por los atacantes.

Los objetivos de la campaña incluyen organizaciones de tecnología de la información que desarrollan software para los sectores industrial e investigativo en los EE. UU., empresas de energía en Europa y el sector farmacéutico en Asia, lo que indica una amplia gama de víctimas.

SE HA IDENTIFICADO UN ACTOR DE AMENAZAS HASTA AHORA NO DOCUMENTADO, LLAMADO LILACSQUID, INVOLUCRADO EN ATAQUES DIRIGIDOS QUE ABARCAN MÚLTIPLES SECTORES EN LOS ESTADOS UNIDOS (EE. UU.), EUROPA Y ASIA DESDE AL MENOS 2021 COMO PARTE DE UNA CAMPAÑA DE ROBO DE DATOS.



Se ha observado que las cadenas de ataque explotan vulnerabilidades conocidas públicamente para comprometer servidores de aplicaciones conectados a Internet, o utilizan credenciales de protocolo de escritorio remoto (RDP) comprometidas para implementar una combinación de herramientas de código abierto y malware personalizado.

La característica más distintiva de la campaña es el uso de una herramienta de administración remota de código abierto llamada MeshAgent, que actúa como canal para entregar una versión personalizada de Quasar RAT, con el nombre en código PurpleInk.

Los procedimientos de infección alternativos, que aprovechan las credenciales RDP comprometidas, muestran un modus operandi ligeramente diferente. En estos casos, los actores de amenazas eligen implementar MeshAgent o colocar un cargador basado en .NET llamado InkLoader para desplegar PurpleInk.

"Un inicio de sesión exitoso a través de RDP conduce a la descarga de InkLoader y PurpleInk, a la copia de estos artefactos en los directorios deseados en el disco y al posterior registro de InkLoader como un servicio que luego comienza a implementar InkLoader y, a su vez, PurpleInk", explicó Malhotra.

PurpleInk, mantenido activamente por LilacSquid desde 2021, es altamente obfuscado y versátil, lo que le permite ejecutar nuevas aplicaciones, realizar operaciones de archivos, obtener información del sistema, enumerar directorios y procesos, iniciar un shell remoto y conectarse a una dirección remota específica proporcionada por un servidor de comando y control (C2).

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

ALERTA DE CIBERESPIONAJE: LILACSQUID APUNTA A LOS SECTORES DE TI, ENERGÍA Y FARMACIA.

Las variantes recientes del troyano, descubiertas en 2023 y 2024, son mucho más rudimentarias: los autores del malware reducen las funciones para crear un shell inverso y comunicarse con un proxy para la transferencia de datos. Se presume que esto es un intento de eliminar funciones redundantes y evitar la detección.

Talos también identificó otra herramienta personalizada llamada InkBox, que se dice que fue utilizada por el adversario para implementar PurpleInk antes de cambiar a InkLoader.

La inclusión de MeshAgent como parte de sus manuales posteriores a la compromisión es notable en parte debido a que es una táctica previamente adoptada por un actor de amenazas norcoreano conocido como Andariel, un subgrupo dentro del infame Grupo Lazarus, en ataques dirigidos a compañías en Corea del Sur.

Otra área de superposición se refiere al uso de herramientas de túneles para mantener el acceso secundario, con LilacSquid implementando Secure Socket Funneling (SSF) para crear un canal de comunicación hacia su infraestructura.

"Múltiples tácticas, técnicas, herramientas y procedimientos (TTP) utilizados en esta campaña se superponen en cierta medida con los grupos APT norcoreanos, como Andariel y su grupo matriz, Lazarus", comentó Malhotra.

The Hacker News. (n.d.). Cyber espionage Alert: LilacSquid targets IT, energy, and pharma sectors. https://thehackernews.com/2024/05/cyber-espionage-alert-lilacsquid.html

CISA ESTÁ EMITIENDO UNA ALERTA A LAS AGENCIAS FEDERALES PARA QUE APLIQUEN PARCHES A UNA VULNERABILIDAD EN EL KERNEL DE LINUX QUE ESTÁ SIENDO ACTIVAMENTE EXPLOTADA.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha añadido una vulnerabilidad que afecta al kernel de Linux al catálogo de vulnerabilidades explotadas conocidas (KEV), citando evidencia de explotación activa.

Identificada como CVE-2024-1086 (con una puntuación CVSS de 7.8), esta vulnerabilidad de alta gravedad está relacionada con un error de uso después de la liberación en el componente netfilter. Esto permite a un atacante local elevar los privilegios de un usuario normal a root y posiblemente ejecutar código arbitrario.

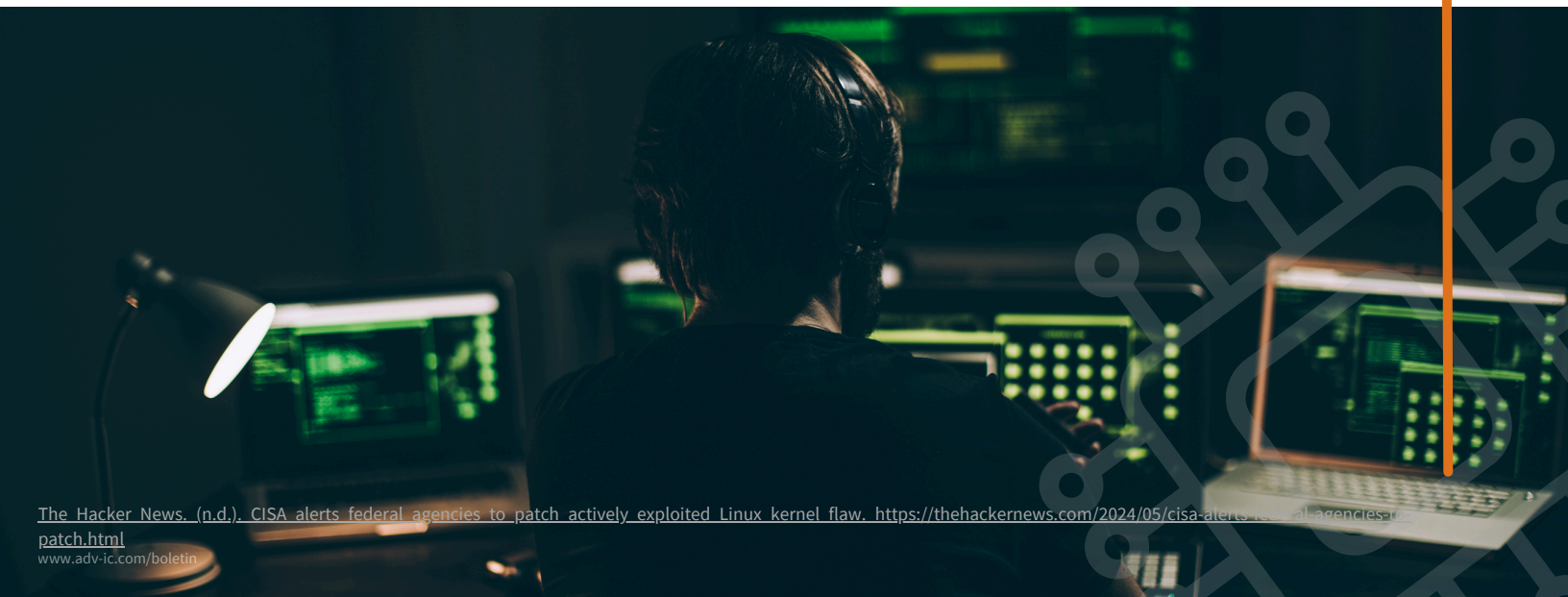
"CISA advierte que el kernel de Linux contiene una vulnerabilidad de uso después de la liberación en el componente netfilter, específicamente en nf_tables, lo que permite a un atacante lograr una escalada de privilegios local", explicó la agencia.

Netfilter es un marco proporcionado por el kernel de Linux que permite la implementación de diversas operaciones relacionadas con la red, como el filtrado de paquetes, la traducción de direcciones de red y la traducción de puertos, a través de controladores personalizados.

La vulnerabilidad se solucionó en enero de 2024. Sin embargo, actualmente se desconoce la naturaleza exacta de los ataques que aprovechan esta falla.

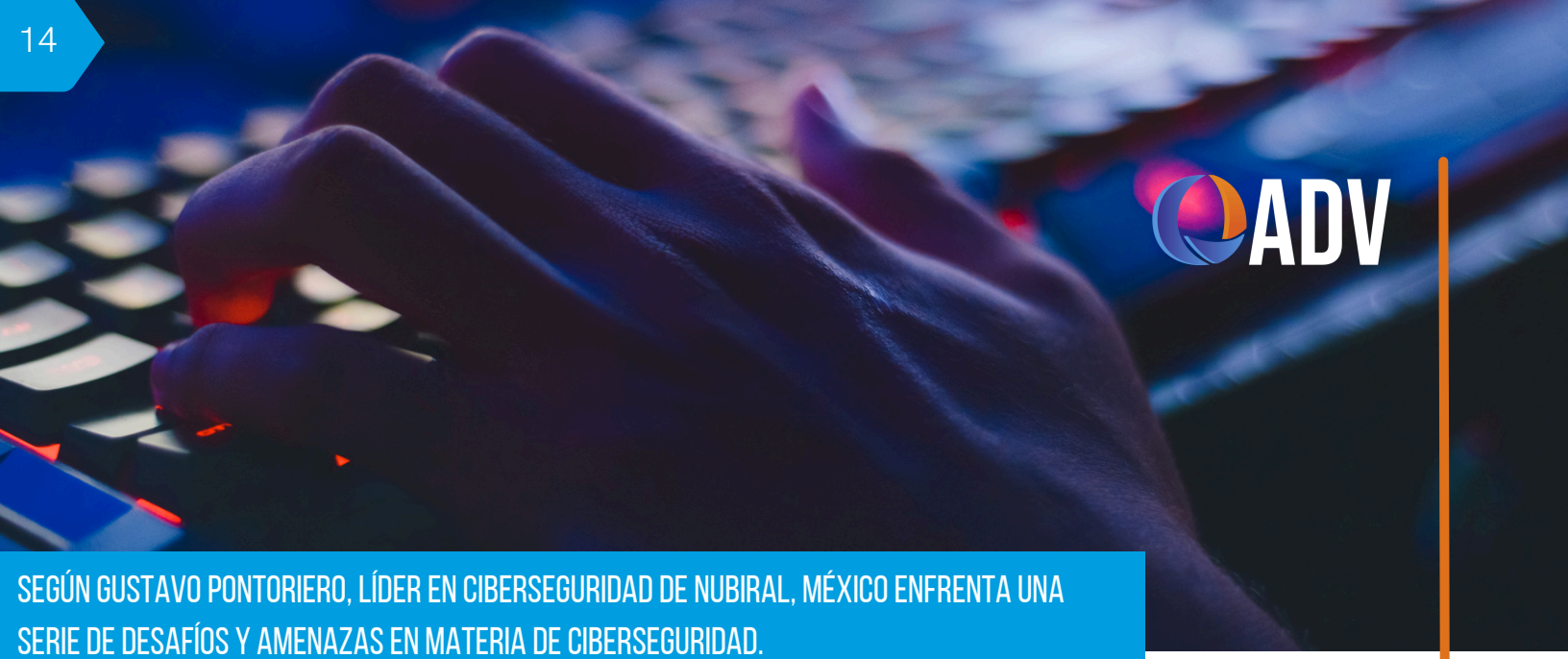
Además, se ha añadido al catálogo de KEV una recién revelada vulnerabilidad de seguridad que afecta a los productos de seguridad de la puerta de enlace de red de Check Point (CVE-2024-24919, con una puntuación CVSS de 7.5). Esta vulnerabilidad permite a un atacante leer información confidencial en puertas de enlace conectadas a Internet con acceso remoto VPN o acceso móvil habilitado.

Dada la explotación activa de CVE-2024-1086 y CVE-2024-24919, se recomienda a las agencias federales aplicar las últimas correcciones antes del 20 de junio de 2024 para proteger sus redes contra posibles amenazas.



The Hacker News. (n.d.). CISA alerts federal agencies to patch actively exploited Linux kernel flaw. https://thehackernews.com/2024/05/cisa-alerts-federal-agencies-to-patch.html

NOTICIAS NACIONALES



SEGÚN GUSTAVO PONTORIERO, LÍDER EN CIBERSEGURIDAD DE NUBIRAL, MÉXICO ENFRENTA UNA SERIE DE DESAFÍOS Y AMENAZAS EN MATERIA DE CIBERSEGURIDAD.

CIBERSEGURIDAD EN MÉXICO, LA INMADUREZ Y LA CONCIENCIA

México está en una coyuntura crítica en materia de ciberseguridad. Por un lado, su atractivo para los cibercriminales se debe a su creciente actividad digital, una cultura de seguridad cibernética aún en desarrollo y una legislación rezagada. Por otro lado, hay un aumento en la conciencia sobre la importancia de la ciberseguridad, tanto en el sector público como en el privado, lo que ha generado iniciativas para mejorar la situación.

Según Gustavo Pontoriero, líder en ciberseguridad de Nubiral, México enfrenta una serie de desafíos y amenazas en materia de ciberseguridad:

1. Atractivo para cibercriminales: México es un objetivo atractivo para los cibercriminales debido a su gran número de usuarios de internet, un sector financiero en crecimiento y una infraestructura digital en desarrollo.
2. Falta de madurez en la cultura de seguridad cibernética: Existe una falta de conciencia sobre los riesgos cibernéticos tanto en la población como en las empresas, lo que aumenta su vulnerabilidad.
3. Legislación obsoleta: La Ley de Protección de Datos Personales en México, de 2011, no está adaptada a las nuevas amenazas y desafíos, dejando lagunas en la protección.

Pontoriero mencionó que muchas empresas adoptan un enfoque reactivo en ciberseguridad, abordando los problemas solo después de que ocurre un incidente.

A pesar de estos desafíos, hay avances y oportunidades en la ciberseguridad en México:

1. Creciente conciencia: Tanto el sector público como el privado están tomando conciencia de la importancia de la ciberseguridad.
2. Iniciativas gubernamentales: El gobierno está trabajando en una ley de ciberseguridad y en la implementación de un Centro Nacional de Respuesta a Incidentes Cibernéticos.
3. Soluciones tecnológicas: Hay cada vez más soluciones disponibles para protegerse contra los ciberataques.

CIBERSEGURIDAD EN MÉXICO, LA INMADUREZ Y LA CONCIENCIA

Andrés Mendoza, de ManageEngine, advirtió sobre el aumento en sofisticación y número de grupos cibercriminales locales.

Las recomendaciones para mejorar la ciberseguridad incluyen:

1. Fortalecer la cultura de seguridad cibernética mediante la educación de la población y las empresas.
2. Modernizar la legislación para adaptarla a los nuevos desafíos.
3. Invertir en tecnología para protegerse contra los ciberataques.
4. Promover la colaboración entre el sector público, el privado y la academia para combatir la ciberdelincuencia.

Pontoriero destacó la importancia de la resiliencia en caso de un ataque, ya que la ciberseguridad no es infalible.

Riquelme, R. (2024, May 5). Ciberseguridad en México: entre la inmadurez y la conciencia. El Economista. https://www.eleconomista.com.mx/tecnologia/Ciberseguridad-en-Mexico-entre-la-inmadurez-y-la-conciencia-20240503-0095.html

MÁS DEL 50% DEL TRÁFICO EN INTERNET EN MÉXICO ES GENERADO POR BOTS.

Según el estudio de Imperva, en México, los bots buenos representan apenas el 10.3% del tráfico de internet, mientras que los bots maliciosos constituyen el 42.8%. Las conexiones realizadas por seres humanos representan el 46.9% restante del tráfico total.

El 53% del tráfico de internet en México transita a través de redes de bots, tanto buenos como maliciosos, según un análisis de Imperva, una división de Thales, una empresa de ciberseguridad.

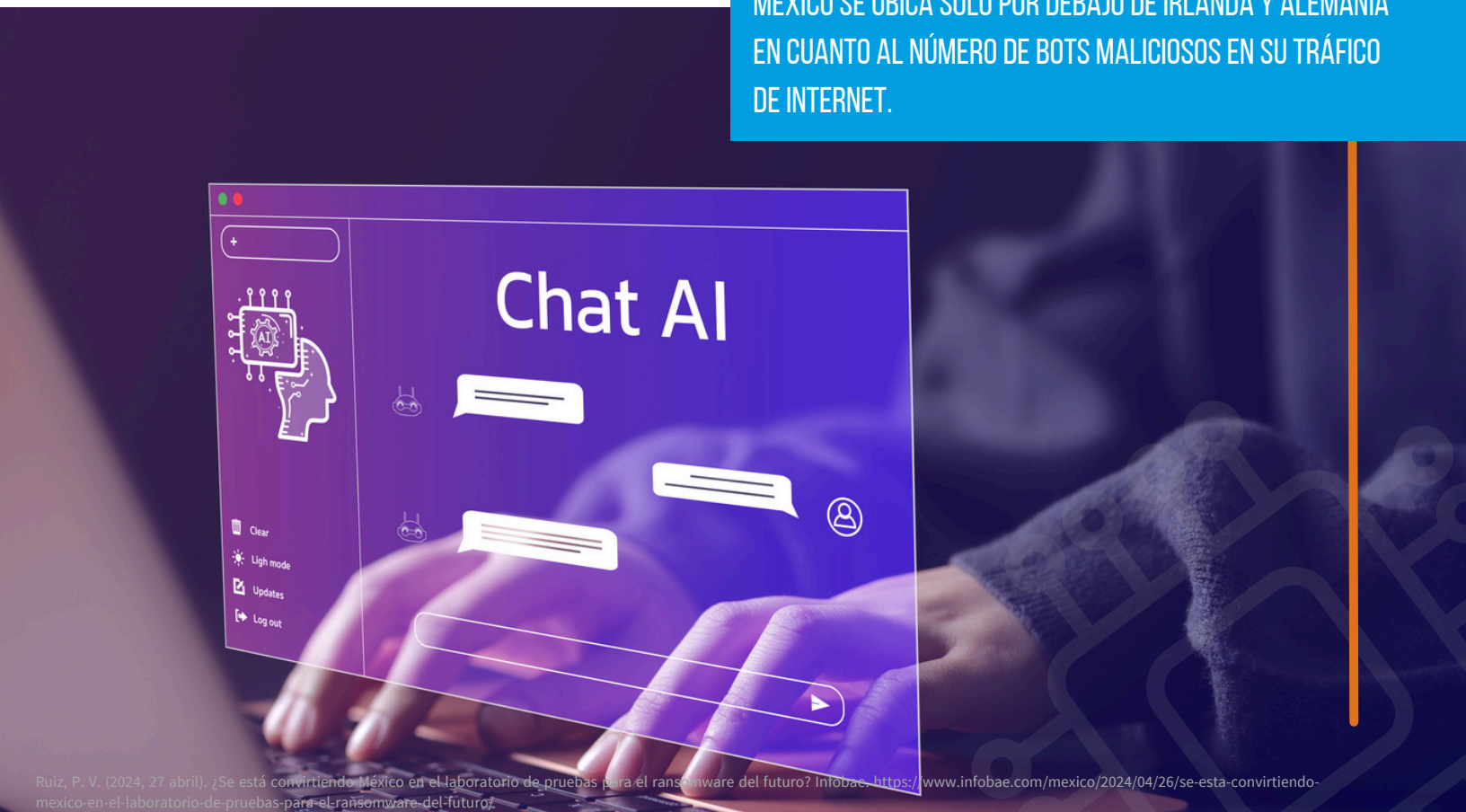
Por otro lado, el 46.9% del tráfico en las redes de internet en el país es generado por software y dispositivos controlados por seres humanos, de acuerdo con el mismo estudio.

Esto posiciona a México como uno de los países donde el tráfico de internet está mayormente influenciado por redes de bots.

Un bot es una aplicación de software que realiza tareas de forma automatizada, que van desde acciones simples como llenar formularios hasta tareas más complejas como analizar sitios web en busca de datos.

Existen bots buenos, como los encargados de indexar contenido en internet, y bots maliciosos, cuyas acciones tienen un propósito dañino, como extraer datos de sitios web sin permiso o realizar ataques de Denegación de Servicio (DDoS).

MÉXICO SE UBICA SOLO POR DEBAJO DE IRLANDA Y ALEMANIA EN CUANTO AL NÚMERO DE BOTS MALICIOSOS EN SU TRÁFICO DE INTERNET.



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/

MÁS DEL 50% DEL TRÁFICO EN INTERNET EN MÉXICO ES GENERADO POR BOTS.

En México, los bots buenos representan solo el 10.3% del tráfico de internet, mientras que el 42.8% corresponde a bots maliciosos. Las conexiones realizadas por seres humanos constituyen el 46.9% restante del tráfico total.

México se ubica solo por debajo de Irlanda y Alemania en cuanto al número de bots maliciosos en su tráfico de internet. Sin embargo, la mayoría de los ataques de redes de bots no se originan en los países con mayor presencia de estos, sino en Estados Unidos, Países Bajos, Australia, Reino Unido, entre otros.

Sergio Martínez, Director de Investigación y Desarrollo de IQSEC, destaca la importancia del conocimiento y la conciencia sobre los riesgos digitales, especialmente en el contexto de las elecciones, como primera línea de defensa para los electores y la población en general, para salvaguardar su privacidad y seguridad en línea.

Riquelme, R. (2024, May 14). La mitad del tráfico en internet en México pasa por bots. El Economista. https://www.eleconomista.com.mx/tecnologia/La-mitad-del-trafico-en-internet-en-Mexico-pasa-por-bots-20240513-0079.html

DURANTE EL AÑO, LOS INTENTOS DE ATAQUES CIBERNÉTICOS CONTRA EL INSTITUTO NACIONAL ELECTORAL (INE) EXPERIMENTARON UN INCREMENTO SUPERIOR AL 500 POR CIENTO.

PROCESO ELECTORAL EN MÉXICO ENFRENTA RIESGO POR ACTIVIDAD DE CIBERCRIMINALES.

En el contexto del proceso electoral de México, programado para el 2 de junio y que involucra la elección de más de 20 mil cargos públicos, los expertos en ciberseguridad mantienen una preocupación significativa. Existe un gran riesgo de que el Instituto Nacional Electoral (INE) sea objeto de un ataque informático, lo que podría cuestionar los resultados de la elección.

Verónica Becerra, miembro del Consejo de Seguridad de Información y Ciberseguridad (Consejociac), advirtió que la probabilidad de un ciberataque durante el proceso electoral es alta, dado que el INE ha experimentado un aumento significativo en el número de intentos de ciberataques desde el inicio de 2024.

Según datos proporcionados por el propio órgano electoral, los intentos de ciberataques han aumentado en más del 500 por ciento en comparación con el año anterior. Mientras que en 2023 se registraban seis intentos por minuto, este año se han registrado en promedio 32 intentos por minuto.

Hasta el momento, el órgano responsable de la organización de las elecciones en el país ha sido blanco de al menos 8.2 millones de intentos de ciberataques en lo que va del año. Según los expertos, esto debería considerarse como una señal de alarma sobre lo que podría suceder durante la jornada electoral de este domingo.

Víctor Ruiz, fundador de la empresa de ciberseguridad Silikn, destacó la necesidad de que tanto las autoridades gubernamentales como los organismos electorales y los proveedores de servicios en línea colaboren estrechamente para mitigar los riesgos de ataques durante la elección.

Según el experto, el principal riesgo al que se enfrenta el INE es ser blanco de un ataque de denegación de servicio (DDoS), que busca saturar los servidores con un flujo masivo de tráfico malicioso, lo que dejaría los servicios inaccesibles para los usuarios.

Durante el segundo semestre de 2023, México enfrentó un total de 16,711 ataques en línea de tipo DDoS, según datos del Reporte sobre ataques DDoS elaborado por Netscout System. Este tipo de amenaza se posicionó como la tercera más significativa, después del ransomware y el phishing.

PROCESO ELECTORAL EN MÉXICO ENFRENTA RIESGO POR ACTIVIDAD DE CIBERCRIMINALES.

La reducción en el presupuesto del INE a lo largo del mandato de Andrés Manuel López Obrador es motivo de preocupación tanto para expertos como para empresas de ciberseguridad. Esta disminución ha elevado las alertas sobre la posibilidad de un ataque a los servidores del organismo electoral.

En 2024, año de la elección más grande en la historia de México, el Congreso asignó al INE un presupuesto de 8,808 millones de pesos, lo que representó una reducción de 552 millones de pesos en comparación con los 9,355 millones de pesos aprobados para 2023, un año en el que solo se llevaron a cabo elecciones en tres estados del país (Tamaulipas, Coahuila y Estado de México).

Verónica Becerra, también cofundadora de la empresa de ciberseguridad Offhack, advirtió que el recorte presupuestario al INE es uno de los principales riesgos identificados, ya que podría afectar la capacidad de prevención y respuesta ante un ciberataque. Sin embargo, destacó que con la implementación adecuada de políticas y tecnología, se puede minimizar el riesgo de un eventual ataque cibernético.

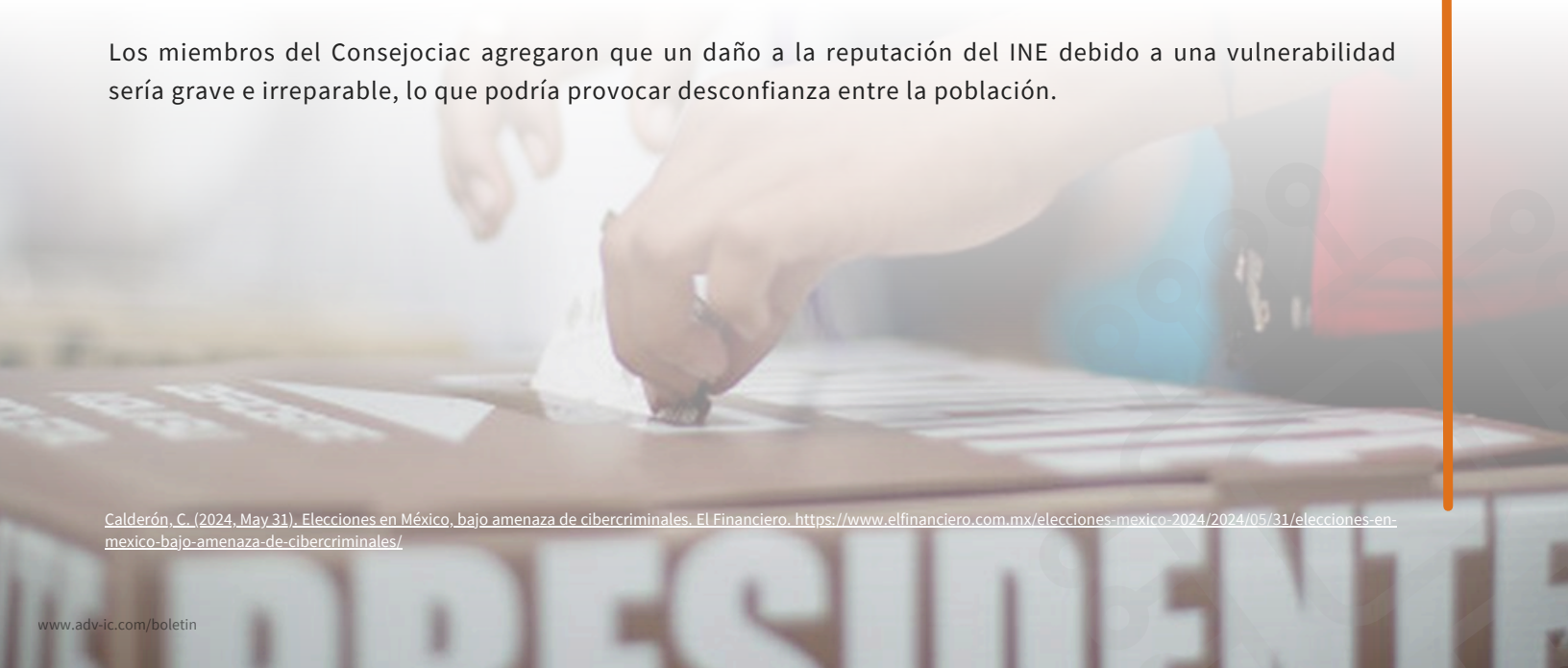
Víctor Ruiz advirtió que la reducción presupuestaria podría convertir al INE en un objetivo para hackers de distintos países, interesados en interferir en el proceso electoral mexicano por motivos políticos o para perpetrar delitos financieros.

"Este informe es preocupante porque atrae la atención de grupos de cibercriminales de Rusia, Corea del Norte, China, Estados Unidos, Reino Unido e Israel", señaló el directivo, resaltando que el mayor peligro reside en posibles ataques cibernéticos locales con el objetivo de influir en la elección de este año por motivos políticos.

La reputación del INE está en juego según expertos en ciberseguridad, quienes sostienen que el éxito del proceso electoral del 2 de junio determinará su prestigio y continuidad como organizador de elecciones.

"Es importante recordar que en este gobierno se ha intentado debilitar al INE y si fracasa en este proceso y no asegura la democracia, justificará la narrativa del presidente", comentó el CEO de Silikn.

Los miembros del Consejociac agregaron que un daño a la reputación del INE debido a una vulnerabilidad sería grave e irreparable, lo que podría provocar desconfianza entre la población.



Calderón, C. (2024, May 31). Elecciones en México, bajo amenaza de cibercriminales. El Financiero. https://www.elfinanciero.com.mx/elecciones-mexico-2024/2024/05/31/elecciones-en-mexico-bajo-amenaza-de-cibercriminales/

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: MAYO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-28075	14/05/2024	Fallas de seguridad en productos SolarWinds	CVSS v3.1: 9.0 [critico]	https://https://nvd.nist.gov/vuln/detail/CVE-2024-28075

Descripción: SolarWinds Access Rights Manager era susceptible a una vulnerabilidad de ejecución remota de código. Esta vulnerabilidad permite que un usuario autenticado abuse del servicio SolarWinds, lo que resulta en la ejecución remota de código. Agradecemos a Trend Micro Zero Day Initiative (ZDI) por su asociación continua para coordinar con SolarWinds la divulgación responsable de esta y otras vulnerabilidades potenciales.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-4671	14/05/2024	Fallas de seguridad en productos Google	CVSS v3.1: 9.6 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-4671

Descripción: El uso gratuito en Visuals en Google Chrome anterior a 124.0.6367.201 permitió a un atacante remoto que había comprometido el proceso de renderizado realizar potencialmente un escape de la zona de pruebas a través de una página HTML diseñada. (Severidad de seguridad de Chrome: alta)

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-5150	28/05/2024	Fallas de seguridad en productos WordPress	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-5150

Descripción: El complemento Iniciar sesión con número de teléfono para WordPress es vulnerable a la omisión de autenticación en versiones hasta la 1.7.26 inclusive. Esto se debe a que el valor predeterminado 'activation_code' está vacío y falta la verificación de no vacío en la función 'lwp_ajax_register'. Esto hace posible que atacantes no autenticados inicien sesión como cualquier usuario existente en el sitio, como un administrador, si tienen acceso al correo electrónico del usuario. La vulnerabilidad se parcheó en la versión 1.7.26, pero hay un problema en el parche que hace que toda la función no funcione, y este problema se solucionó en la versión 1.7.27.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-3200	31/05/2024	Fallas de seguridad en productos WordPress	CVSS v3.1: 9.9 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-3200

Descripción: Complemento wpForo Forum para WordPress es vulnerable a la inyección SQL a través del atributo 'slug' del shortcode 'wpforo' en todas las versiones hasta la 2.3.3 inclusive debido a un escape insuficiente en el parámetro proporcionado por el usuario y a la 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-2024-30049	14/05/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 7.8 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-30049

Descripción: Vulnerabilidad de elevación de privilegios del subsistema kernel de Windows Win32.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-30051	14/05/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 7.8 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-30051

Descripción: Vulnerabilidad de elevación de privilegios de la biblioteca principal de Windows DWM

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-3745	18/05/2024	Fallas de seguridad en productos MSI	CVSS v3.1: 7.8 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-3745

Descripción: MSI Afterburner v4.6.6.16381 Beta 3 es vulnerable a una vulnerabilidad de derivación de ACL en el controlador RTCore64.sys, lo que provoca la activación de vulnerabilidades como CVE-2024-1443 y CVE-2024-1460 por parte de un usuario con pocos privilegios.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-52827	21/05/2024	Fallas de seguridad en productos Linux	CVSS v3.1: 8.1 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2023-52827

Descripción: En el kernel de Linux, se resolvió la siguiente vulnerabilidad: wifi: ath12k: corrige una posible lectura fuera de límites en ath12k_htt_pull_ppdu_stats() len se extrae del mensaje HTT y podría ser un valor inesperado en caso de que ocurran errores, así que agregue validación antes de usarlo para evitar una posible lectura fuera de límites en la siguiente iteración y análisis del mensaje. El mismo problema también se aplica a ppdu_info->ppdu_stats.common.num_users, así que valídelo antes de usarlo también. Estos se encuentran durante la revisión del código. Compilar solo prueba.

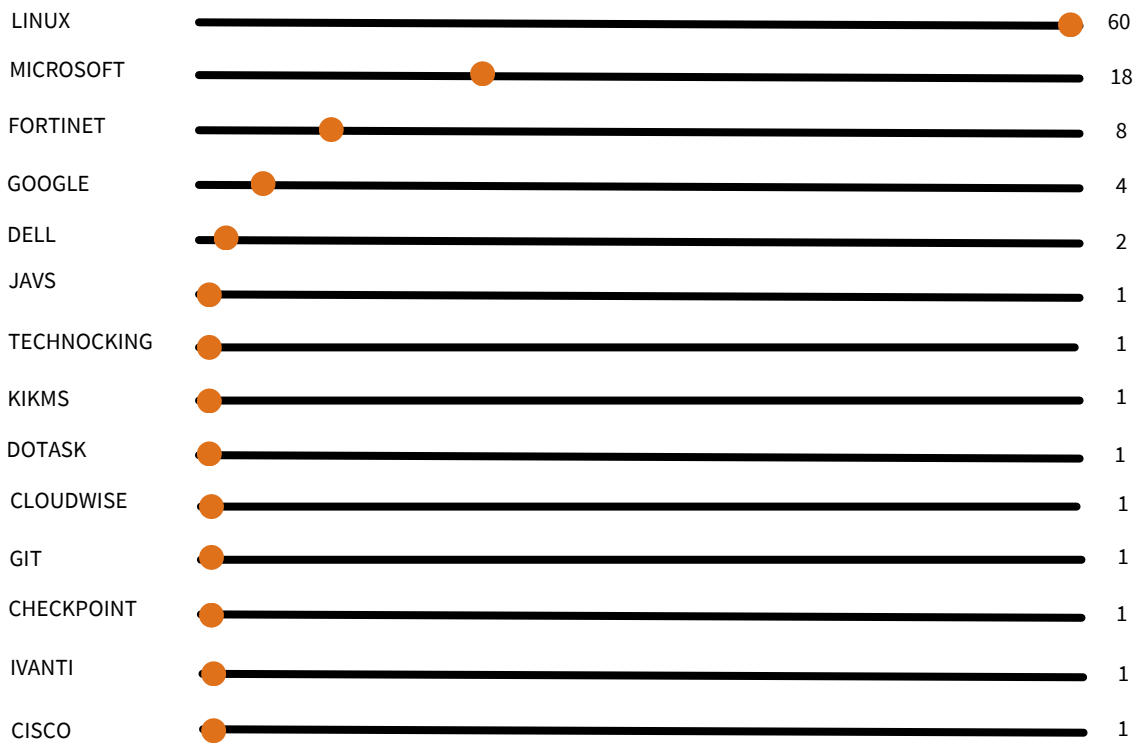
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-30280	23/05/2024	Fallas de seguridad en productos ADOBE	CVSS v3.1: 7.8 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-30280

Descripción: Las versiones de Acrobat Reader 20.005.30574, 24.002.20736 y anteriores se ven afectadas por una vulnerabilidad de lectura fuera de límites al analizar un archivo manipulado, lo que podría resultar en una lectura más allá del final de una estructura de memoria asignada. Un atacante podría aprovechar esta vulnerabilidad para ejecutar código en el contexto del usuario actual. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.

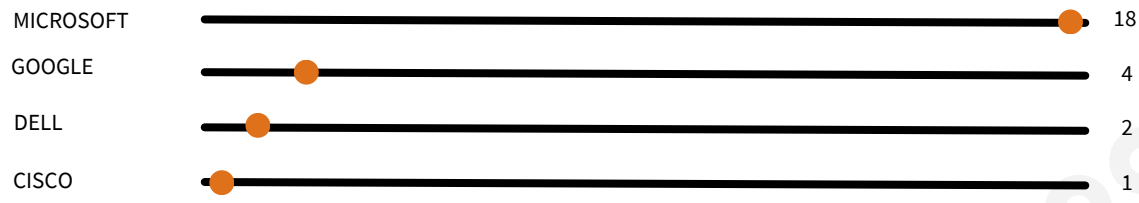
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-5274	28/05/2024	Fallas de seguridad en productos Google	CVSS v3.1: 8.8 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-5274

Descripción: Type Confusion en V8 en Google Chrome anterior a 125.0.6422.112 permitía a un atacante remoto ejecutar código arbitrario dentro de un sandbox a través de una página HTML diseñada. (Severidad de seguridad de Chrome: alta)r

FABRICANTES CON VULNERABILIDADES RELEVANTES: MAYO DE 2024



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: MAYO DE 2024



CULTURA DE CIBERSEGURIDAD

PRETEXTING

DEFINICIÓN

Es una técnica de ingeniería social en la que un atacante crea un pretexto o una historia convincente para engañar a una víctima y obtener información sensible o realizar acciones en nombre de la víctima. Estas estafas presentan una situación falsa pero creíble.

CÓMO FUNCIONA

- *Investigación Inicial:* El atacante recolecta información básica sobre la
- víctima para crear un pretexto convincente.
- *Creación del Pretexto:* Con la información recolectada, el atacante crea una historia o un escenario que parece legítimo. Esto puede ser un supuesto problema con una cuenta bancaria, una oportunidad laboral, una solicitud de asistencia técnica, etc.
- *Contacto con la Víctima:* El atacante se pone en contacto con la víctima, ya sea por teléfono, correo electrónico, redes sociales u otros medios de comunicación. Utiliza el pretexto creado para establecer una interacción.
- *Engaño y Persuasión:* A través del diálogo y la interacción, el atacante utiliza técnicas de persuasión para ganar la confianza de la víctima.
- *Explotación de la Información:* Una vez que el atacante obtiene la información deseada, la utiliza para sus fines, que pueden incluir el acceso a cuentas, robo de identidad, fraude financiero, etc.

RIESGOS / IMPORTANCIA DE CONOCER

Los ataques de pretexting pueden acarrear serias consecuencias para las víctimas, especialmente en el ámbito empresarial. Tales repercusiones incluyen:

- Divulgación de datos financieros sensibles.
- Exposición de información estratégica de la empresa.
- Riesgo de acceso no autorizado a sistemas y cuentas.
- Vulnerabilidad a futuros ataques y fraudes.
- Daño a la reputación y pérdida de confianza de los clientes.
- Posibles sanciones legales por incumplimiento de normativas de protección de datos.

CÓMO EVITARLO

Verificación de Identidad: Siempre verifica la identidad de la persona que solicita información sensible. Contacta a la organización directamente utilizando números de teléfono o direcciones de correo electrónico oficiales.

Cuidado con la Información Pública: Tener cuidado con la cantidad de información personal que se comparte en línea y en redes sociales, ya que los atacantes pueden utilizar estos datos para crear pretextos más creíbles.

Eitel, B. (2023, 1 junio). Dongles, sticks, unidades y llaves: lo que hay que saber sobre los medios extraíbles. Alianza Nacional de Ciberseguridad. https://staysafeonline.org/es/online-safety-privacy-basics/best-practices-for-removable-media-and-devices/

Formación del personal en ciberseguridad: La formación del personal en ciberseguridad es esencial para prevenir ataques de pretexting. Se deben impartir sesiones informativas periódicas sobre técnicas de engaño, identificación de riesgos y buenas prácticas en la protección de datos.

Implementación de protocolos de seguridad: La implementación de protocolos de seguridad robustos es clave en la prevención de ataques de pretexting. Es fundamental establecer políticas claras de acceso a la información, autenticación de usuarios y medidas de control de accesos para evitar filtraciones de datos sensibles.

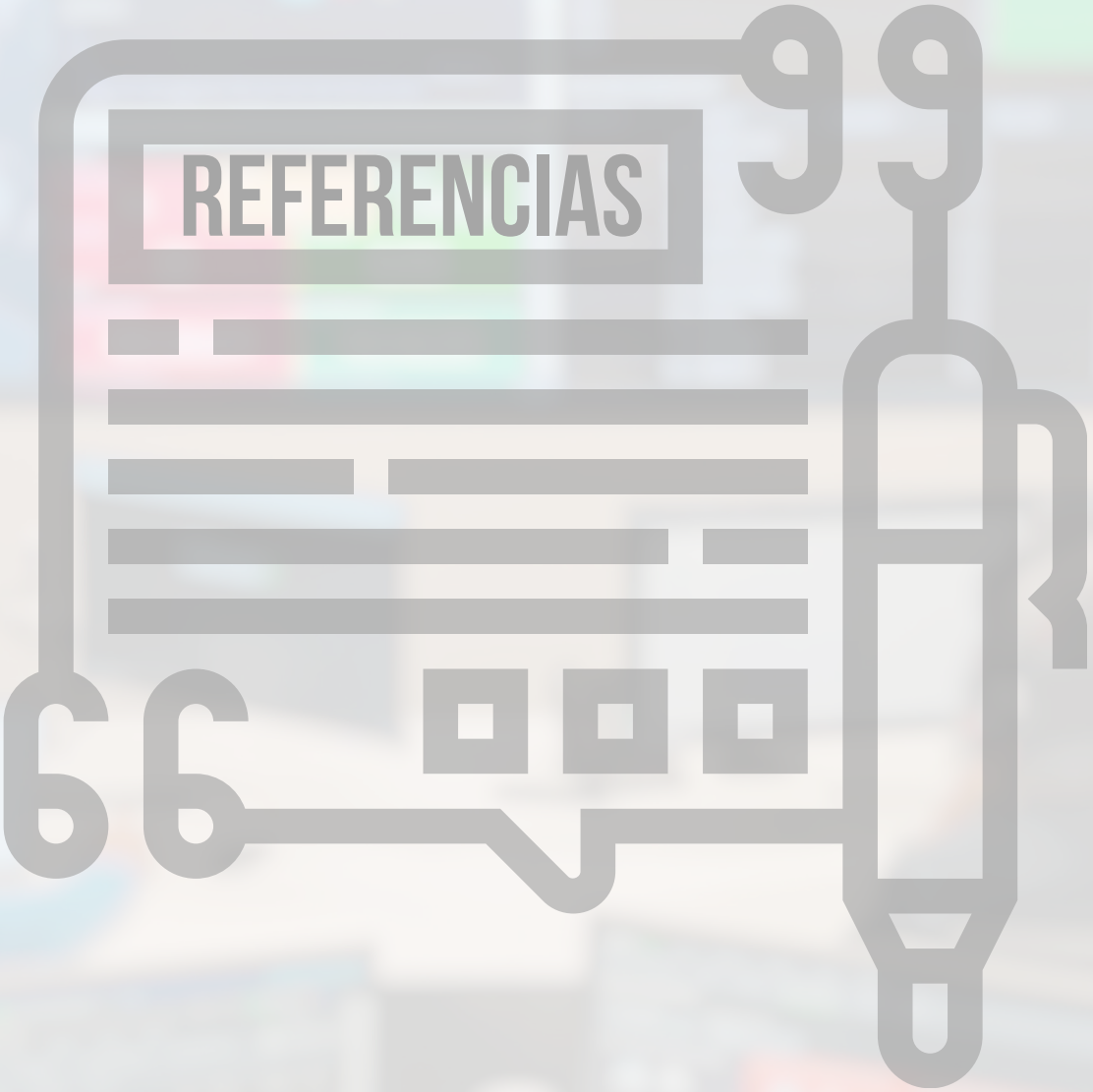
CÓMO DETECTARLO

Siempre verificando la identidad de la persona que solicita información sensible. Contactando a la organización directamente utilizando números de teléfono o direcciones de correo electrónico oficiales.

Desconfía de cualquier solicitud de información personal o financiera, especialmente si no esperabas la solicitud o si proviene de un contacto no verificado.

IBM. (s. f.). https://www.ibm.com/es-es/topics/social-engineering

REFERENCIAS



REFERENCIAS

- The Hacker News. (n.d.). Hackers exploiting LiteSpeed cache bug to gain full control of WordPress sites. https://thehackernews.com/2024/05/hackers-exploiting-litespeed-cache-bug.html
- The Hacker News. (n.d.). Malicious Python package hides Sliver C2 framework in fake requests library logo. https://thehackernews.com/2024/05/malicious-python-package-hides-sliver.html
- The Hacker News. (n.d.). Researchers warn of CatDDOS Botnet and DNSBomb DDoS attack technique. https://thehackernews.com/2024/05/researchers-warn-of-catddos-botnet-and.html
- The Hacker News. (n.d.). Cyber espionage Alert: LilacSquid targets IT, energy, and pharma sectors. https://thehackernews.com/2024/05/cyber-espionage-alert-lilacsquid.html
- The Hacker News. (n.d.). CISA alerts federal agencies to patch actively exploited Linux kernel flaw. https://thehackernews.com/2024/05/cisa-alerts-federal-agencies-to-patch.html
- Riquelme, R. (2024, May 5). Ciberseguridad en México: entre la inmadurez y la conciencia. El Economista. https://www.eleconomista.com.mx/tecnologia/Ciberseguridad-en-Mexico-entre-la-inmadurez-y-la-conciencia-20240503-0095.html
- Riquelme, R. (2024, May 14). La mitad del tráfico en internet en México pasa por bots. El Economista. https://www.eleconomista.com.mx/tecnologia/La-mitad-del-trafico-en-internet-en-Mexico-pasa-por-bots-20240513-0079.html
- Calderón, C. (2024, May 31). Elecciones en México, bajo amenaza de cibercriminales. El Financiero. https://www.elfinanciero.com.mx/elecciones-mexico-2024/2024/05/31/elecciones-en-mexico-bajo-amenaza-de-cibercriminales/

ZERU Cybersecurity Services

Security Operation Center - SOC by ADV

+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 Integradores y Consultores | adv-ic.mx | ADV.Integradores