BOLETÍN DE CIBERSEGURIDAD
JULIO 2024

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

ÍNDICE

NOTICIAS INTERNACIONALES

MALWARE VINCULADO A COREA DEL NORTE APUNTA A DESARROLLADORES EN WINDOWS, LINUX Y MACOS

LOS ACTORES DE AMENAZAS RESPONSABLES DE UNA CAMPAÑA DE MALWARE EN CURSO QUE TIENE COMO OBJETIVO A DESARROLLADORES DE SOFTWARE HAN PRESENTADO NUEVAS VARIANTES Y TÁCTICAS, AMPLIANDO SU ENFOQUE PARA INCLUIR SISTEMAS WINDOWS, LINUX Y MACOS.

Este grupo de actividad, conocido como DEV#POPPER y vinculado a Corea del Norte, ha identificado a víctimas en Corea del Sur, América del Norte, Europa y Oriente Medio.

"Este tipo de ataque es una forma avanzada de ingeniería social, diseñada para manipular a las personas y hacer que revelen información confidencial o realicen acciones que normalmente no llevarían a cabo," comentaron los investigadores Den Iuzvyk y Tim Peck de Securonix en un nuevo informe compartido con The Hacker News.

Ciberseguridad

DEV#POPPER es el nombre asignado a una activa campaña de malware que engaña a los desarrolladores de software para que descarguen software comprometido alojado en GitHub bajo la apariencia de una entrevista de trabajo. Esta campaña tiene similitudes con una rastreada por Palo Alto Networks Unit 42 bajo el nombre de Entrevista Contagiosa.

Los signos de que la campaña era más amplia y abarcaba múltiples plataformas surgieron a principios de este mes, cuando los investigadores descubrieron artefactos dirigidos tanto a Windows como a macOS que distribuían una versión actualizada de un malware llamado BeaverTail.

Malware Vinculado a Corea del Norte

El documento de ataque de Securonix muestra que los actores de amenazas se hacen pasar por entrevistadores para un puesto de desarrollador e instan a los candidatos a descargar un archivo ZIP para una tarea de codificación.

Dentro del archivo ZIP se encuentra un módulo npm que, una vez instalado, ejecuta un JavaScript ofuscado (es decir, BeaverTail) que identifica el sistema operativo en el que se ejecuta y establece contacto con un servidor remoto para exfiltrar datos de interés.

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

MALWARE VINCULADO A COREA DEL NORTE APUNTA A DESARROLLADORES EN WINDOWS, LINUX Y MACOS

También tiene la capacidad de descargar cargas útiles adicionales, incluyendo un backdoor en Python conocido como InvisibleFerret, diseñado para recopilar metadatos detallados del sistema, acceder a cookies almacenadas en navegadores web, ejecutar comandos, subir/descargar archivos, así como registrar pulsaciones de teclas y contenido del portapapeles.

Entre las nuevas características de las muestras recientes se incluyen el uso de ofuscación avanzada, software de monitoreo y gestión remota (RMM) AnyDesk para persistencia, y mejoras en el mecanismo FTP utilizado para la exfiltración de datos.

Además, el script en Python actúa como un conducto para ejecutar un script auxiliar encargado de robar información sensible de varios navegadores web – Google Chrome, Opera y Brave – en diferentes sistemas operativos.

"Esta extensión sofisticada de la campaña DEV#POPPER original sigue utilizando scripts en Python para ejecutar un ataque de múltiples etapas centrado en la exfiltración de información sensible de las víctimas, ahora con capacidades mucho más robustas," indicaron los investigadores.

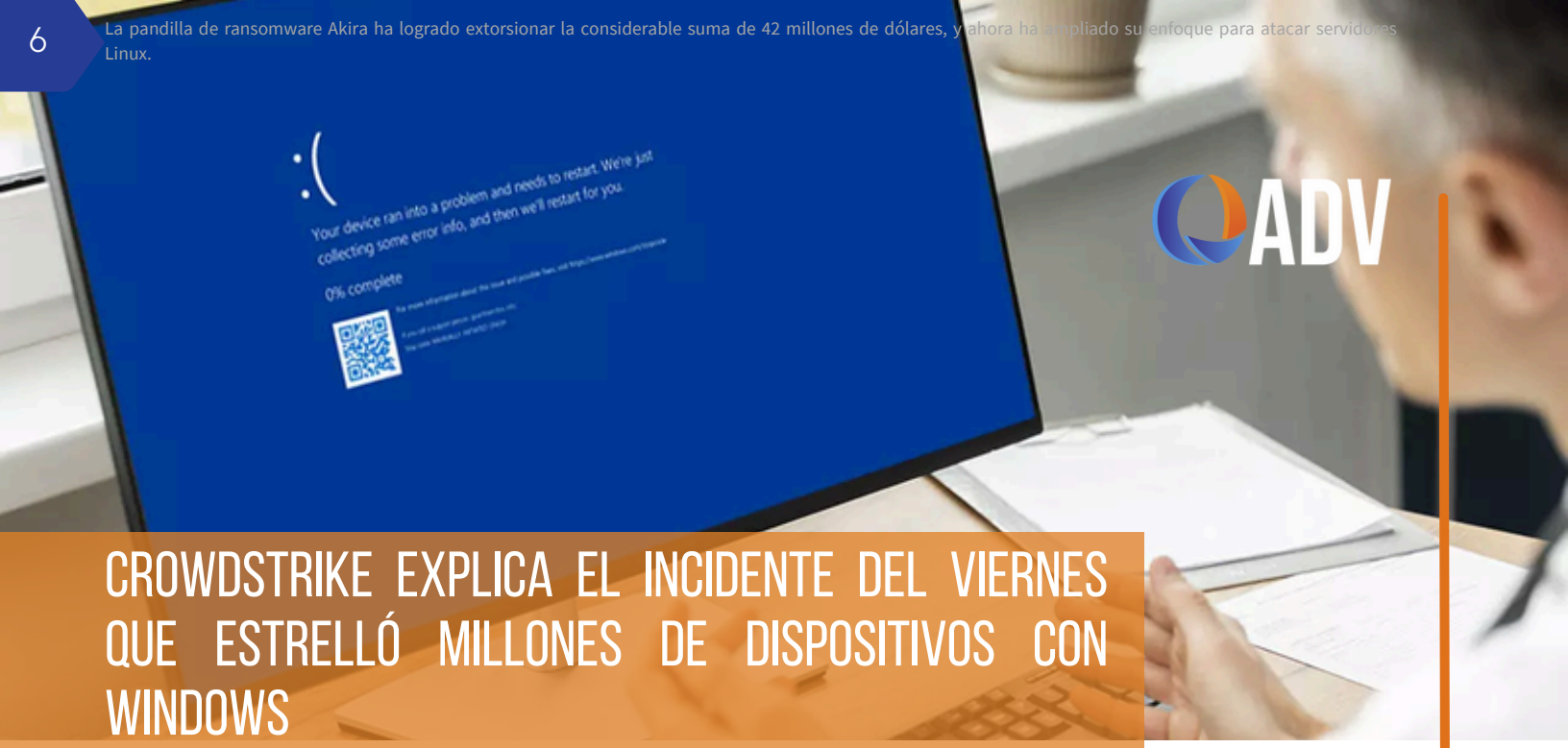
Estos hallazgos se producen cuando Recorded Future reveló que Corea del Norte ha continuado utilizando tecnología extranjera – como dispositivos de Apple, Samsung, Huawei y Xiaomi, así como diversas plataformas de redes sociales como Facebook, X, Instagram, WeChat, LINE y QQ – para acceder a Internet a pesar de las estrictas sanciones.

Otro cambio significativo en el comportamiento de los usuarios de Internet es el uso de redes privadas virtuales (VPN) y proxies para evadir la censura y la vigilancia, así como la utilización de software antivirus de McAfee, lo que indica que el país no está tan aislado como se cree.

"A pesar de las sanciones, Corea del Norte sigue importando tecnología extranjera, a menudo a través de sus relaciones comerciales con China y Rusia," comentó la empresa. "Esto marca un cambio hacia una mayor conciencia de seguridad operativa entre los usuarios que buscan evitar la detección por parte del régimen."

The Hacker News. (s. f.). North Korea-Linked Malware Targets Developers on Windows, Linux, and macOS. https://thehackernews.com/2024/07/north-korea-linked-malware-targets.html

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.



CROWDSTRIKE EXPLICA EL INCIDENTE DEL VIERNES QUE ESTRELLÓ MILLONES DE DISPOSITIVOS CON WINDOWS

"El viernes 19 de julio de 2024 a las 04:09 UTC, como parte de las operaciones regulares, CrowdStrike lanzó una actualización de configuración de contenido para el sensor de Windows con el fin de recopilar telemetría sobre posibles nuevas técnicas de amenaza," indicó la empresa en su Revisión Preliminar del Incidente (PIR).

"Estas actualizaciones son una parte regular de los mecanismos de protección dinámica de la plataforma Falcon. La actualización problemática de Configuración de Contenido de Respuesta Rápida resultó en un bloqueo del sistema Windows."

El incidente afectó a los equipos Windows que ejecutaban la versión 7.11 del sensor o superior y que estaban en línea entre el 19 de julio de 2024, a las 04:09 UTC y las 05:27 UTC, y que recibieron la actualización. Los sistemas Apple macOS y Linux no se vieron afectados.

CrowdStrike explicó que entrega actualizaciones de configuración de contenido de seguridad de dos maneras: una a través del Contenido del Sensor, que se envía con el Falcon Sensor, y otra a través del Contenido de Respuesta Rápida, que permite identificar amenazas novedosas mediante diversas técnicas de coincidencia de patrones de comportamiento.

Se afirma que el bloqueo fue causado por una actualización de Contenido de Respuesta Rápida que contenía un error previamente no detectado. Cabe destacar que dichas actualizaciones se entregan en forma de Instancias de Plantilla, correspondientes a comportamientos específicos, cada una mapeada a un Tipo de Plantilla único, para habilitar nueva telemetría y detección.

Las Instancias de Plantilla se crean usando un Sistema de Configuración de Contenido, y luego se despliegan al sensor a través de la nube mediante un mecanismo denominado Archivos de Canal, que finalmente se escriben en el disco de la máquina Windows. El sistema también incluye un componente Validador de Contenido que realiza verificaciones en el contenido antes de su publicación.

"El Contenido de Respuesta Rápida proporciona visibilidad y detección en el sensor sin requerir cambios en el código del sensor," explicó la empresa.

"Esta capacidad es utilizada por los ingenieros de detección de amenazas para recopilar telemetría, identificar indicadores de comportamiento adversario y realizar detecciones y prevenciones. El Contenido de Respuesta

CROWDSTRIKE EXPLICA EL INCIDENTE DEL VIERNES QUE ESTRELLÓ MILLONES DE DISPOSITIVOS CON WINDOWS

Rápida se basa en heurísticas de comportamiento, distintas y separadas de las capacidades de prevención y detección basadas en IA del sensor de CrowdStrike."

Estas actualizaciones son luego procesadas por el Intérprete de Contenido del sensor Falcon, que permite que el Motor de Detección del Sensor detecte o prevenga actividades maliciosas, dependiendo de la configuración de política del cliente.

Aunque cada nuevo Tipo de Plantilla es sometido a pruebas de estrés para parámetros como utilización de recursos e impacto en el rendimiento, CrowdStrike rastrea la causa raíz del problema hasta el lanzamiento del Tipo de Plantilla de Comunicación entre Procesos (IPC) el 28 de febrero de 2024, diseñado para detectar ataques que abusan de pipes nombrados.

La cronología de eventos es la siguiente:

- 28 de febrero de 2024: CrowdStrike lanza la versión 7.11 del sensor con el nuevo Tipo de Plantilla IPC
- 5 de marzo de 2024: El Tipo de Plantilla IPC pasa la prueba de estrés y es validado para su uso
- 5 de marzo de 2024: La Instancia de Plantilla IPC se lanza en producción a través del Archivo de Canal 291
- 8 - 24 de abril de 2024: Se despliegan tres Instancias de Plantilla IPC adicionales en producción
- 19 de julio de 2024: Se despliegan dos Instancias de Plantilla IPC adicionales, una de las cuales pasa la validación a pesar de tener datos de contenido problemáticos
- "Basado en las pruebas realizadas antes del despliegue inicial del Tipo de Plantilla (el 5 de marzo de 2024), la confianza en las verificaciones realizadas por el Validador de Contenido y los despliegues exitosos anteriores de Instancias de Plantilla IPC, estas instancias fueron desplegadas en producción," señaló CrowdStrike.

"Cuando fueron recibidas por el sensor y cargadas en el Intérprete de Contenido, el contenido problemático en el Archivo de Canal 291 resultó en una lectura de memoria fuera de límites que desencadenó una excepción. Esta excepción inesperada no pudo ser manejada adecuadamente, resultando en un bloqueo del sistema operativo Windows (BSoD)."

En respuesta a las interrupciones causadas por el bloqueo y para prevenir futuros incidentes, la empresa con sede en Texas dijo que ha mejorado sus procesos de prueba y ha reforzado su mecanismo de manejo de errores en el Intérprete de Contenido. También planea implementar una estrategia de despliegue escalonado para el Contenido de Respuesta Rápida.

LA FIRMA DE CIBERSEGURIDAD CROWDSTRIKE EXPLICÓ QUE UN PROBLEMA EN SU SISTEMA DE VALIDACIÓN FUE LA CAUSA DE QUE MILLONES DE DISPOSITIVOS CON WINDOWS SE BLOQUEARAN DURANTE UNA INTERRUPCIÓN GENERALIZADA A FINALES DE LA SEMANA PASADA.

The Hacker News. (s. f.-a). CrowdStrike Explains Friday Incident Crashing Millions of Windows Devices. https://thehackernews.com/2024/07/crowdstrike-explains-friday-windows.html

AT&T CONFIRMA BRECHA DE DATOS QUE AFECTA A CASI TODOS LOS CLIENTES DE TELEFONÍA MÓVIL

EL PROVEEDOR DE TELECOMUNICACIONES ESTADOUNIDENSE AT&T HA CONFIRMADO QUE LOS ACTORES DE AMENAZAS LOGRARON ACCEDER A DATOS PERTENECIENTES A "CASI TODOS" SUS CLIENTES DE TELEFONÍA MÓVIL, ASÍ COMO A CLIENTES DE OPERADORES DE RED VIRTUAL MÓVIL (MVNO) QUE UTILIZAN LA RED INALÁMBRICA DE AT&T.

"AT&T ha confirmado que actores maliciosos accedieron de manera ilegal a un espacio de trabajo de AT&T en una plataforma de nube de terceros y, entre el 14 de abril y el 25 de abril de 2024, exfiltraron archivos que contenían registros de interacciones de llamadas y mensajes de texto de clientes de AT&T que ocurrieron aproximadamente entre el 1 de mayo y el 31 de octubre de 2022, así como el 2 de enero de 2023," indicó la empresa.

Estos registros incluyen números de teléfono con los que interactuaron los números inalámbricos de AT&T o de MVNO, incluyendo números de clientes de línea fija de AT&T y de otros operadores, el número de esas interacciones y la duración total de las llamadas para un día o mes.

Un subconjunto de estos registros también contenía uno o más números de identificación de sitios de celdas, lo que podría haber permitido a los atacantes triangulizar la ubicación aproximada de un cliente al realizar una llamada o enviar un mensaje de texto. AT&T dijo que alertará a los clientes actuales y anteriores si su información se vio involucrada.

Ciberseguridad

"Los actores de amenazas han utilizado datos de compromisos anteriores para vincular números de teléfono con identidades," comentó Jake Williams, ex hacker de la NSA y miembro de la facultad en IANS Research. "Lo que los atacantes robaron aquí son efectivamente registros de datos de llamadas (CDR), que son un tesoro en el análisis de inteligencia porque pueden usarse para entender quién está hablando con quién — y cuándo."

La lista de MVNO de AT&T incluye Black Wireless, Boost Infinite, Consumer Cellular, Cricket Wireless, FreedomPop, FreeUp Mobile, Good2Go, H2O Wireless, PureTalk, Red Pocket, Straight Talk Wireless, TracFone Wireless, Unreal Mobile y Wing.

AT&T CONFIRMA BRECHA DE DATOS QUE AFECTA A CASI TODOS LOS CLIENTES DE TELEFONÍA MÓVIL

El nombre del proveedor de nube de terceros no fue revelado por AT&T, pero Snowflake ha confirmado que la brecha está vinculada al hack que ha afectado a otros clientes, como Ticketmaster, Santander, Neiman Marcus y LendingTree, según Bloomberg.

La empresa indicó que se enteró del incidente el 19 de abril de 2024 y activó inmediatamente sus esfuerzos de respuesta. Además, señaló que está colaborando con las fuerzas del orden en sus esfuerzos para arrestar a los implicados, y que "al menos una persona ha sido detenida."

404 Media informó que un ciudadano estadounidense de 24 años, llamado John Binns, que fue arrestado previamente en Turquía en mayo de 2024, está relacionado con el evento de seguridad, citando a tres fuentes no reveladas. Binns también fue acusado en EE.UU. por infiltrarse en T-Mobile en 2021 y vender sus datos de clientes.

Sin embargo, AT&T enfatizó que la información accedida no incluye el contenido de llamadas o mensajes de texto, información personal como números de Seguro Social, fechas de nacimiento u otra información identificable.

"Si bien los datos no incluyen nombres de clientes, a menudo hay maneras, usando herramientas en línea disponibles públicamente, de encontrar el nombre asociado con un número de teléfono específico," dijo en un informe presentado a la Comisión de Bolsa y Valores de EE.UU. (SEC).

También está instando a los usuarios a estar atentos a phishing, smishing y fraudes en línea, y a solo abrir mensajes de texto de remitentes confiables. Además, los clientes pueden solicitar obtener los números de teléfono de sus llamadas y mensajes de texto en los datos descargados ilegalmente.

La campaña de cibercrimen malicioso que afecta a Snowflake ha puesto en el punto de mira a hasta 165 clientes, con Mandiant, propiedad de Google, atribuyendo la actividad a un actor de amenazas motivado financieramente denominado UNC5537, que incluye "miembros basados en América del Norte y colabora con un miembro adicional en Turquía."

Los criminales han exigido pagos de entre $300,000 y $5 millones a cambio de los datos robados. El último desarrollo muestra que las repercusiones del ataque cibernético se están expandiendo y han tenido un efecto en cascada.

WIRED reveló el mes pasado cómo los hackers detrás de los robos de datos y ataques de extorsión obtuvieron credenciales de Snowflake robadas de servicios de la dark web que venden acceso a nombres de usuario, contraseñas y tokens de autenticación capturados por malware ladrón. Esto incluyó el acceso a través de un contratista externo llamado EPAM Systems.

Por su parte, Snowflake anunció esta semana que los administradores ahora pueden exigir autenticación multifactor obligatoria (MFA) para todos los usuarios para mitigar el riesgo de toma de control de cuentas. También dijo que pronto requerirá MFA para todos los usuarios en cuentas de Snowflake recién creadas.

The Hacker News. (s. f.-a). AT&T confirms data breach affecting nearly all wireless customers. https://thehackernews.com/2024/07/at-confirms-data-breach-affecting.html

HACKERS CHINOS EXPLOTAN VULNERABILIDAD ZERO-DAY EN SWITCHES DE CISCO PARA DISTRIBUIR MALWARE

La vulnerabilidad, identificada como CVE-2024-20399 (con una puntuación CVSS de 6.0), se refiere a un caso de inyección de comandos que permite a un atacante local y autenticado ejecutar comandos arbitrarios como root en el sistema operativo subyacente de un dispositivo afectado.

"Al explotar esta vulnerabilidad, Velvet Ant ejecutó con éxito un malware personalizado previamente desconocido que permitió al grupo de amenazas conectarse de manera remota a los dispositivos Cisco Nexus comprometidos, cargar archivos adicionales y ejecutar código en los dispositivos," indicó la firma de ciberseguridad Sygnia en una declaración compartida con The Hacker News.

Cisco explicó que el problema se origina en la validación insuficiente de los argumentos que se pasan a ciertos comandos CLI de configuración, los cuales pueden ser explotados por un adversario incluyendo entradas manipuladas como argumentos de un comando CLI afectado.

Además, esta vulnerabilidad permite a un usuario con privilegios de administrador ejecutar comandos sin que se generen mensajes en el syslog del sistema, lo que facilita la ocultación de la ejecución de comandos en dispositivos comprometidos.

A pesar de que la vulnerabilidad permite la ejecución de código, su menor gravedad se debe a que la explotación exitosa requiere que el atacante ya posea credenciales de administrador y tenga acceso a comandos de configuración específicos. Los dispositivos afectados por CVE-2024-20399 incluyen:

- Switches Multicapa Serie MDS 9000
- Switches Serie Nexus 3000
- Switches Plataforma Nexus 5500
- Switches Plataforma Nexus 5600
- Switches Serie Nexus 6000
- Switches Serie Nexus 7000
- Switches Serie Nexus 9000 en modo standalone NX-OS

UN GRUPO DE CIBERESPIONAJE CON NEXOS EN CHINA, CONOCIDO COMO VELVET ANT, HA SIDO OBSERVADO EXPLOTANDO UNA VULNERABILIDAD DE DÍA CERO EN EL SOFTWARE CISCO NX-OS UTILIZADO EN SUS SWITCHES PARA DISTRIBUIR MALWARE.

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

HACKERS CHINOS EXPLOTAN VULNERABILIDAD ZERO-DAY EN SWITCHES DE CISCO PARA DISTRIBUIR MALWARE

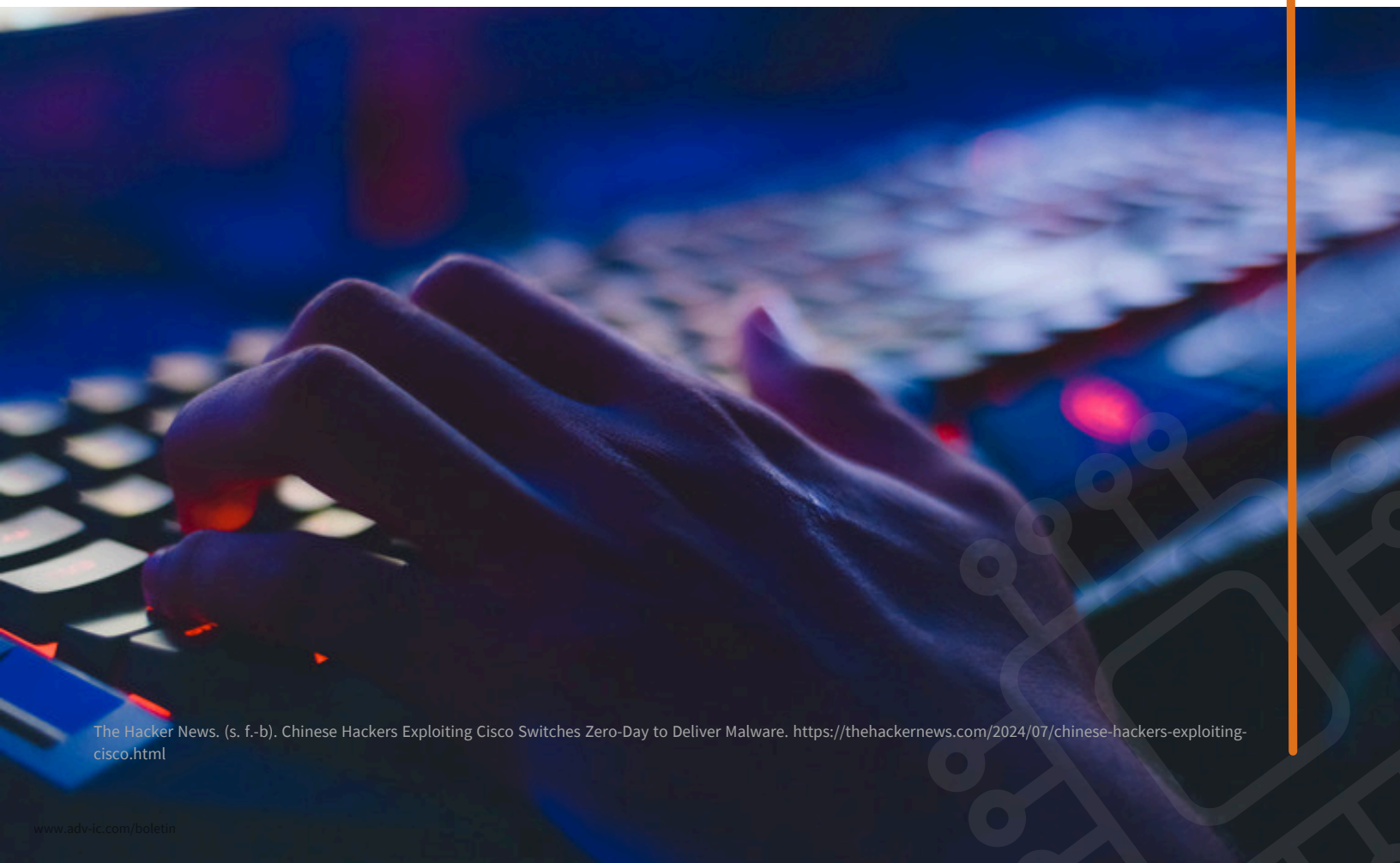
Sygnia descubrió la explotación en el mundo real de CVE-2024-20399 durante una investigación forense más amplia que ocurrió durante el año pasado. Cisco, sin embargo, indicó que se dio cuenta de intentos de explotación de la vulnerabilidad en abril de 2024.

Velvet Ant fue documentado por primera vez el mes pasado por la firma de ciberseguridad israelí en conexión con un ataque cibernético dirigido a una organización no revelada ubicada en Asia Oriental durante un período de aproximadamente tres años, estableciendo persistencia mediante el uso de dispositivos obsoletos F5 BIG-IP para robar información de clientes y financiera de manera sigilosa.

"Los dispositivos de red, particularmente los switches, a menudo no son monitoreados y sus registros no se envían con frecuencia a un sistema de registro centralizado," dijo Sygnia. "Esta falta de monitoreo crea desafíos significativos para identificar e investigar actividades maliciosas."

Este desarrollo ocurre en paralelo con la explotación de una vulnerabilidad crítica que afecta a routers Wi-Fi D-Link DIR-859 (CVE-2024-0769, con una puntuación CVSS de 9.8) – un problema de traversal de ruta que conduce a la divulgación de información – para recolectar información de cuentas como nombres, contraseñas, grupos y descripciones de todos los usuarios.

"Las variaciones del exploit [...] permiten la extracción de detalles de cuentas desde el dispositivo," comentó la firma de inteligencia de amenazas GreyNoise. "El producto está en su fin de vida, por lo que no se parcheará, lo que representa riesgos de explotación a largo plazo. Múltiples archivos XML pueden ser invocados utilizando la vulnerabilidad."



The Hacker News. (s. f.-b). Chinese Hackers Exploiting Cisco Switches Zero-Day to Deliver Malware. https://thehackernews.com/2024/07/chinese-hackers-exploiting-cisco.html

NOTICIAS NACIONALES

BBVA TENDRÁ UN CENTRO DE CIBERSEGURIDAD EN MÉXICO

EL LUNES 22DE JUNIO, BBVA REVELÓ UNA NUEVA ASOCIACIÓN CON LA EMPRESA TELEFÓNICA TECH PARA POTENCIAR LA CIBERSEGURIDAD A NIVEL GLOBAL.

El acuerdo contempla la creación de un centro especializado en ciberseguridad en México, que estará en funcionamiento completo durante el mes de julio.

Este nuevo centro actuará como una extensión del Centro Global de Ciberseguridad de BBVA en España, permitiendo así una cobertura continua y completa para todo el grupo.

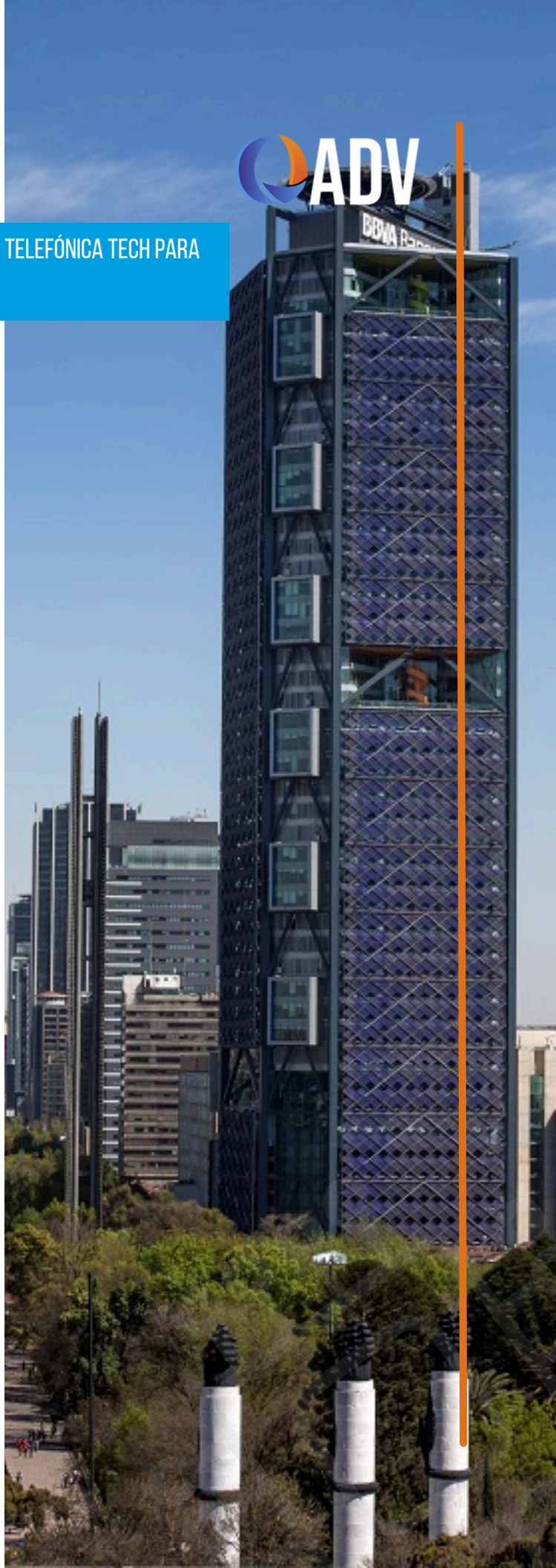
“Los dos centros contarán con cerca de 200 expertos en ciberseguridad de Telefónica Tech, quienes colaborarán estrechamente con el equipo de BBVA para ofrecer un servicio global y complementario. Esto permitirá formar uno de los centros de ciberseguridad más grandes en el sector financiero,” explicó la entidad bancaria.

Según el último Reporte de Estabilidad Financiera del Banco de México (Banxico), los riesgos cibernéticos siguen siendo una preocupación significativa a nivel global debido al incremento en la frecuencia y sofisticación de los ciberataques, los cuales se estima que se han duplicado desde antes de la pandemia de Covid-19.

Hasta el primer semestre de 2023, el informe menciona que las instituciones financieras en México reportaron dos incidentes cibernéticos importantes: uno afectó a una sociedad financiera popular (sofipo) y otro a un banco.

En relación con la alianza, Sergio Fidalgo, responsable global de ciberseguridad en BBVA, destacó que estos dos centros especializados son únicos en la industria financiera y representan un avance importante en la protección de las infraestructuras con las tecnologías más recientes.

“Queremos convertirnos en un banco cada vez más seguro y capaz de enfrentar cualquier tipo de ataque, ofreciendo a nuestros clientes el máximo nivel de seguridad del mercado,” afirmó.



BBVA TENDRÁ UN CENTRO DE CIBERSEGURIDAD EN MÉXICO

Integración de Tecnologías Avanzadas

BBVA explicó que la colaboración con Telefónica Tech permitirá la incorporación de las tecnologías más avanzadas en inteligencia artificial y automatización de procesos para prevenir ciberamenazas.

El banco integrará los últimos desarrollos de Telefónica Tech, aprovechando su experiencia global y las capacidades de la inteligencia artificial para detectar, identificar y responder a posibles amenazas, así como para monitorear la actividad de los ciberatacantes.

Telefónica Tech ofrecerá cerca de 50 servicios destinados a proporcionar una respuesta integral de seguridad para cada aspecto operativo y de negocio del banco. Estos servicios incluyen soluciones para anticipar amenazas de manera proactiva, definir prácticas operativas, reforzar la resiliencia de BBVA y proteger los Centros de Procesamiento de Datos.

“Con esta evolución en las operaciones de ciberseguridad, BBVA avanza en su proceso de transformación digital, adoptando las tecnologías más avanzadas en inteligencia artificial y automatización de procesos junto con Telefónica Tech, para mejorar la protección de los clientes digitales en los más de 25 países donde el banco opera,” concluyó.

El Economista. (2024, 22 de julio). BBVA tendrá un centro de ciberseguridad en México. El Economista. https://www.eleconomista.com.mx/sectorfinanciero/BBVA-tendra-un-centro-de-ciberseguridad-en-Mexico-20240722-0074.html

ROBO AL GOBIERNO DE MÉXICO DE DATOS CONFIDENCIALES SE DISPARÓ 81% EN 2024: SILIKN

DURANTE LOS PRIMEROS SIETE MESES DE 2024, SE REGISTRÓ UN AUMENTO DEL 81% EN EL ROBO DE INFORMACIÓN CONFIDENCIAL Y RESERVADA EN DEPENDENCIAS GUBERNAMENTALES EN MÉXICO, SEGÚN UN ESTUDIO DE SILIKN, UNA FIRMA ESPECIALIZADA EN CIBERSEGURIDAD.

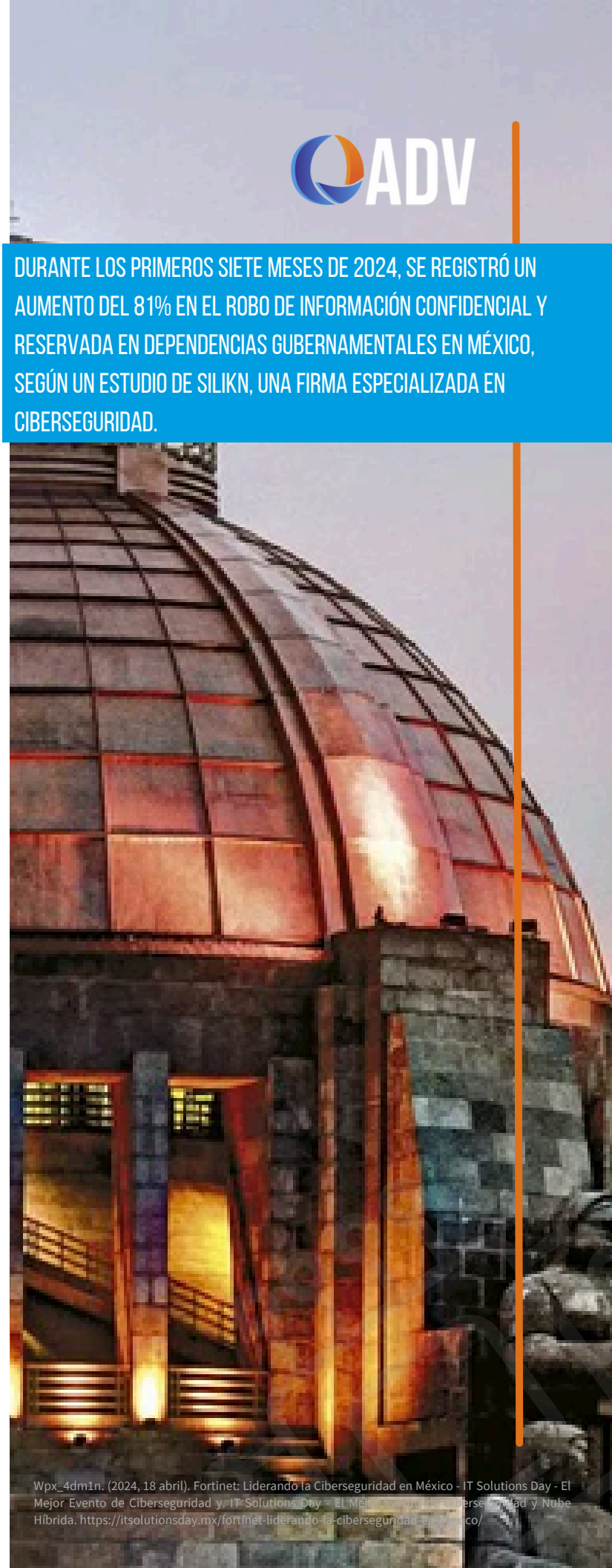
El análisis, presentado por Víctor Ruiz, fundador de SILIKN, revela que el costo promedio de una filtración de datos en este año alcanzó los $92 millones de pesos, lo que representa un incremento del 20.5% en comparación con 2023.

SILIKN también destacó que el 80.3% de las dependencias afectadas reportaron interrupciones significativas o muy significativas debido a estas filtraciones, subrayando el impacto económico y operativo de estos incidentes.

La advertencia se basa en casos ampliamente divulgados, aunque muchos otros no se conocen públicamente. Entre las instituciones afectadas se encuentran el Gobierno de la Ciudad de México (con los llamados “Chilango Leaks”), el Servicio de Administración Tributaria y la Secretaría de Seguridad y Protección Ciudadana de Oaxaca.

También se han registrado ataques en entidades como el Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas de la UNAM, el Órgano de Fiscalización Superior del estado de Veracruz (ORFIS), el Sistema de Acreditación de Prensa de la Presidencia, el Sistema Integral Informático de la Dirección de Fortalecimiento Institucional de la Secretaría de Educación Pública, la Dirección General de Bibliotecas de la Secretaría de Cultura, el Municipio de Matamoros, Coahuila; la Secretaría de Seguridad de Hidalgo (C5i) y la alcaldía Miguel Hidalgo de la CDMX, entre otros.

Víctor Ruiz señaló que la falta de medidas de seguridad ha expuesto a las instituciones gubernamentales a ataques cibernéticos, poniendo en riesgo la información personal de los ciudadanos.



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/

ROBO AL GOBIERNO DE MÉXICO DE DATOS CONFIDENCIALES SE DISPARÓ 81% EN 2024: SILIKN

Recuperación costosa y prolongada

El estudio de SILIKN indica que la recuperación total tras una filtración de datos puede tomar más de 145 días para la mayoría de las dependencias afectadas. Muchas filtraciones involucraron datos en múltiples entornos, y el 39.6% incluyó datos ocultos, dificultando aún más la identificación y contención de los ataques.
El aumento en los costos asociados con las filtraciones de datos se debe principalmente a la pérdida de información confidencial y a los costos de respuesta hacia la ciudadanía. La prolongada duración de estas filtraciones también contribuye al incremento de los costos, exacerbando las dificultades financieras y operativas de las dependencias gubernamentales.

Robo de credenciales como vector común

Víctor Ruiz también destacó que el robo o compromiso de credenciales representa el 64.6% de los incidentes, lo que pone en riesgo la seguridad de las plataformas digitales gubernamentales y los datos de los ciudadanos. Un ejemplo es el caso de “Llave CDMX”, donde se filtraron miles de accesos a la plataforma digital del gobierno capitalino, llevando a la implementación de autenticación de doble factor para reforzar la seguridad.

Deficiencias en la protección gubernamental

El estudio también subraya la falta de implementación de buenas prácticas en el gobierno de México, la ausencia de planes de respuesta a incidentes, y la falta de actualizaciones y parches de seguridad como factores clave que han facilitado el acceso de ciberatacantes a los sistemas gubernamentales.

Víctor Ruiz advirtió que la gestión inadecuada de la seguridad de los datos, el control deficiente de accesos y permisos de usuarios, y la falta de identificación y resolución de vulnerabilidades han dejado a las dependencias gubernamentales extremadamente vulnerables.

Villaseñor, I. G. (2024, 31 julio). Robo al gobierno de México de datos confidenciales se disparó 81% en 2024: SILIKN. Publimetro México. https://www.publimetro.com.mx/noticias/2024/07/31/robo-al-gobierno-de-mexico-de-datos-confidenciales-se-disparo-81-en-2024-silikn/

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

CAÍDA DE MICROSOFT 'CORTA LAS ALAS' DE AEROPUERTOS: ¿QUÉ AEROLÍNEAS CANCELARON VUELOS EN MÉXICO?

Una falla a nivel mundial en los sistemas operativos de Microsoft ha causado severas interrupciones en la industria aérea, afectando especialmente a México este viernes. A las 7:30 horas, varias aerolíneas que operan en el Aeropuerto Internacional de la Ciudad de México (AICM) cancelaron al menos seis vuelos debido a problemas informáticos relacionados con la ciberseguridad de Windows.

Cancelaciones y Retrasos en Aerolíneas

Viva Aerobus informó que se vio obligada a cancelar vuelos internacionales programados para el 19 de julio debido a la caída de sistemas. La aerolínea ha suspendido cuatro vuelos con destino a Estados Unidos, incluyendo Nueva York, Florida y Los Ángeles. Las reservas se devolverán una vez que los sistemas se reinicien. La falla también afecta los procesos de documentación para vuelos nacionales, por lo que se recomienda a los pasajeros llegar con mayor anticipación.

United Airlines también reportó la suspensión de vuelos hacia San Francisco debido a intermitencias en sus sistemas. El AICM instó a los pasajeros a contactar a sus aerolíneas para obtener información actualizada sobre el estado de sus vuelos.

Impacto en Otros Aeropuertos

La falla también ha tenido repercusiones en otros aeropuertos en México. El Aeropuerto Internacional de Monterrey reporta largas filas y retrasos debido a la caída global de Microsoft. Ricardo Dueñas, director general de OMA Aeropuertos, recomendó a los pasajeros llegar temprano y mantener comunicación con sus aerolíneas.

En el Aeropuerto Internacional de Cancún, se cancelaron 24 vuelos y se produjeron demoras en 99 más. Los vuelos afectados incluyen llegadas y salidas de aerolíneas como Viva Aerobus, United, Spirit, y Aeroméxico. La gobernadora Mara Lezama señaló que los aeropuertos en Chetumal, Tulum y Cozumel no presentan afectaciones.

Problemas en Otros Aeropuertos y Sistemas de Reservaciones

En el Aeropuerto Internacional de Veracruz, los retrasos afectan a vuelos de Viva Aerobus, Aeroméxico y United. Los pasajeros han expresado molestias por la falta de compensación por parte de las aerolíneas. El Aeropuerto Internacional de La Paz reporta demoras en vuelos con VivaAerobus y Volaris, mientras que en el Aeropuerto Internacional de San José del Cabo, se observan retrasos en vuelos de American Airlines, Southwest y United Airlines.

CAÍDA DE MICROSOFT ‘CORTA LAS ALAS’ DE AEROPUERTOS: ¿QUÉ AEROLÍNEAS CANCELARON VUELOS EN MÉXICO?

Falla en Sistemas de Microsoft y Causas

La falla se debió a un error en una actualización del software de CrowdStrike, una empresa de ciberseguridad, que provocó la caída de miles de servidores de Microsoft. Este problema ha impactado a empresas de diversos sectores a nivel global, incluyendo el aéreo, financiero, energético y de medios de comunicación. CrowdStrike ha comenzado a implementar medidas de mitigación para restaurar la normalidad en los servicios.

Munguía, A. (2024, 19 julio). Caída de Microsoft ‘corta las alas’ de aeropuertos: ¿Qué aerolíneas cancelaron vuelos en México? El Financiero. https://www.elfinanciero.com.mx/empresas/2024/07/19/caida-de-microsoft-que-aerolineas-cancelan-vuelos-en-mexico-hoy-19-de-julio/

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: JULIO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-38182	31/07/2024	Vulnerabilidad de Elevación de Privilegios en Microsoft Dynamics 365 Nuevamente	CVSS v3.1: 9.0 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-38182

Descripción: Autenticación débil en Microsoft Dynamics 365 permite a un atacante no autenticado elevar privilegios a través de una red.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21181	16/07/2024	Vulnerabilidad en el producto Oracle WebLogic Server de Oracle Fusion Middleware	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-21181

Descripción: Vulnerabilidad en el producto Oracle WebLogic Server de Oracle Fusion Middleware (componente: Core). Las versiones afectadas son 12.2.1.4.0 y 14.1.1.0.0. Una vulnerabilidad fácilmente explotable permite a un atacante no autenticado con acceso a través de T3 o IIOP comprometer Oracle WebLogic Server. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de Oracle WebLogic Server.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-39736	14/07/2024	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8 y 9.1.9 es vulnerable a la inyección de encabezados HTTP	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-39736

Descripción: Debido a una validación inadecuada de la entrada por parte de los encabezados HOST. Esto podría permitir a un atacante llevar a cabo varios ataques contra el sistema vulnerable, incluidos el secuestro de sesión, el envenenamiento de caché o el scripting entre sitios. IBM X-Force ID: 296003.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-4879	10/07/2024	ServiceNow ha abordado una vulnerabilidad de validación de entrada que se identificó en las versiones de la plataforma Now de Vancouver y Washington DC.	CVSS v3.1: 9.3 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-4879

Descripción: Esta vulnerabilidad podría permitir a un usuario no autenticado ejecutar código de manera remota dentro del contexto de la plataforma Now. ServiceNow aplicó una actualización a las instancias alojadas y publicó la actualización para nuestros socios y clientes que gestionan sus propias instalaciones. A continuación se enumeran los parches y correcciones que abordan la vulnerabilidad. Si aún no lo ha hecho, recomendamos aplicar los parches de seguridad relevantes para su instancia lo antes posible.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-38089	09/07/2024	Vulnerabilidad de Elevación de Privilegios en Microsoft Defender for IoT	CVSS v3.1: 9.9 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-38089

Descripción: La vulnerabilidad en Microsoft Defender for IoT permite a un atacante elevar privilegios. Esta vulnerabilidad podría comprometer la seguridad de los dispositivos y sistemas protegidos por Microsoft Defender for IoT, potencialmente otorgando acceso no autorizado a funcionalidades o datos sensibles.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-38077	09/07/2024	Vulnerabilidad de Ejecución Remota de Código en el Servicio de Licencias de Escritorio Remoto de Windows	CVSS v3.1: 9.8 [Critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-38077

Descripción: La vulnerabilidad en el Servicio de Licencias de Escritorio Remoto de Windows permite la ejecución remota de código. Un atacante podría explotar esta vulnerabilidad para ejecutar código arbitrario en el sistema objetivo, lo que podría comprometer la seguridad y el control del sistema afectado.

Para mitigar el riesgo, es importante aplicar las actualizaciones y parches de seguridad recomendados por Microsoft para proteger los sistemas afectados.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-37185	02/07/2024	En OpenHarmony v4.0.0 y versiones anteriores, una vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en aplicaciones preinstaladas a través de una escritura fuera de límites.	CVSS v3.1: 9.8 [Critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-37185

Descripción: Un atacante remoto puede ejecutar código en cualquier aplicación mediante esta vulnerabilidad.

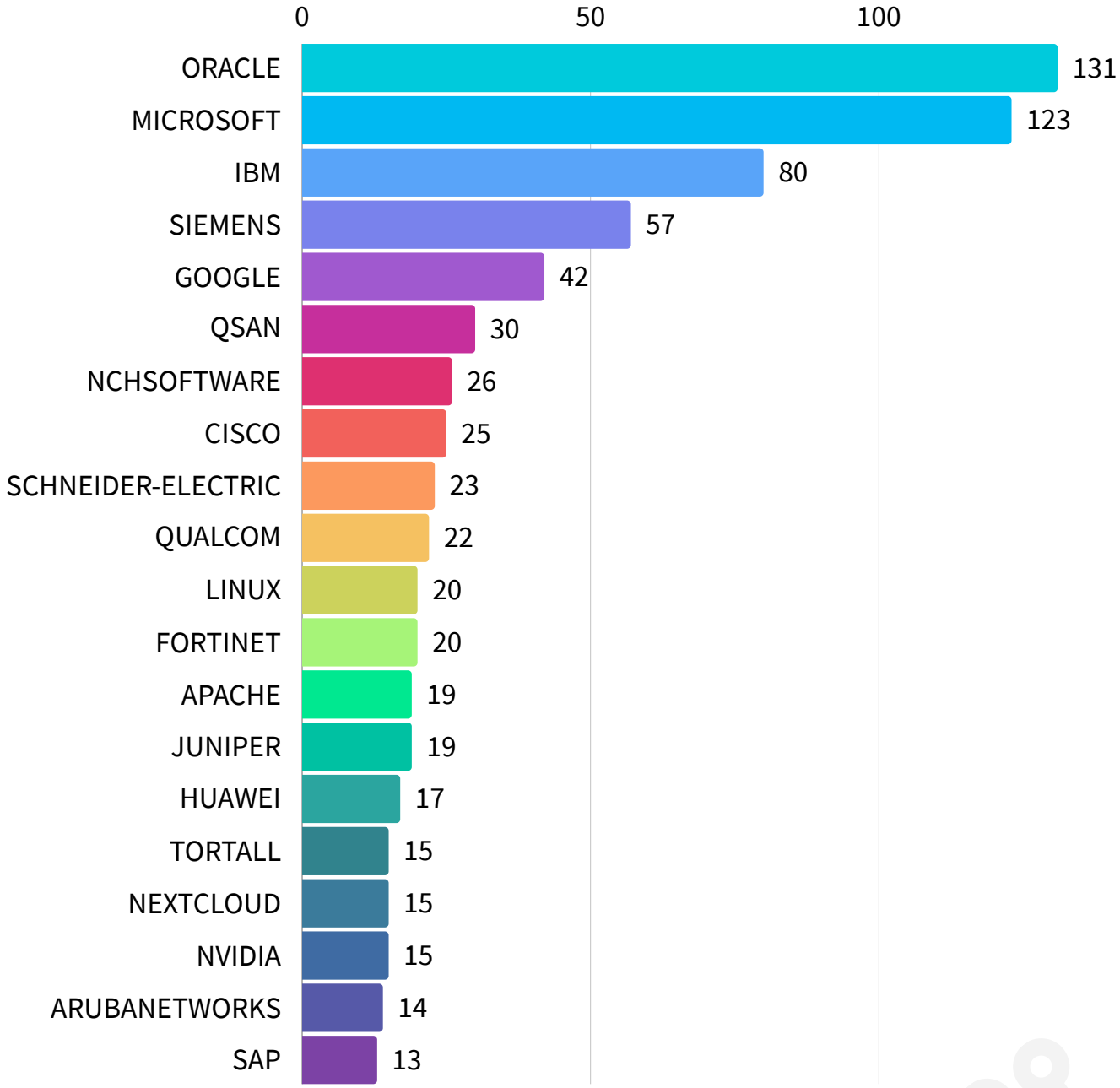
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-28751	09/07/2024	Un atacante remoto con altos privilegios puede habilitar el acceso Telnet que acepta credenciales codificadas.	CVSS v3.1: 9.1 [Critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-28751

Descripción: Vulnerabilidad de seguridad que permite a un atacante remoto con altos privilegios habilitar el acceso Telnet en un sistema, el cual acepta credenciales codificadas.

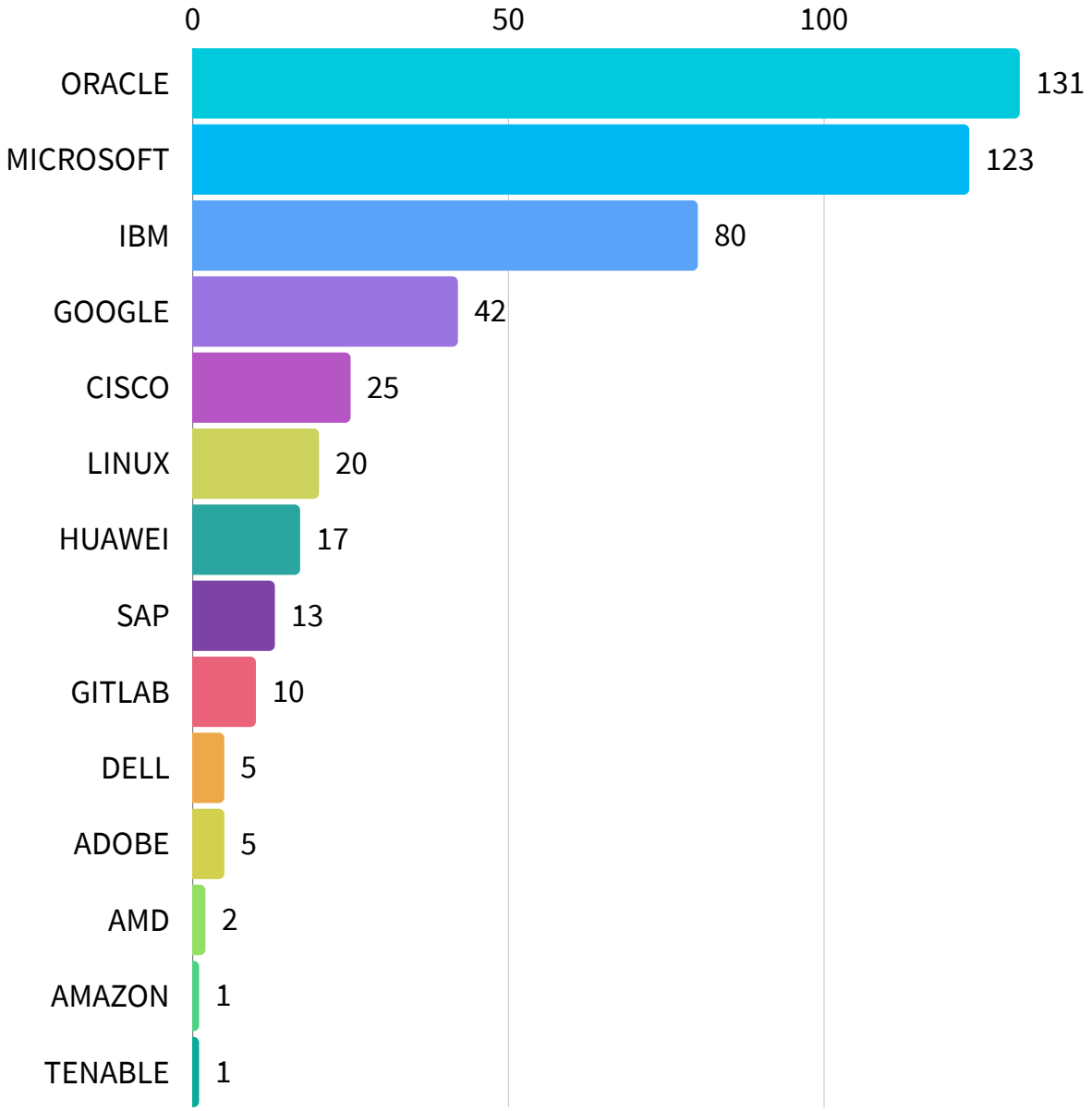
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-6365	09/07/2024	El plugin Product Table by WBW para WordPress es vulnerable a la Ejecución Remota de Código.	CVSS v3.1: 9.8 [Critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-6365

Descripción: Esto se debe a la falta de autorización y a la falta de saneamiento de los datos añadidos en el archivo languages/customTitle.php. Esto permite que atacantes no autenticados puedan ejecutar código en el servidor.

FABRICANTES CON VULNERABILIDADES RELEVANTES: JULIO DE 2024



EMPRESAS MULTINACIONALES CON VULNERABILIDADES RELEVANTES: JULIO DE 2024



CULTURA DE CIBERSEGURIDAD

SUPLANTACIÓN DEL SISTEMA DE NOMBRES DE DOMINIO (DNS)

¿QUÉ ES LA SUPLANTACIÓN DEL SISTEMA DE NOMBRES DE DOMINIO (DNS)?

La suplantación del Sistema de Nombres de Dominio (DNS), también conocida como envenenamiento de caché DNS, es un tipo de ataque cibernético donde los atacantes manipulan los registros DNS para redirigir a los usuarios hacia sitios web fraudulentos. Estos sitios maliciosos a menudo imitan sitios legítimos, engañando a los usuarios para que ingresen información sensible como credenciales de inicio de sesión. Además, estos sitios pueden instalar malware en el dispositivo del usuario, dando a los atacantes acceso prolongado a sus datos y sistemas.

¿CÓMO FUNCIONA LA SUPLANTACIÓN DE DNS?

La suplantación de DNS explota vulnerabilidades en los protocolos DNS mediante varios métodos:

- **Suplantación del Protocolo de Resolución de Direcciones (ARP):** Los atacantes utilizan la suplantación de ARP para interceptar y modificar el tráfico entre routers y dispositivos, alterando los registros de resolución de nombres de dominio.
- **Compromiso de Servidores DNS Autoritativos:** Los atacantes toman el control de servidores DNS, modificando sus registros para redirigir el tráfico hacia sitios maliciosos.
- **Explotación de la Caché DNS:** Los atacantes apuntan a servidores DNS intermedios, manipulando su caché para realizar ataques de Hombre en el Medio (MITM).

¿A QUIÉNES AFECTA LA SUPLANTACIÓN DE DNS?

La suplantación de DNS puede afectar a cualquier persona que utilice internet, incluyendo:

- **Usuarios Individuales:** Los individuos pueden ser redirigidos a sitios maliciosos donde se puede robar su información personal.
- **Empresas:** Las compañías pueden sufrir brechas de datos, pérdidas financieras y daños a su reputación si los empleados son engañados para ingresar credenciales en sitios falsos.
- **Proveedores de Servicios de Internet (ISP):** Los servidores DNS de los ISP pueden ser objetivo para redirigir a múltiples usuarios, amplificando el impacto del ataque.

¿CÓMO MITIGAR LA SUPLANTACIÓN DE DNS?

Se pueden implementar varias estrategias para mitigar la suplantación de DNS:

- **Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC):** DNSSEC proporciona autenticación de origen de datos y verificación de integridad para los datos DNS. Aunque no cifra los datos, asegura la autenticidad de las respuestas DNS.
- **Usar Servidores DNS Confiables:** Confiar en servidores DNS reputados y seguros reduce el riesgo de encontrar registros DNS suplantados.
- **Comunicación Criptográficamente Segura:** Protocolos como DNSCrypt se pueden usar para asegurar las comunicaciones con servidores DNS, asegurando que las respuestas sean auténticas y no hayan sido manipuladas.

Ehel, 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/

- **Actualizaciones Regulares del Sistema:** Mantener el software DNS y los sistemas actualizados asegura que se apliquen los últimos parches de seguridad, protegiendo contra vulnerabilidades conocidas.
- **Medidas de Seguridad en la Red:** Implementar cortafuegos de aplicaciones web (WAF), sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) puede ayudar a detectar y bloquear intentos de suplantación de DNS.
- **IPSec (Seguridad del Protocolo de Internet):** IPSec proporciona seguridad criptográfica para las comunicaciones IP, mejorando la seguridad del flujo de datos entre hosts y redes.

¿QUÉ PUEDE OFRECER UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA LA MITIGACIÓN?

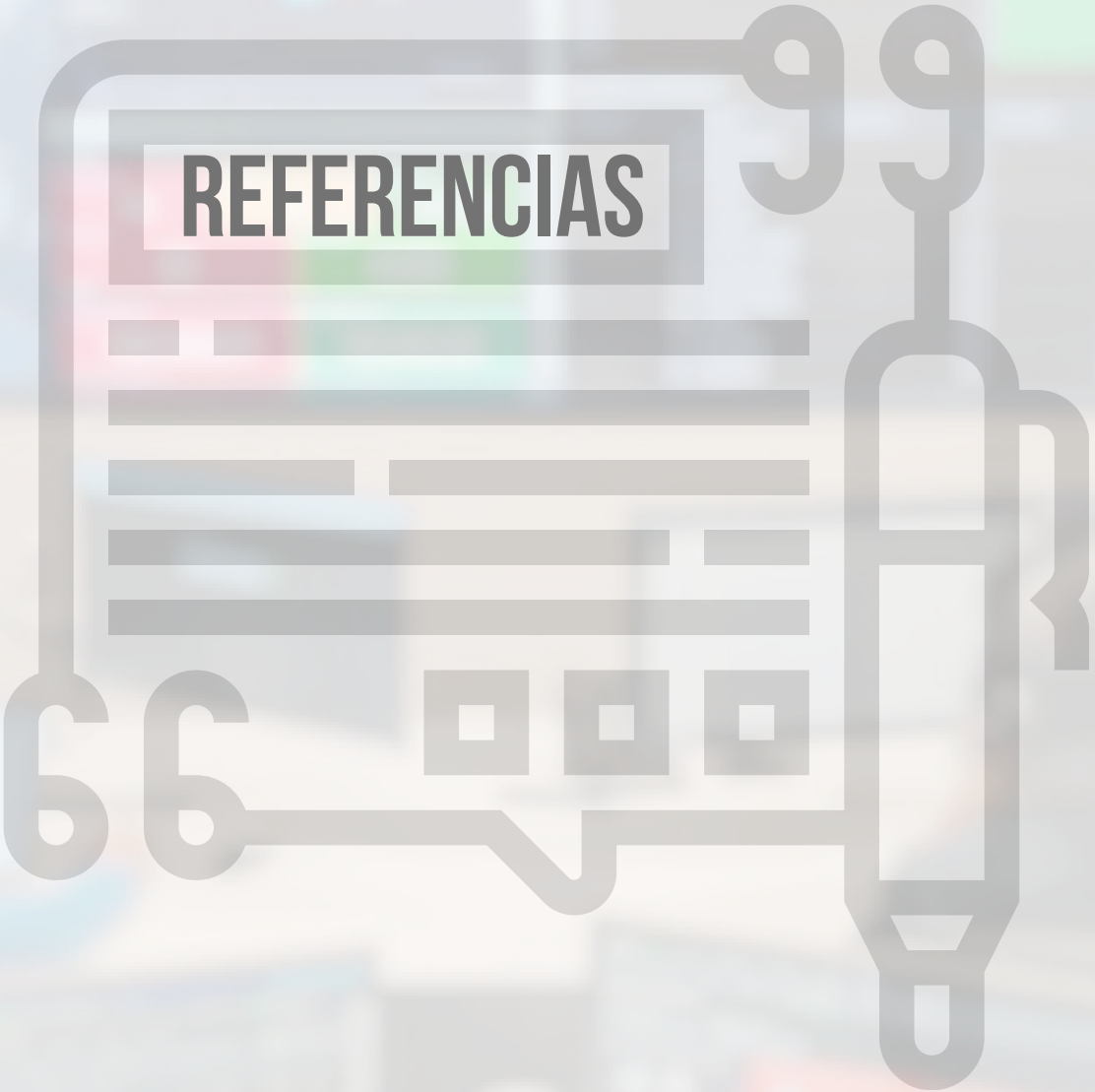
Un Centro de Operaciones de Seguridad (SOC) desempeña un papel crítico en la mitigación de la suplantación de DNS a través de:

- **Monitoreo Continuo:** Los equipos de SOC monitorean continuamente el tráfico de red en busca de signos de suplantación de DNS y otras actividades maliciosas.
- **Respuesta a Incidentes:** En caso de un ataque de suplantación de DNS, los SOC pueden responder rápidamente para contener y remediar la amenaza, minimizando su impacto.
- **Inteligencia de Amenazas:** Los SOC utilizan inteligencia de amenazas para mantenerse informados sobre nuevas técnicas de suplantación de DNS y actualizar los mecanismos de defensa en consecuencia.

Al implementar estas medidas, un SOC puede mejorar significativamente la capacidad de una organización para prevenir, detectar y responder a ataques de suplantación de DNS, protegiendo datos sensibles y manteniendo la integridad de las comunicaciones de la red.

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/

REFERENCIAS



REFERENCIAS

- The Hacker News. (s. f.). North Korea-Linked Malware Targets Developers on Windows, Linux, and macOS. https://thehackernews.com/2024/07/north-korea-linked-malware-targets.html
- The Hacker News. (s. f.-a). CrowdStrike Explains Friday Incident Crashing Millions of Windows Devices. https://thehackernews.com/2024/07/crowdstrike-explains-friday-windows.html
- The Hacker News. (s. f.-a). AT&T confirms data breach affecting nearly all wireless customers. https://thehackernews.com/2024/07/at-confirms-data-breach-affecting.html
- The Hacker News. (s. f.-b). Chinese Hackers Exploiting Cisco Switches Zero-Day to Deliver Malware. https://thehackernews.com/2024/07/chinese-hackers-exploiting-cisco.html
- El Economista. (2024, 22 de julio). BBVA tendrá un centro de ciberseguridad en México. El Economista. https://www.eleconomista.com.mx/sectorfinanciero/BBVA-tendra-un-centro-de-ciberseguridad-en-Mexico-20240722-0074.html
- Villaseñor, I. G. (2024, 31 julio). Robo al gobierno de México de datos confidenciales se disparó 81% en 2024: SILIKN. Publimetro México. https://www.publimetro.com.mx/noticias/2024/07/31/robo-al-gobierno-de-mexico-de-datos-confidenciales-se-disparo-81-en-2024-silikn/
- Munguía, A. (2024, 19 julio). Caída de Microsoft ‘corta las alas’ de aeropuertos: ¿Qué aerolíneas cancelaron vuelos en México? El Financiero. https://www.elfinanciero.com.mx/empresas/2024/07/19/caida-de-microsoft-que-aerolineas-cancelan-vuelos-en-mexico-hoy-19-de-julio/

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