BOLETÍN DE CIBERSEGURIDAD
JUNIO 2024

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

ÍNDICE

NOTICIAS INTERNACIONALES

EL NUEVO KIT DE PHISHING V3B ATACA A CLIENTES DE 54 BANCOS EUROPEOS

LOS DELINCUENTES CIBERNÉTICOS ESTÁN PROMOCIONANDO ACTIVAMENTE EN TELEGRAM UN NUEVO KIT DE PHISHING LLAMADO 'V3B'

Este “Kit” cual actualmente está dirigido a clientes de 54 instituciones financieras clave en Irlanda, Países Bajos, Finlandia, Austria, Alemania, Francia, Bélgica, Grecia, Luxemburgo e Italia.

Este kit de phishing, disponible por precios que varían entre 130 y 450 dólares al mes dependiendo de las características seleccionadas, ofrece técnicas avanzadas de ofuscación, capacidades de localización, soporte para OTP/TAN/2FA, comunicación en vivo con las víctimas y múltiples métodos de evasión.

Investigadores de Resecurity, quienes descubrieron el kit V3B, reportan que su canal en Telegram ya cuenta con más de 1.250 miembros, lo que sugiere un crecimiento rápido de esta nueva plataforma de phishing como servicio (PhaaS) en el ámbito del cibercrimen.

V3B emplea un código JavaScript altamente ofuscado sobre un CMS personalizado para eludir la detección por parte de sistemas antiphishing y motores de búsqueda, así como para protegerse de investigadores.

Además, incluye páginas traducidas profesionalmente a varios idiomas como finlandés, francés, italiano, polaco y alemán. Este enfoque mejora la efectividad de los ataques de phishing y permite a los perpetradores llevar a cabo campañas en múltiples países.

El kit, diseñado para operar en plataformas móviles y de escritorio por igual, tiene la capacidad de interceptar credenciales e información bancaria, así como detalles de tarjetas de crédito.

Además, cuenta con un panel de administración (uPanel) que permite a los estafadores interactuar en tiempo real con las víctimas a través de un sistema de chat. Esto facilita la obtención de contraseñas de un solo uso (OTP) mediante el envío de notificaciones personalizadas.
La información robada se transmite a los ciberdelincuentes a través de la API de Telegram.

EL NUEVO KIT DE PHISHING V3B ATACA A CLIENTES DE 54 BANCOS EUROPEOS

Una de las funciones de interacción en tiempo real incluye el robo de inicio de sesión mediante código QR, permitiendo a los atacantes generar códigos QR para páginas de phishing. Esto se aprovecha de la falsa sensación de legitimidad que las víctimas tienen al estar familiarizadas con servicios confiables que utilizan este método.

Otro aspecto destacado del kit V3B es su soporte para PhotoTAN y Smart ID, destinado a evadir las tecnologías de autenticación avanzadas ampliamente utilizadas por bancos en Alemania y Suiza.

Resecurity explica: "Las tecnologías utilizadas para la autenticación de clientes pueden variar entre los bancos. Sin embargo, el hecho de que los estafadores estén implementando soporte para mecanismos alternativos de validación OTP/TAN, en lugar de depender exclusivamente de métodos tradicionales basados en SMS, subraya los desafíos que enfrentan los equipos de prevención de fraude al combatir la apropiación de cuentas tanto individuales como corporativas".

Los kits de phishing son herramientas clave para los ciberdelincuentes menos expertos, permitiéndoles llevar a cabo ataques altamente perjudiciales contra clientes bancarios desprevenidos.

Recientemente, las autoridades policiales desmantelaron LabHost, una de las mayores operaciones de PhaaS dirigida principalmente a bancos en Estados Unidos y Canadá. En el operativo, 37 personas, incluido el promotor original, fueron detenidas.

Toulas, B. (2024, June 4). New V3B phishing kit targets customers of 54 European banks. BleepingComputer. https://www.bleepingcomputer.com/news/security/new-v3b-phishing-kit-targets-customers-of-54-european-banks/

MICROSOFT HA ALERTADO SOBRE UNA VULNERABILIDAD EN LAS ETIQUETAS DE SERVICIO DE AZURE QUE PODRÍA SER EXPLOTADA POR PIRATAS INFORMÁTICOS.

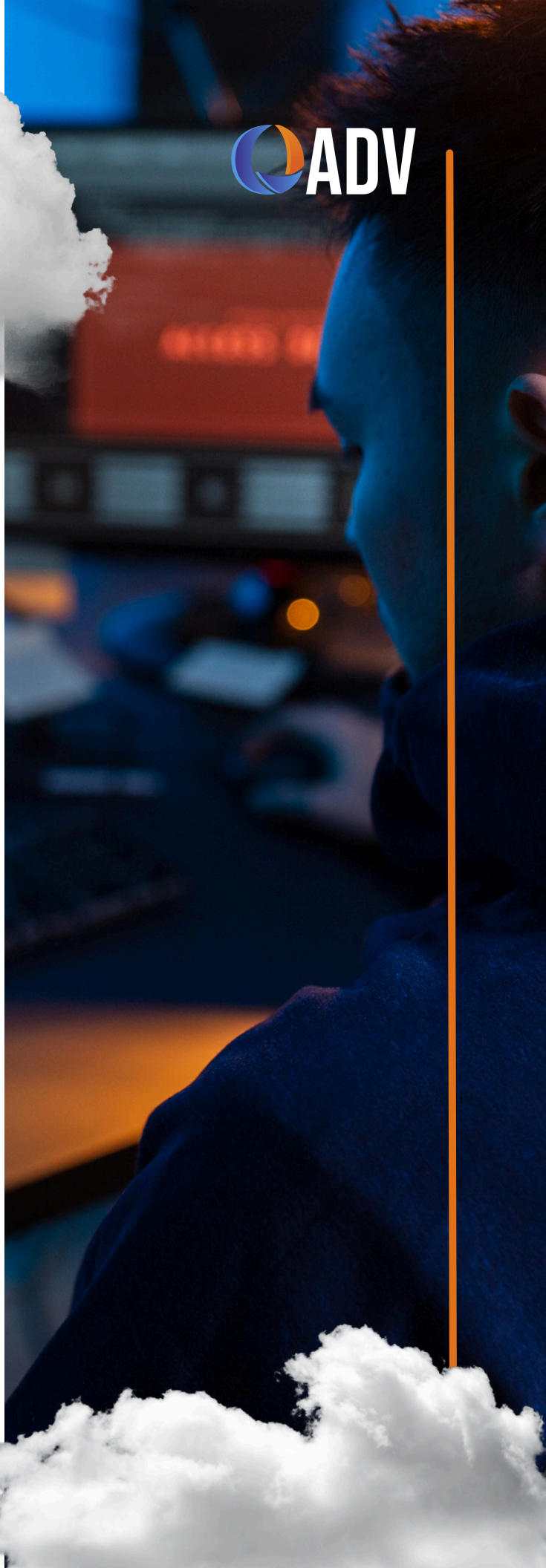
MICROSOFT HA EMITIDO UNA ADVERTENCIA SOBRE EL POTENCIAL ABUSO DE LAS ETIQUETAS DE SERVICIO DE AZURE POR PARTE DE ACTORES MALINTENCIONADOS.

Esto podría permitirles falsificar solicitudes hacia un servicio confiable y eludir las reglas del firewall, potencialmente obteniendo acceso no autorizado a recursos en la nube.

El Centro de Respuesta de Seguridad de Microsoft (MSRC) señaló que este caso subraya un riesgo inherente en depender exclusivamente de las etiquetas de servicio como método para verificar el tráfico entrante. En una guía reciente, MSRC enfatizó que las etiquetas de servicio no deben considerarse como un límite de seguridad por sí mismas, sino que deben utilizarse junto con controles de validación adicionales. Además, destacaron que las etiquetas de servicio no proporcionan una protección completa contra vulnerabilidades asociadas con solicitudes web y no sustituyen la necesidad de validar la entrada adecuadamente.

Esta advertencia resalta la importancia de implementar estrategias de seguridad robustas y multifactoriales para proteger los entornos en la nube contra posibles explotaciones y accesos no autorizados.

La declaración surge en respuesta a los hallazgos de la empresa de ciberseguridad Tenable, que reveló una vulnerabilidad en Azure donde las reglas de firewall dependientes de etiquetas de servicio podrían ser eludidas. Aunque no hay evidencia de que esta característica haya sido explotada en la práctica, el problema radica en que algunos servicios de Azure permiten el tráfico entrante basado únicamente en una etiqueta de servicio. Esto potencialmente permitiría a un atacante enviar solicitudes diseñadas específicamente para acceder a recursos en otro inquilino de Azure, asumiendo que el servicio está configurado para permitir tráfico desde esa etiqueta sin requerir autenticación adicional.



MICROSOFT HA ALERTADO SOBRE UNA VULNERABILIDAD EN LAS ETIQUETAS DE SERVICIO DE AZURE QUE PODRÍA SER EXPLOTADA POR PIRATAS INFORMÁTICOS.

Según Tenable, se identificaron 10 servicios de Azure afectados por esta vulnerabilidad, incluyendo Azure Application Insights, Azure DevOps, Azure Machine Learning, Azure Logic Apps, Azure Container Registry, Azure Load Testing, Azure API Management, Azure Data Factory, Azure Action Group, Azure AI Video Indexer y Azure Chaos Studio.

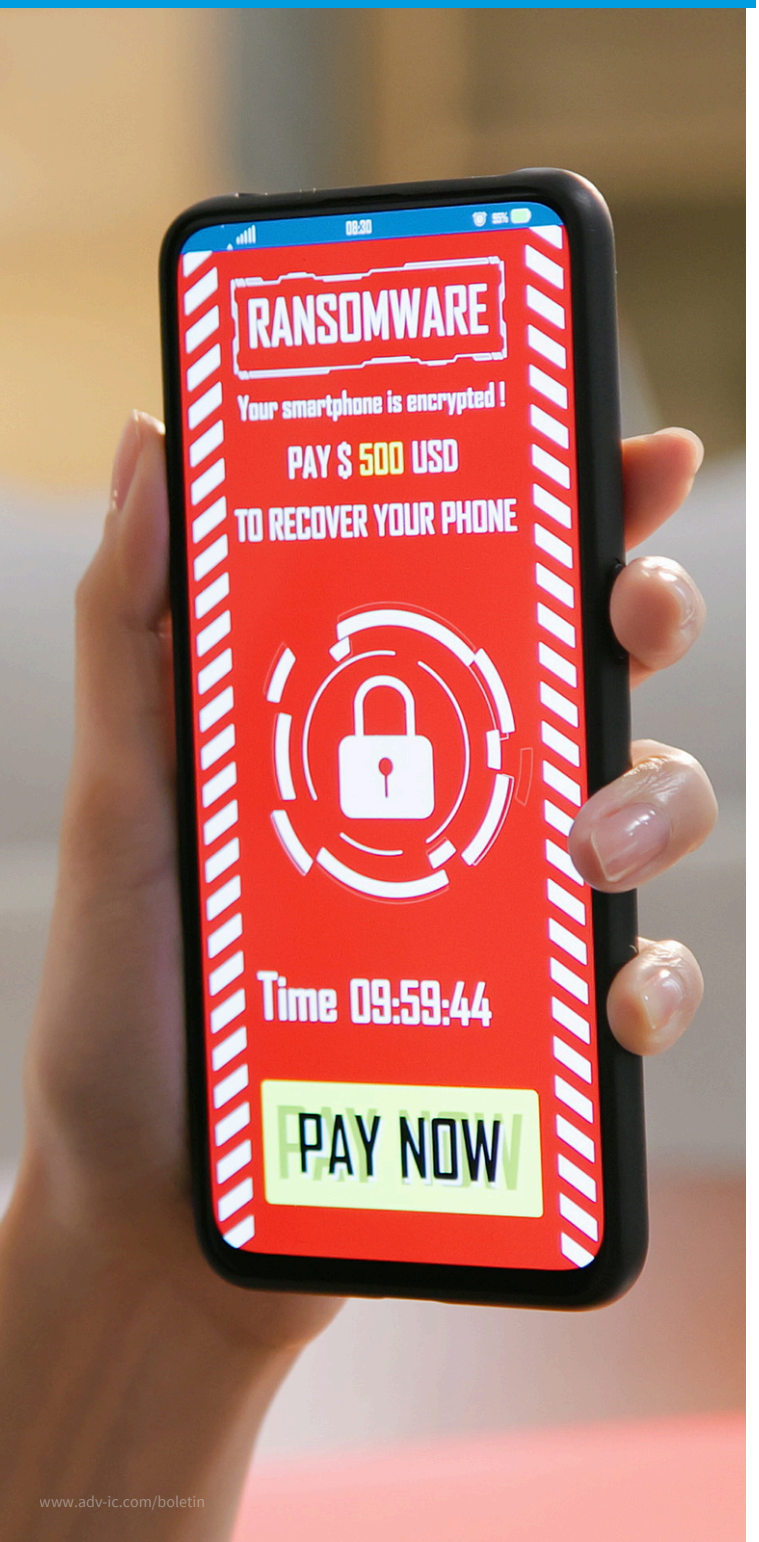
Liv Matan, investigadora de Tenable, explicó: "Esta vulnerabilidad permite a un atacante controlar solicitudes del lado del servidor, haciéndose pasar por servicios confiables de Azure. Esto les permite eludir los controles de red basados en etiquetas de servicio, que generalmente se utilizan para proteger activos, datos y servicios internos de los clientes de Azure contra acceso no autorizado".

En respuesta a estos hallazgos, Microsoft actualizó la documentación a fines de enero de 2024 para enfatizar que "las etiquetas de servicio por sí solas no son suficientes para proteger el tráfico sin considerar la naturaleza del servicio y el tráfico que envía". Se recomienda a los clientes revisar y asegurar adecuadamente el uso de etiquetas de servicio, implementando medidas de seguridad adicionales para autenticar el tráfico de red de manera confiable.

The Hacker News. (n.d.). Azure Service Tags Vulnerability: Microsoft warns of potential abuse by hackers. https://thehackernews.com/2024/06/azure-service-tags-vulnerability.html

LA FILTRACIÓN DE DATOS DE SNOWFLAKE HA EXPUESTO LA INFORMACIÓN DE 165 CLIENTES, QUIENES AHORA ESTÁN SIENDO OBJETO DE UNA CAMPAÑA DE EXTORSIÓN EN CURSO.

SE INFORMA QUE HASTA 165 CLIENTES DE SNOWFLAKE HAN TENIDO SU INFORMACIÓN POTENCIALMENTE EXPUESTA



Se informa que hasta 165 clientes de Snowflake han tenido su información potencialmente expuesta como parte de una campaña en curso destinada a facilitar el robo de datos y la extorsión. La empresa Mandiant, propiedad de Google, está ayudando a Snowflake en sus esfuerzos de respuesta ante este incidente. Mandiant está rastreando al grupo de amenazas conocido como UNC5537, descrito como un actor con motivaciones financieras.

Según Mandiant, UNC5537 está comprometiendo de manera sistemática las instancias de clientes de Snowflake utilizando credenciales robadas. El grupo está publicitando los datos de las víctimas para su venta en foros de delitos cibernéticos y tratando de extorsionar a muchas de ellas. Este grupo ha atacado a cientos de organizaciones en todo el mundo y opera bajo varios alias en canales de Telegram y foros de delitos cibernéticos.

Hay pruebas que sugieren que los miembros de UNC5537 están basados en América del Norte y se cree que colaboran con al menos otro grupo ubicado en Turquía.

Esta es la primera vez que se revela oficialmente el número de clientes afectados. Previamente, Snowflake había mencionado que un "número limitado" de sus clientes se vieron afectados por el incidente, a pesar de tener más de 9,820 clientes en todo el mundo.

La campaña, según Snowflake, se origina a partir de credenciales de clientes comprometidas que fueron adquiridas en foros de delitos cibernéticos o obtenidas a través de malware como Lumma, MetaStealer, Raccoon, RedLine, RisePro y Vidar. Se estima que esta actividad comenzó el 14 de abril de 2024.

En varios casos, se han detectado infecciones de malware en sistemas de contratistas que también se utilizaban para actividades personales, como juegos y descargas de software pirateado, siendo este último un método conocido para la distribución de malware.

LA FILTRACIÓN DE DATOS DE SNOWFLAKE HA EXPUESTO LA INFORMACIÓN DE 165 CLIENTES, QUIENES AHORA ESTÁN SIENDO OBJETO DE UNA CAMPAÑA DE EXTORSIÓN EN CURSO.

Se ha descubierto que el acceso no autorizado a las instancias de los clientes de Snowflake ha facilitado el uso de una herramienta de reconocimiento llamada FROSTBITE (también conocida como "rapeflake"), diseñada para ejecutar consultas SQL y obtener información crítica como usuarios, roles actuales, direcciones IP, IDs de sesión y nombres de organizaciones.

Mandiant ha informado que no ha podido obtener una muestra completa de FROSTBITE, pero ha destacado que el actor de amenazas también utiliza una herramienta legítima llamada DBeaver Ultimate para conectar y ejecutar consultas SQL en las instancias comprometidas de Snowflake. La fase final del ataque involucra la ejecución de comandos para preparar y extraer datos sensibles.

Snowflake, en una actualización reciente, ha afirmado que está colaborando estrechamente con sus clientes para fortalecer las medidas de seguridad. Además, está desarrollando un plan para requerir a los clientes que implementen controles avanzados de seguridad, como autenticación multifactor (MFA) y políticas de red más estrictas.

Mandiant ha señalado que estos ataques han sido exitosos debido a tres razones principales: la falta de implementación de autenticación multifactor (MFA), la falta de rotación periódica de credenciales y la falta de controles efectivos para restringir el acceso solo a ubicaciones confiables.

"La primera fecha de infección por robo de información observada asociada con una credencial aprovechada por el actor de amenazas se remonta a noviembre de 2020", declaró Mandiant, añadiendo que "se identificaron cientos de credenciales de clientes de Snowflake expuestas a través de ladrones de información desde 2020".

Esta campaña destaca las consecuencias de la circulación masiva de credenciales en el mercado de robo de información y puede reflejar un enfoque específico de los actores de amenazas hacia plataformas SaaS similares.

Los hallazgos subrayan la creciente demanda en el mercado de ladrones de información y la amenaza generalizada que representan para las organizaciones, con la continua aparición de nuevas variantes como AsukaStealer, Cuckoo, Iluria, k1w1, SamsStealer y Seidr, disponibles para la venta a otros criminales.

"En febrero, Sultan, conocido por el malware Vidar, compartió una imagen donde los ladrones Lumma y Raccoon aparecían juntos, desafiando las soluciones antivirus", según un análisis reciente de Cyfirma. "Esto sugiere una colaboración entre actores de amenazas, uniéndose y compartiendo infraestructura para alcanzar sus objetivos".

The Hacker News. (n.d.). Snowflake Breach exposes 165 customers' data in ongoing extortion campaign. https://thehackernews.com/2024/06/snowflake-breach-exposes-165-customers.html

AMD ESTÁ INVESTIGANDO UNA VIOLACIÓN DE SEGURIDAD DESPUÉS DE QUE DATOS SE PUSIERAN A LA VENTA EN UN FORO DE PIRATERÍA.

Los datos mencionados incluyen información de empleados de AMD, documentos financieros y otra información confidencial.

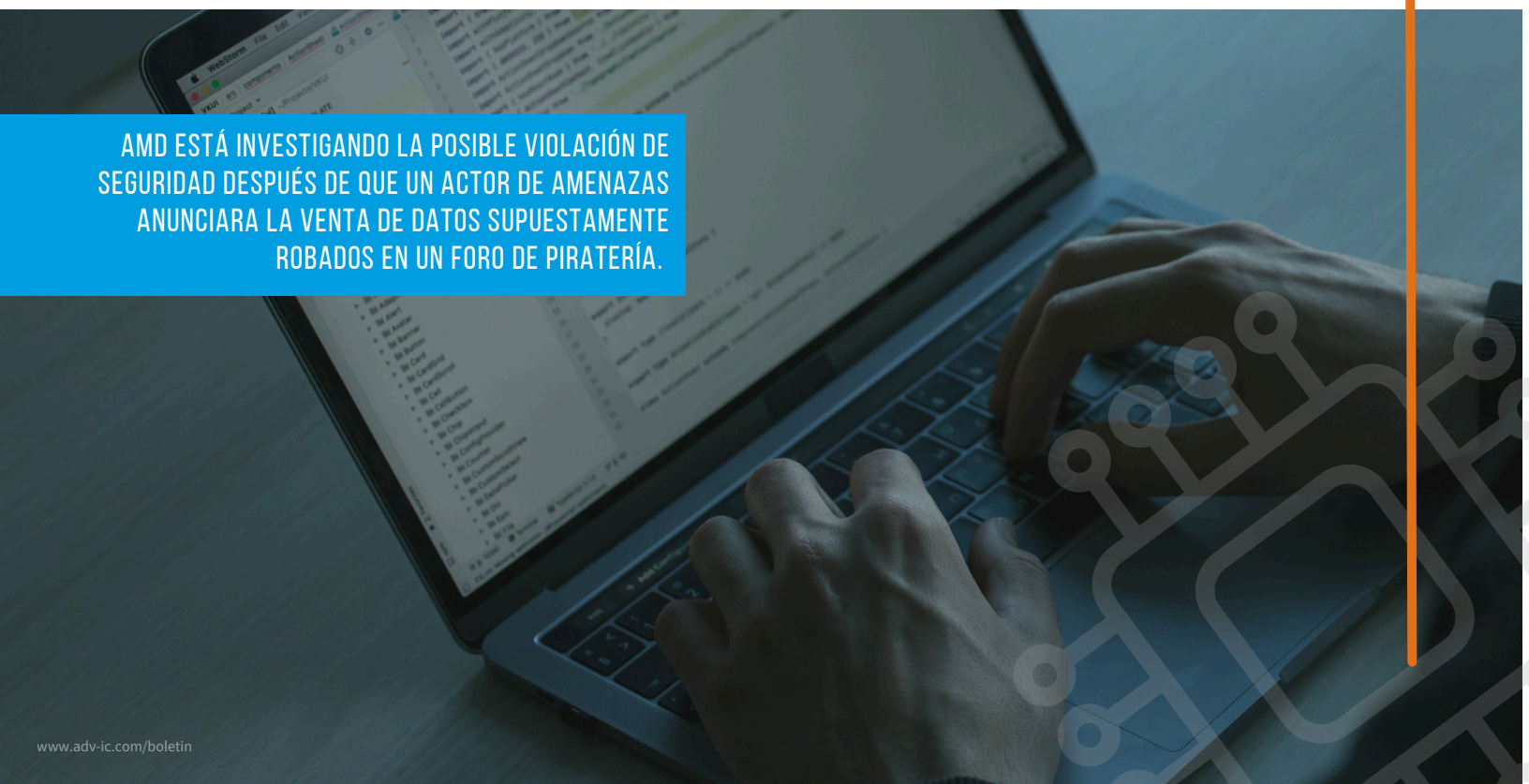
En un comunicado a BleepingComputer, AMD declaró: "Tenemos conocimiento de una organización cibercriminal que afirma estar en posesión de datos robados de AMD. Estamos trabajando estrechamente con las autoridades policiales y un proveedor externo de alojamiento para investigar esta denuncia y la naturaleza de los datos involucrados".

El actor de amenazas conocido como IntelBroker ha compartido capturas de pantalla que supuestamente muestran credenciales robadas de AMD, aunque aún no ha revelado detalles sobre el precio de venta ni cómo obtuvo los datos.

En una publicación en un foro de piratería, IntelBroker declaró: "Hoy vendo la filtración de datos de AMD.com. ¡Gracias por leer y que lo disfruten!". Además, mencionó que en junio de 2024 AMD sufrió una filtración de datos que incluye información comprometida como futuros productos, hojas de especificaciones, bases de datos de empleados y clientes, archivos de propiedad, ROM, código fuente, firmware y datos financieros.

Según informes de DarkWebInformer, el actor de amenazas afirmó que los datos incluyen una base de datos de empleados que contiene identificaciones de usuario, nombres y apellidos, roles laborales, números de teléfono comerciales, direcciones de correo electrónico y estado laboral.

AMD está investigando activamente esta situación en colaboración con las autoridades policiales y un proveedor externo de alojamiento, para determinar la veracidad y la extensión de la brecha de seguridad reportada.



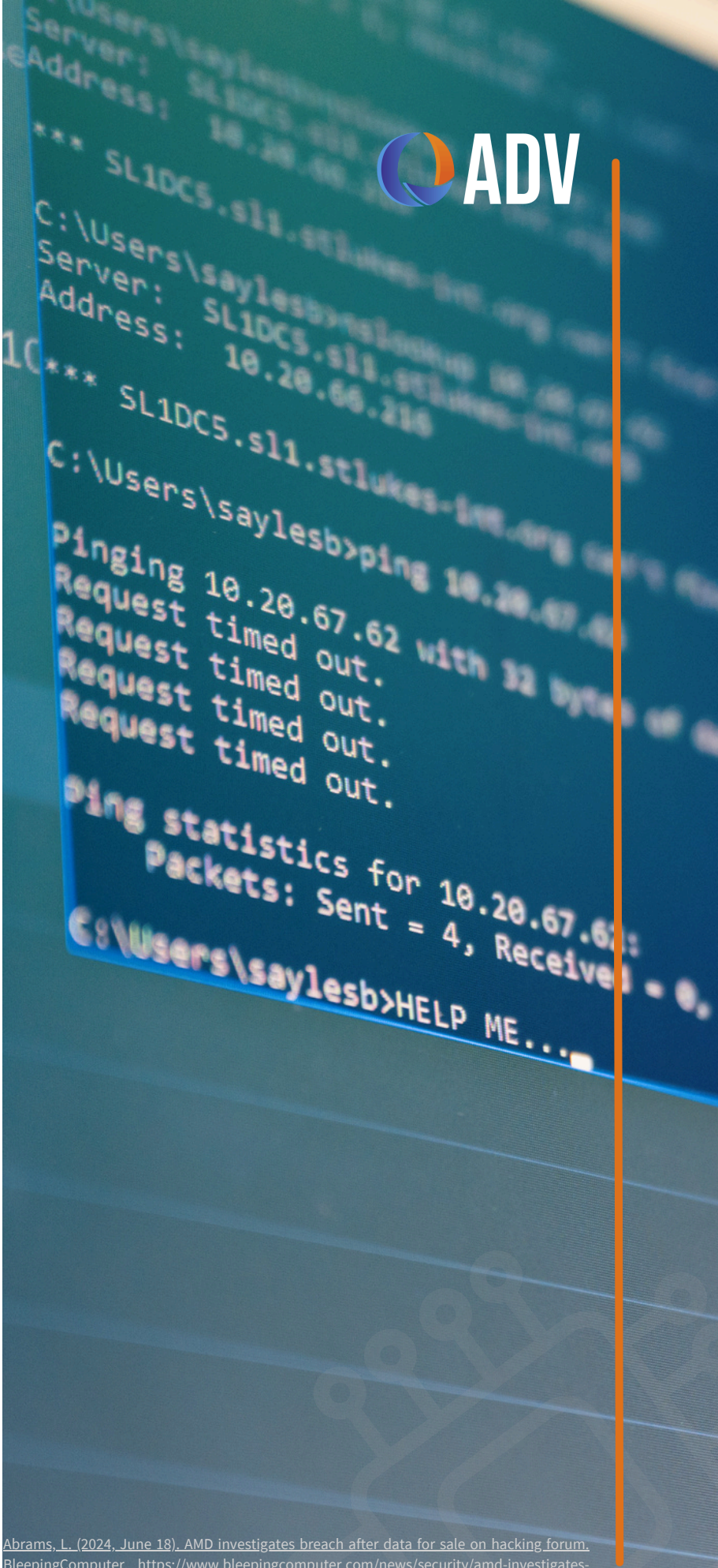
AMD ESTÁ INVESTIGANDO LA POSIBLE VIOLACIÓN DE SEGURIDAD DESPUÉS DE QUE UN ACTOR DE AMENAZAS ANUNCIARA LA VENTA DE DATOS SUPUESTAMENTE ROBADOS EN UN FORO DE PIRATERÍA.

AMD ESTÁ INVESTIGANDO UNA VIOLACIÓN DE SEGURIDAD DESPUÉS DE QUE DATOS SE PUSIERAN A LA VENTA EN UN FORO DE PIRATERÍA.

IntelBroker es conocido por haber perpetrado violaciones de seguridad significativas en el pasado. En primer lugar, fue responsable de la violación de DC Health Link, que expuso los datos personales de miembros y personal de la Cámara de Representantes de EE. UU., lo que llevó a una audiencia en el Congreso.

Más recientemente, IntelBroker estuvo involucrado en la violación de la Plataforma de Expertos de Europol (EPE), un portal utilizado por agencias internacionales de aplicación de la ley para compartir información.

En relación con AMD, en junio de 2022, la empresa investigó una violación de seguridad vinculada a la banda de extorsión RansomHouse, que afirmó haber robado 450 GB de datos de la compañía.
Estos incidentes resaltan la actividad persistente y preocupante de IntelBroker en el ámbito de la ciberdelincuencia, afectando a organizaciones de alto perfil y sus datos sensibles.



Abrams, L. (2024, June 18). AMD investigates breach after data for sale on hacking forum. BleepingComputer. https://www.bleepingcomputer.com/news/security/amd-investigates-breach-after-data-for-sale-on-hacking-forum/

EL RANSOMWARE RANSOMHUB DISEÑADO PARA SISTEMAS LINUX ESTÁ ATACANDO A LAS MÁQUINAS VIRTUALES QUE CORREN EN VMWARE ESXI.

RansomHub es una plataforma de ransomware como servicio (RaaS) que se lanzó en febrero de 2024. Ha sido asociada con superposiciones de código y colaboraciones con otros grupos como ALPHV/BlackCat y Knight ransomware. Hasta la fecha, ha afectado a más de 45 víctimas en 18 países.

La existencia de un cifrador RansomHub para sistemas operativos Windows y Linux fue confirmada a principios de mayo. Según informes de Recorded Future, el grupo de amenazas también ha desarrollado una variante especializada para VMware ESXi, detectada por primera vez en abril de 2024.

A diferencia de las versiones de RansomHub para Windows y Linux, que están programadas en Go, la versión para ESXi está escrita en C++, posiblemente derivada del ransomware Knight, que ya no está activo.

Según Recorded Future, se encontró un error simple en la variante ESXi que los defensores pueden explotar para ponerla en un bucle infinito y evitar el proceso de cifrado.

Muchas empresas, incluida la mencionada empresa, están optando por utilizar máquinas virtuales para alojar sus servidores debido a las ventajas en la gestión de recursos como CPU, memoria y almacenamiento.

Esta mayor adopción ha llevado a que casi todas las bandas de ransomware que atacan a empresas desarrollen cifradores dedicados para VMware ESXi con el objetivo específico de comprometer estos servidores.

RansomHub sigue la tendencia general entre los ransomwares dirigidos a VMware ESXi, ofreciendo un cifrador con diversas opciones de línea de comandos. Estas opciones incluyen la capacidad de establecer un retraso en la ejecución, especificar qué máquinas virtuales deben excluirse del cifrado, y definir rutas de directorio específicas, entre otras configuraciones.

Además, RansomHub incorpora comandos específicos para VMware ESXi, como 'vim-cmd vmsvc/getallvms' y 'vim-cmd vmsvc/snapshot.removeall' para la gestión de instantáneas, así como 'esxcli vm process kill' para forzar el apagado de máquinas virtuales. Estas funcionalidades permiten al ransomware manipular las operaciones del entorno de virtualización para sus fines de cifrado y control durante un ataque.

LA OPERACIÓN DEL RANSOMWARE RANSOMHUB HA DESARROLLADO UN CIFRADOR ESPECÍFICAMENTE DISEÑADO PARA CIFRAR ENTORNOS VMWARE ESXI EN ATAQUES DIRIGIDOS A EMPRESAS.

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

EL RANSOMWARE RANSOMHUB DISEÑADO PARA SISTEMAS LINUX ESTÁ ATACANDO A LAS MÁQUINAS VIRTUALES QUE CORREN EN VMWARE ESXI.

El cifrador de RansomHub también incluye funcionalidades para desactivar servicios críticos como syslog, lo cual dificulta el registro de actividad durante el ataque. Además, puede configurarse para eliminar todos sus rastros después de la ejecución, lo que ayuda a evitar la detección y el análisis forense.

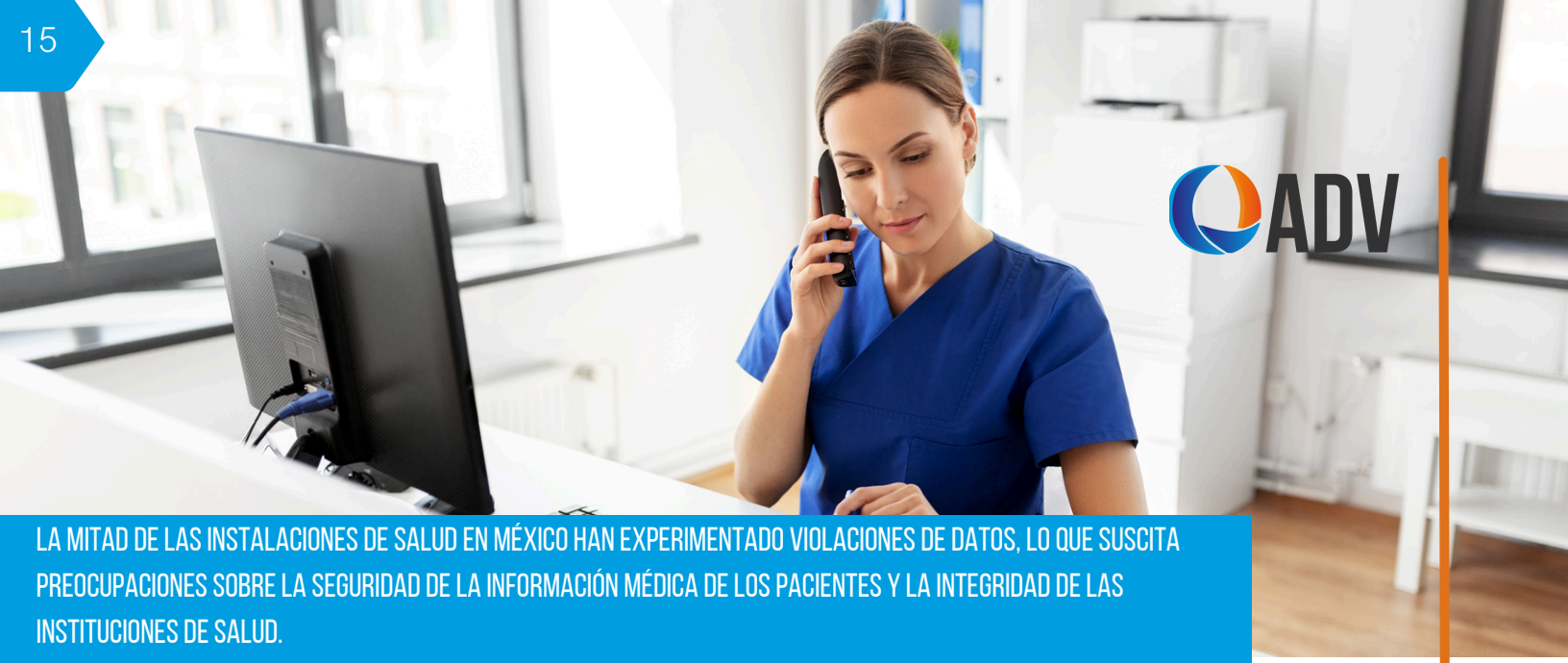
En cuanto al esquema de cifrado utilizado, RansomHub emplea ChaCha20 con Curve25519 para generar claves públicas y privadas. Este cifrado se aplica de manera parcial a ciertos tipos de archivos relacionados con ESXi, como '.vmdk', '.vmx', '.vmsn', con el objetivo de mantener un rendimiento rápido.

Específicamente, el cifrador encripta solo el primer megabyte de archivos que superan los 1 MB de tamaño, repitiendo los bloques de cifrado cada 11 MB. Además, cada archivo cifrado recibe un pie de página de 113 bytes que contiene la clave pública de la víctima, el nonce ChaCha20 y el recuento de fragmentos, para facilitar el proceso de descifrado en caso de pago del rescate.

La nota de rescate generada por RansomHub se escribe estratégicamente en dos ubicaciones específicas dentro del entorno comprometido de VMware ESXi: '/etc/motd' (Mensaje del día) y '/usr/lib/vmware/hostd/docroot/ui/index.html'. Estas ubicaciones son seleccionadas para asegurar que el mensaje de rescate sea visible tanto en las pantallas de inicio de sesión como en las interfaces web del sistema afectado. De esta manera, los atacantes aseguran que su demanda de rescate sea claramente comunicada a los usuarios y administradores que interactúan con el entorno comprometido.

Toulas, B. (2024, June 20). Linux version of RansomHub ransomware targets VMware ESXi VMs. BleepingComputer. https://www.bleepingcomputer.com/news/security/linux-version-of-ransomhub-ransomware-targets-vmware-esxi-vms/

NOTICIAS NACIONALES



LA MITAD DE LAS INSTALACIONES DE SALUD EN MÉXICO HAN EXPERIMENTADO VIOLACIONES DE DATOS, LO QUE SUSCITA PREOCUPACIONES SOBRE LA SEGURIDAD DE LA INFORMACIÓN MÉDICA DE LOS PACIENTES Y LA INTEGRIDAD DE LAS INSTITUCIONES DE SALUD.

SEGÚN EL INFORME DE LA SECRETARÍA DE SALUD DE MÉXICO (SOTI), EL 50% DE LOS CENTROS DE SALUD EN MÉXICO HA EXPERIMENTADO ALGUNA FORMA DE VIOLACIÓN DE DATOS.

Según el informe '¿Prosperará o Sobrevivirá el Cuidado de la Salud?' de SOTI, el 50% de los centros de salud en México ha enfrentado incidentes de seguridad que comprometen la información de los pacientes. Este hallazgo subraya la vulnerabilidad del sistema de salud mexicano ante ciberataques y otras formas de violación de datos.

Entre los incidentes más frecuentes reportados se incluyen filtraciones de datos por parte de terceros, ataques de ransomware y filtraciones accidentales de datos por parte del personal interno. Estos problemas no solo comprometen la información personal de los pacientes, sino que también resultan en costos económicos considerables y afectan la reputación de las instituciones involucradas.

La situación en México no es única, ya que otros países también enfrentan desafíos importantes en cuanto a la protección de datos en el sector de la salud. Sin embargo, la magnitud y las causas de estos incidentes varían considerablemente entre naciones.

En los Países Bajos, el 55% de las organizaciones de salud informaron de filtraciones de datos por parte de fuentes externas, y un 52% sufrió ataques de ransomware. A pesar de estas cifras preocupantes, solo el 15% de los responsables de TI en los Países Bajos consideran que la seguridad de los datos es su principal preocupación en TI.

Por otro lado, en Canadá se observa un alto número de filtraciones de datos tanto internas como externas, siendo la seguridad de los datos la principal preocupación para el 31% de los responsables de TI. Esto coincide con la alta incidencia de violaciones de datos en el país, donde el 46% de las organizaciones de salud han reportado incidentes similares.

El Reino Unido y los Estados Unidos también muestran niveles significativos de preocupación y frecuencia de incidentes. En el Reino Unido, el 49% de las organizaciones han experimentado filtraciones de datos, mientras que en los Estados Unidos, esta cifra alcanza el 50%.

SEGÚN EL INFORME DE LA SECRETARÍA DE SALUD DE MÉXICO (SOTI), EL 50% DE LOS CENTROS DE SALUD EN MÉXICO HA EXPERIMENTADO ALGUNA FORMA DE VIOLACIÓN DE DATOS.

Según el informe de SOTI, a nivel global, la principal preocupación en el sector de la salud en relación con la seguridad de los datos es el posible robo de registros de pacientes durante ciberataques externos, mencionado por el 42% de los encuestados. Otras inquietudes incluyen el daño a la reputación después de una filtración (38%), los costos financieros asociados con violaciones de datos (36%) y la revelación de información de pacientes sin su consentimiento (37%).

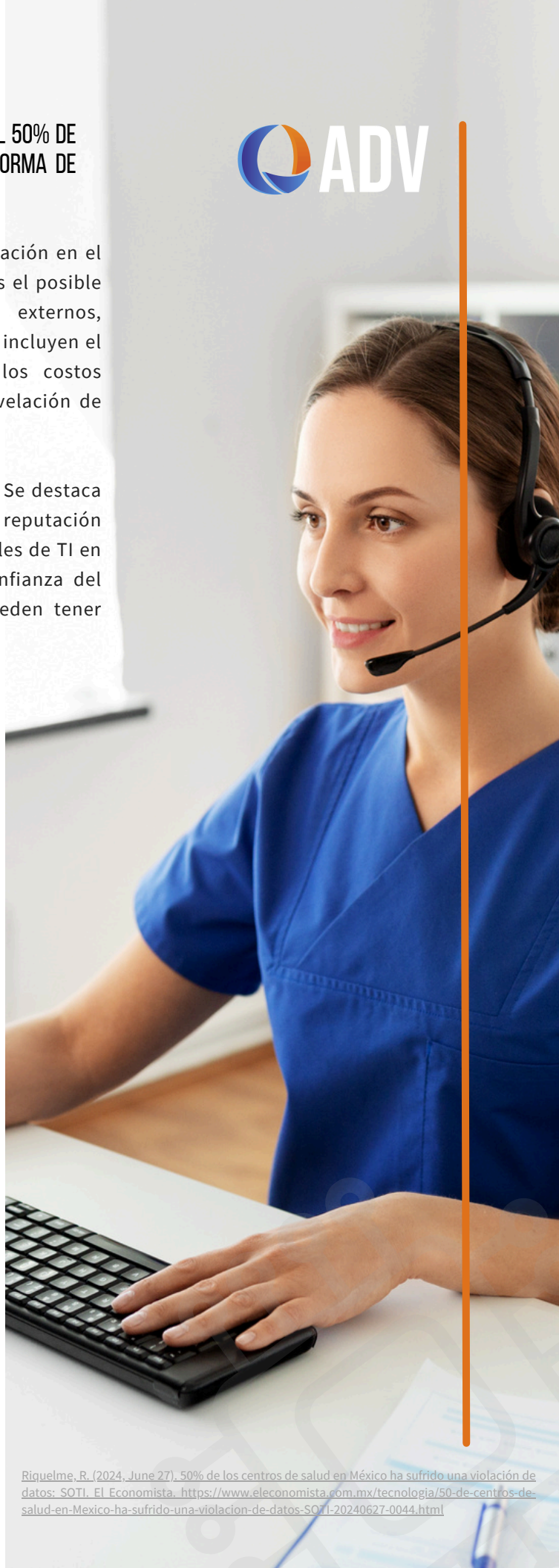
En México, las preocupaciones son similares según el informe. Se destaca que la revelación de información de pacientes y el daño a la reputación son dos de las principales preocupaciones entre los responsables de TI en el sector de la salud. Estos riesgos no solo impactan la confianza del público en las instituciones de salud, sino que también pueden tener consecuencias legales y financieras significativas.

El informe de SOTI se fundamentó en una encuesta realizada a 1450 responsables de decisiones en tecnología de la información en el sector de la salud, abarcando varios países como Estados Unidos, Canadá, México, Reino Unido, Alemania, Francia, Suecia, Países Bajos y Australia.

La recolección de datos se llevó a cabo del 7 al 25 de marzo de 2024. Para garantizar la representatividad de los datos, se incluyeron profesionales de diversas áreas dentro del sector de la salud. Un tercio de los encuestados trabajaban en clínicas o consultorios médicos generales, mientras que el 25% procedía de clínicas que ofrecían atención de emergencia, incluyendo áreas como salud mental y neurología.

Además, un 24% de los encuestados trabajaban en hospitales y un 18% en servicios de telemedicina.

SOTI es una compañía especializada en soluciones de gestión de movilidad empresarial (EMM) y del Internet de las Cosas (IoT). Fundada en 1995, SOTI ofrece software y servicios diseñados para ayudar a las organizaciones a administrar, asegurar y respaldar dispositivos móviles y otros puntos finales conectados en sus redes.



Riquelme, R. (2024, June 27). 50% de los centros de salud en México ha sufrido una violación de datos: SOTI. El Economista. https://www.eleconomista.com.mx/tecnologia/50-de-centros-de-salud-en-Mexico-ha-sufrido-una-violacion-de-datos-SOTI-20240627-0044.html

LA POLICÍA CIBERNÉTICA DE TAMAULIPAS ESTÁ OCUPADA GESTIONANDO MÁS DE 1,500 REPORTES HASTA EL MOMENTO.

Estos reportes principalmente relacionados con amenazas derivadas del cobro extrajudicial de aplicaciones de préstamos. Según informó el policía segundo Javier Galindo Hernández, esta unidad ha observado un alto volumen de incidentes en municipios como Reynosa, Ciudad Victoria, Matamoros y Tampico.

Galindo explicó que uno de los factores que contribuyen a este problema es la falta de atención a los términos y condiciones por parte de los usuarios al descargar aplicaciones. Esta falta de atención puede resultar en la concesión inadvertida de acceso a datos personales sensibles, como la cámara, la galería de fotos y la agenda de contactos, a los operadores de estas aplicaciones maliciosas.

Para prevenir ser víctima de estas aplicaciones fraudulentas, el policía recomendó a los ciudadanos verificar el registro de las aplicaciones ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) antes de instalarlas en sus dispositivos electrónicos. Esta precaución adicional podría ayudar a evitar problemas graves de seguridad y proteger la información personal contra el abuso y el acceso no autorizado.

Además, Galindo destacó que la disposición de la ciudadanía de Tamaulipas para reportar estos incidentes es fundamental, ya que refleja una mayor conciencia sobre la importancia de la seguridad cibernética y la protección de los datos personales. Este aumento en las denuncias también demuestra un aumento en la confianza de la población en las autoridades para abordar y resolver estos problemas, lo cual es crucial para mantener un entorno digital más seguro y protegido para todos los usuarios.

LA GUARDIA ESTATAL CIBERNÉTICA DE TAMAULIPAS, BAJO LA SECRETARÍA DE SEGURIDAD PÚBLICA, HA RESPONDIDO A MÁS DE 1,500 REPORTES DESDE ENERO HASTA MAYO.

Aguilar, R. (2024, June 5). Atiende Policía Cibernética más de mil 500 reportes en Tamaulipas. El Universal. https://www.eluniversal.com.mx/estados/atiende-policia-cibernetica-mas-de-mil-500-reportes-en-tamaulipas/

Ciberseguridad, prioridad de la banca mexicana. (2024, junio 29). Imagen Radio 90.5. https://www.imagenradio.com.mx/ciberseguridad-prioridad-de-la-banca-mexicana

LOS BANCOS MEXICANOS TIENEN PLANEADO DESTINAR ALREDEDOR DE 24 MIL MILLONES DE PESOS ESTE AÑO EN MEJORAR LA CIBERSEGURIDAD Y EXPANDIR SUS SERVICIOS DIGITALES

LA SEGURIDAD DIGITAL SE CONSIDERA UNA PRIORIDAD FUNDAMENTAL PARA LOS BANCOS EN MÉXICO.

Según la Asociación de Bancos de México (ABM). Julio Carranza, líder de los banqueros, subrayó que el año pasado se había asignado una suma similar para protegerse contra ciberdelincuentes y ampliar los productos digitales debido a la creciente adopción de servicios financieros en línea.

Carranza opinó que este nivel de inversión debería tranquilizar a los usuarios sobre el compromiso de las instituciones financieras para evitar ciberataques que puedan comprometer sus operaciones, así como para ofrecer una gama completa de servicios a través de internet.

Según el Banco de México (Banxico), el sistema financiero reportó cuatro incidentes cibernéticos en 2023, con un costo total de 89.07 millones de pesos. Los incidentes incluyeron problemas en cajeros automáticos en febrero, afectaciones a transferencias electrónicas en marzo, y otros eventos en mayo y julio que afectaron a la banca por internet, sucursales, transferencias electrónicas y cajeros automáticos.

Eduardo Osuna, vicepresidente de la organización, destacó que la banca está trabajando de manera integral para mitigar riesgos, dado que los hábitos de los clientes se vuelven cada vez más digitales. La inversión incluye capacitación para los clientes y mejoras en las plataformas en colaboración con empresas que ofrecen nuevos modelos de negocio, facilitando así la entrega de servicios.

Además, la banca ha implementado medidas beneficiosas para los clientes, como la adopción de chip y NIP en tarjetas de débito y crédito, lo que ha reducido el fraude en un 71% en años recientes. Este sistema coloca a México en la vanguardia en seguridad para transacciones con tarjetas, ya que el 96% de estas operan bajo este formato.

Osuna explicó que los antiguos sistemas de banda magnética eran vulnerables a la clonación y al fraude, mientras que el nuevo sistema requiere la presencia física de la tarjeta y del cliente para autenticar las transacciones, lo que ayuda a prevenir la falsificación y las pérdidas económicas.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: JUNIO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-6265	29/06/2024	Fallas de seguridad en productos WordPress	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-6265

Descripción: El complemento UsersWP – Front-end login form, User Registration, User Profile & Members Directory para WordPress es vulnerable a la inyección SQL basada en tiempo a través del parámetro 'uwp_sort_by' en todas las versiones hasta la 1.2.10 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 atacantes no autenticados agreguen consultas SQL adicionales a consultas ya existentes que se pueden usar para extraer información confidencial de la base de datos.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-3912	14/06/2024	Fallas de seguridad en productos ASUS	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-3912

Descripción: Algunos modelos de enrutadores ASUS tienen una vulnerabilidad de carga de firmware arbitraria. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para ejecutar comandos de sistema arbitrarios en el dispositivo.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-3080	13/06/2024	Fallas de seguridad en productos ASUS	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-3080

Descripción: Ciertos modelos de enrutadores ASUS tienen una vulnerabilidad de omisión de autenticación, lo que permite que atacantes remotos no autenticados inicien sesión en el dispositivo.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-30299	13/06/2024	Fallas de seguridad en productos Adobe	CVSS v3.1: 10.0 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-30299

Descripción: Las versiones 2020.3, 2022.2 y anteriores de Adobe Framemaker Publishing Server se ven afectadas por una vulnerabilidad de autenticación incorrecta que podría provocar una escalada de privilegios. Un atacante podría aprovechar esta vulnerabilidad para obtener acceso no autorizado o privilegios elevados dentro de la aplicación. La explotación de este problema no requiere la interacción del usuario.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-34108	13/06/2024	Fallas de seguridad en productos Adobe	CVSS v3.1: 9.1 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-34108

Descripción: Las versiones 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 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 se requieren privilegios de administrador.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-30080	11/06/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 9.8 [Critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-30080

Descripción: Vulnerabilidad de ejecución remota de código en Microsoft Message Queue (MSMQ)

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-5526	05/06/2024	Fallas de seguridad en productos Grafana	CVSS v3.1: 9.1 [Critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-5526

Descripción: Grafana OnCall es una herramienta de gestión de guardias fácil de usar que ayudará a reducir el trabajo en la gestión de guardias a través de flujos de trabajo e interfaces más simples que están diseñados específicamente para ingenieros. Grafana OnCall, desde la versión 1.1.37 hasta la 1.5.2, es vulnerable a una vulnerabilidad de falsificación de solicitud del lado del servidor (SSRF) en la funcionalidad de webhook. Este problema se solucionó en la versión 1.5.2

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-38667	24/06/2024	Fallas de seguridad en productos Linux	CVSS v3.1: 7.8 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-38667

Descripción: En el kernel de Linux, se ha resuelto la siguiente vulnerabilidad: riscv: evitar la corrupción de pt_regs para subprocesos inactivos secundarios La parte superior de la pila de subprocesos del kernel debería reservarse para pt_regs. Sin embargo, este no es el caso de los subprocesos inactivos de los harts de arranque secundarios. Sus pilas se superponen con sus pt_regs, por lo que ambos pueden corromperse. Se ha solucionado un problema similar para el hart principal, consulte c7cdd96eca28 ("riscv: evitar la corrupción de la pila reservando task_pt_regs(p) de forma anticipada"). Sin embargo, esa solución no se propagó a los harts secundarios. El problema se ha detectado en algunas pruebas de conexión en caliente de la CPU con V habilitado. La función smp_callin almacenó varios registros en la pila, corrompiendo la parte superior de la estructura pt_regs, incluido el campo de estado. Como resultado, el kernel intentó guardar o restaurar el contexto V inexistente.

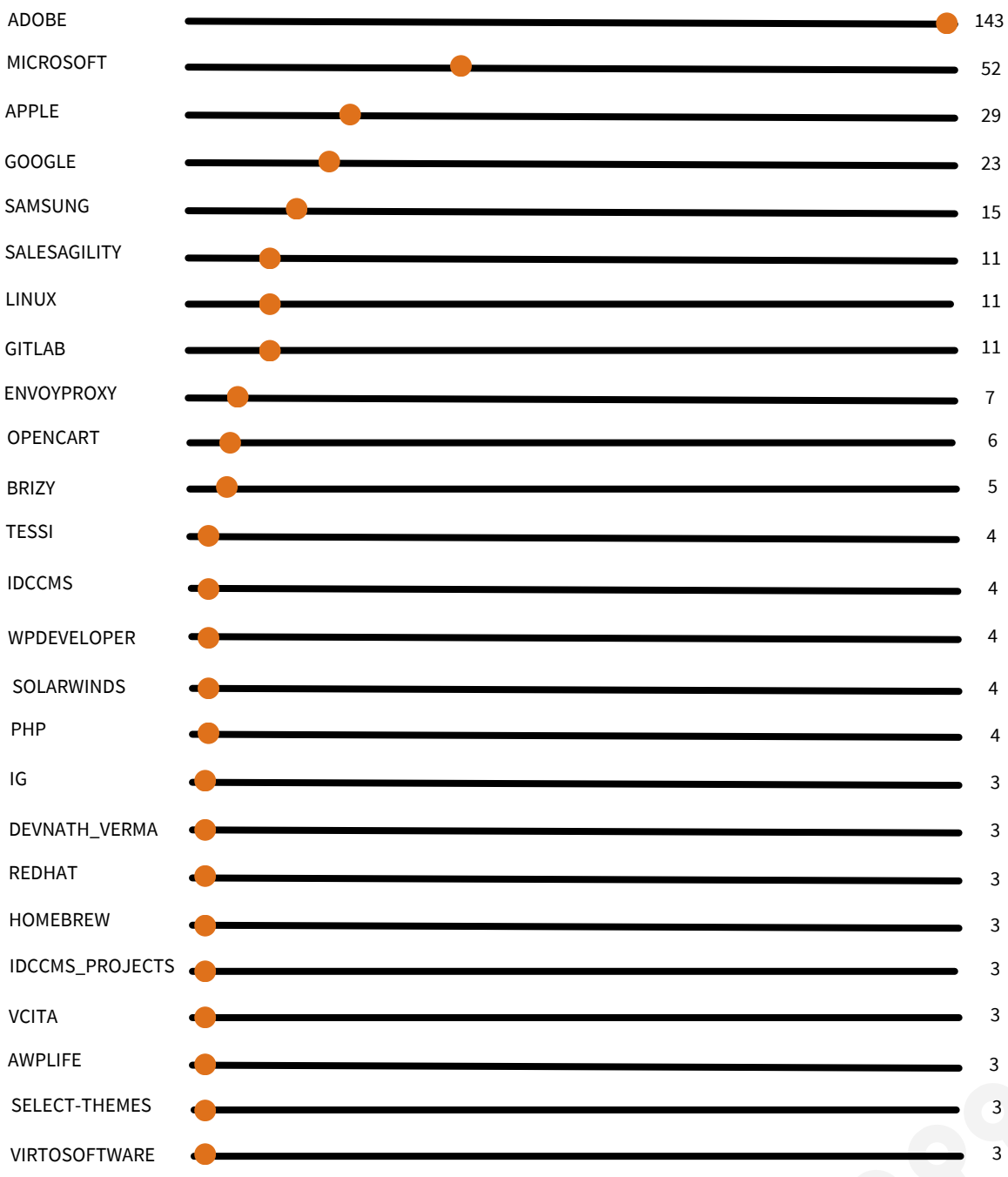
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-34104	13/06/2024	Fallas de seguridad en productos Adobe	CVSS v3.1: 8.5 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2022-34104

Descripción: Las versiones 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 y anteriores de Adobe Commerce se ven afectadas por una vulnerabilidad de autorización incorrecta que podría provocar la omisión de una función de seguridad. Un atacante podría aprovechar esta vulnerabilidad para eludir las medidas de seguridad y obtener acceso no autorizado, lo que afectaría tanto a la confidencialidad como a la integridad. La explotación de este problema no requiere la interacción del usuario.

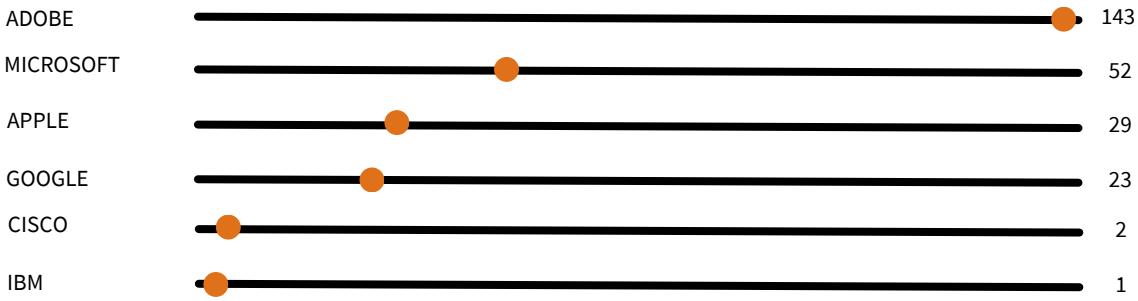
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-35265	11/06/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 7.0 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-35265

Descripción: Vulnerabilidad de elevación de privilegios en el servicio Windows Perception.

FABRICANTES CON VULNERABILIDADES RELEVANTES: JUNIO DE 2024



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: JUNIO DE 2024



CULTURA DE CIBERSEGURIDAD

REDES WI-FI PUBLICAS

El acceso a Internet inalámbrico está ampliamente disponible en diversos lugares como cafeterías, restaurantes, centros comerciales, aeropuertos, hoteles e incluso algunos parques y exposiciones. Esta conveniencia permite trabajar en cualquier lugar o simplemente distraerse mientras se espera. Sin embargo, la accesibilidad de estas redes públicas también las hace vulnerables a ataques de hackers y brechas de seguridad.

Muchos aprecian la posibilidad de estar en un establecimiento durante horas sin consumir sus propios datos móviles, pero es importante ser consciente del riesgo potencial. Conocer estos riesgos puede influir en la decisión de conectarse a ciertos lugares o de realizar ciertas actividades en línea.

No es necesario limitarse exclusivamente a la red doméstica u oficinal, pero es crucial entender los peligros asociados con las redes Wifi públicas si se desea navegar de manera segura mientras se está fuera. Para comprender mejor estos riesgos, es fundamental revisar cómo funcionan este tipo de redes.

¿COMO FUNCIONA UNA RED WI-FI?

La tecnología WiFi, abreviatura de Wireless Fidelity, permite la transmisión inalámbrica de datos a varios dispositivos como computadoras, tablets y móviles. Esta transmisión se realiza utilizando ondas de radio en frecuencias de 2,4 GHz o 5 GHz, siendo esta última la más avanzada.

Para que estas ondas sean transmitidas, se necesita un router que reciba la información de Internet y la convierta en ondas. Estas ondas son captadas por el adaptador inalámbrico del dispositivo conectado a la red, que luego traduce los datos solicitados para su uso.

RIESGOS DE UTILIZAR UNA RED WI-FI PUBLICA

Conociendo cómo funciona una red WiFi, podemos explicar cómo los hackers aprovechan las vulnerabilidades de las redes públicas para atacar a los dispositivos conectados y los métodos a los que estás expuesto.
Un ataque común es el "Man in the Middle" (MitM), donde el hacker se sitúa entre el router y el dispositivo, interceptando toda la información transmitida. Este tipo de ataque es difícil de detectar y puede resultar en la revelación inadvertida de información privada.

Otro riesgo son las redes falsas, donde un atacante se hace pasar por una red legítima o copia su nombre para engañar a los usuarios. Estas redes a menudo no requieren contraseña, lo que las hace atractivas pero peligrosas ya que permiten a los hackers acceder a la información de los usuarios.

Técnicas como el "Snooping" y "Sniffer" también son utilizadas para capturar información transmitida, incluyendo contraseñas y datos sensibles utilizados en redes sociales o transacciones bancarias.

Además, las redes públicas pueden ser utilizadas por hackers para distribuir malware, como ransomware, que secuestra datos y exige un rescate para su liberación.

La seguridad de la conexión también depende del router utilizado. Si el router no está configurado para cifrar datos o no cuenta con medidas de seguridad efectivas, puede ser un punto vulnerable donde la información y los dispositivos están expuestos a riesgos de ciberseguridad.

COMO NAVEGAR DE MANERA SEGURA EN UNA RED WI-FI PUBLICA

Para proteger tu información al conectarte a redes WiFi públicas, considera las siguientes medidas:

1. Mantén actualizados el antivirus y las aplicaciones: Asegúrate de tener las últimas versiones de tus aplicaciones para contar con los parches de seguridad más recientes. Un antivirus actualizado también detectará y protegerá contra nuevas amenazas.
2. Evita realizar operaciones bancarias: Es recomendable abstenerse de acceder a la banca en línea desde redes WiFi públicas, ya que no siempre son seguras.
3. Sé consciente de tus actividades: Evita ingresar contraseñas o acceder a redes sociales desde redes WiFi públicas para proteger tu información sensible.

4. Apaga la conexión WiFi cuando no la necesites: Si no estás utilizando activamente Internet o estás trabajando con archivos que no requieren conexión, desactiva el WiFi de tus dispositivos para evitar conexiones automáticas a redes potencialmente riesgosas.

5. Utiliza sitios web con protocolo HTTPS: Asegúrate de que los sitios que visites utilicen HTTPS, lo cual garantiza que la información intercambiada esté cifrada y sea más segura.

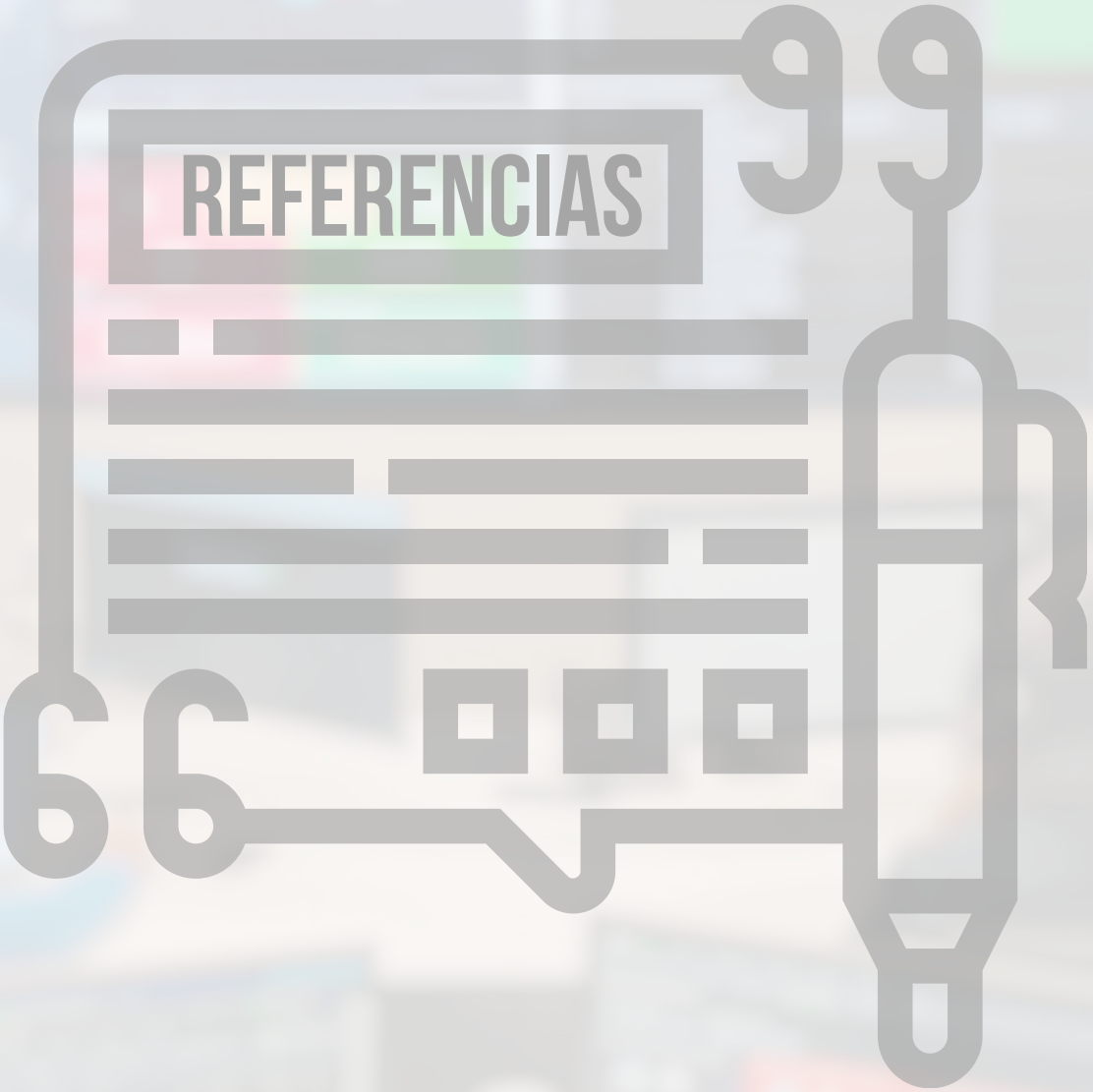
6. Usa una VPN (Red Privada Virtual): Si necesitas trabajar con información delicada, considera utilizar una VPN para cifrar tu conexión y proteger tus datos de posibles interceptaciones.

7. Implementa autenticación de dos factores: Configura la autenticación de dos pasos en tus cuentas importantes. Esto añade una capa adicional de seguridad al solicitar un segundo código además de tu contraseña, dificultando a los hackers el acceso a tus cuentas solo con la contraseña.

Siguiendo estas precauciones, puedes reducir significativamente los riesgos asociados con el uso de redes WiFi públicas y proteger tu información personal y profesional.

Tienda HP Online Jr C. (2023) Redes WiFi Públicas: Riesgos que debes conocer y cómo prevenirlos. <i>HP TECH TAKES (... - HP.com México</i>. Available at: https://www.hp.com/mx-es/shop/tech-takes/riesgos-redes-wifi-publicas (Accessed: 02 July 2024).

REFERENCIAS



REFERENCIAS

- Toulas, B. (2024, June 4). New V3B phishing kit targets customers of 54 European banks. BleepingComputer. https://www.bleepingcomputer.com/news/security/new-v3b-phishing-kit-targets-customers-of-54-european-banks/
- The Hacker News. (n.d.). Azure Service Tags Vulnerability: Microsoft warns of potential abuse by hackers. https://thehackernews.com/2024/06/azure-service-tags-vulnerability.html
- The Hacker News. (n.d.). Snowflake Breach exposes 165 customers' data in ongoing extortion campaign. https://thehackernews.com/2024/06/snowflake-breach-exposes-165-customers.html
- Abrams, L. (2024, June 18). AMD investigates breach after data for sale on hacking forum. BleepingComputer. https://www.bleepingcomputer.com/news/security/amd-investigates-breach-after-data-for-sale-on-hacking-forum/
- Toulas, B. (2024, June 20). Linux version of RansomHub ransomware targets VMware ESXi VMs. BleepingComputer. https://www.bleepingcomputer.com/news/security/linux-version-of-ransomhub-ransomware-targets-vmware-esxi-vms/
- Riquelme, R. (2024, June 27). 50% de los centros de salud en México ha sufrido una violación de datos: SOTI. El Economista. https://www.eleconomista.com.mx/tecnologia/50-de-centros-de-salud-en-Mexico-ha-sufrido-una-violacion-de-datos-SOTI-20240627-0044.html
- Aguilar, R. (2024, June 5). Atiende Policía Cibernética más de mil 500 reportes en Tamaulipas. El Universal. https://www.eluniversal.com.mx/estados/atiende-policia-cibernetica-mas-de-mil-500-reportes-en-tamaulipas/
- Ciberseguridad, prioridad de la banca mexicana. (2024, June 29). Imagen Radio 90.5. https://www.imagenradio.com.mx/ciberseguridad-prioridad-de-la-banca-mexicana
- Tienda HP Online, H.C. (2022) Redes WIFI Públicas: Riesgos que debes conocer y cómo prevenirlos, < HP TECH TAKES /... - HP.com México. Available at: https://www.hp.com/mx-es/shop/tech-takes/riesgos-redes-wifi-publicas (Accessed: 02 July 2024).

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