BOLETÍN DE CIBERSEGURIDAD

OCTUBRE 2023

ÍNDICE

NOTICIAS INTERNACIONALES

LA OCU DETECTA HASTA 61 VULNERABILIDADES EN DISPOSITIVOS INTELIGENTES USADOS EN EL HOGAR, 12 DE ELLAS "CRÍTICAS"

LA ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS HA IDENTIFICADO UN TOTAL DE 61 VULNERABILIDADES EN UN ANÁLISIS DE SEGURIDAD CIBERNÉTICA DE 17 DISPOSITIVOS PARA EL HOGAR CONECTADOS A INTERNET.

incluyendo routers, cerraduras electrónicas, cámaras de vigilancia, enchufes y termostatos inteligentes, altavoces, aspiradoras robot, tablets, smartphones, smartwatches e impresoras. De estas vulnerabilidades, 12 se consideran "críticas".

Las mayores deficiencias de seguridad se han encontrado en cámaras de vigilancia, cerraduras electrónicas y dispositivos portátiles como smartphones, smartwatches y tablets para niños, especialmente en productos disponibles en tiendas en línea poco conocidas, según explicó la organización en un comunicado.

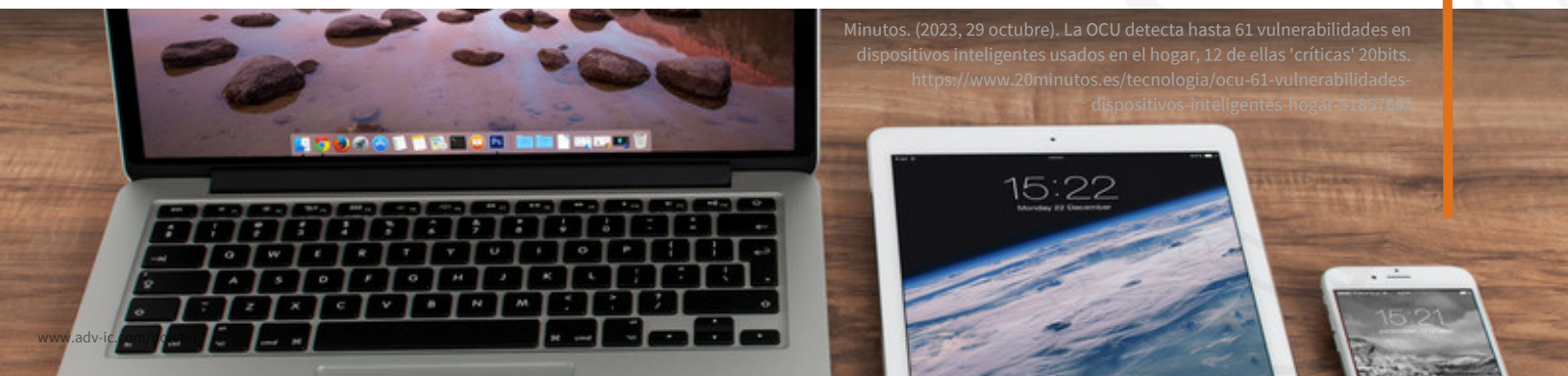
En particular, se ha señalado que nueve de los 17 dispositivos aún permiten contraseñas simples como "123456", y el cifrado de las comunicaciones entre dispositivos y aplicaciones a menudo es débil o inexistente, según la OCU.

También se ha destacado la falta de seguridad en el almacenamiento de datos en tarjetas de memoria, lo que facilita el robo de contraseñas, nombres de usuario y grabaciones de video.

Otro aspecto preocupante es la posibilidad de interceptar y alterar las comunicaciones entre dos partes, lo que se ha observado en cuatro de los productos analizados. Además, la OCU ha encontrado que varios dispositivos del estudio pueden ser desmontados y manipulados por personas con conocimientos técnicos, lo que podría utilizarse para realizar modificaciones maliciosas en el software.

La OCU ha llamado la atención sobre la necesidad de controles más estrictos de seguridad cibernética por parte de las autoridades y la imposición de sanciones significativas a las marcas que no cumplan con los estándares de seguridad. También ha enfatizado que los fabricantes deben no solo garantizar dispositivos seguros, sino también seguir brindando actualizaciones de seguridad durante un período determinado después de la compra del producto.

Como medidas preventivas, la OCU ha aconsejado a los consumidores que prioricen la compra de dispositivos en tiendas en línea con sede en Europa, que cambien las contraseñas predeterminadas de los dispositivos y que verifiquen que el dispositivo esté actualizado con la última versión del sistema operativo. Además, la organización está a la espera de la nueva ley europea de ciberresiliencia, que se espera refuerce la seguridad de los dispositivos, aunque no será obligatoria hasta 2027.



Minutos. (2023, 29 octubre). La OCU detecta hasta 61 vulnerabilidades en dispositivos inteligentes usados en el hogar, 12 de ellas 'críticas' 20bits. https://www.20minutos.es/tecnologia/ocu-61-vulnerabilidades-dispositivos-inteligentes-hogar-5185766/

LAS 'BIG TECH' DE LA IA DESTINAN 10 MILLONES DE DÓLARES PARA LA SEGURIDAD DE SU INVESTIGACIÓN

ESTA SEMANA, LAS PRINCIPALES EMPRESAS TECNOLÓGICAS EN EL CAMPO DE LA INTELIGENCIA ARTIFICIAL (IA) HAN ANUNCIADO LA CREACIÓN DE UN FONDO DEDICADO A LA SEGURIDAD DE LOS AVANCES EN ESTE ÁMBITO.

Palomo, J. (2023, 27 octubre). Las «Big Tech» de la IA destinan 10 millones de dólares para la seguridad de su investigación. Diario ABC. https://www.abc.es/tecnologia/big-tech-ia-destinan-millones-dolares-seguridad-20231027105731-nt.html

El propósito principal del fondo es permitir que investigadores independientes puedan evaluar, probar y desarrollar herramientas relacionadas con los modelos de IA más avanzados. Este anuncio representa el primer comunicado y movimiento financiero por parte de Anthropic, Google, Microsoft y OpenAI en su colaboración conocida como 'Frontier Model Forum', la cual también ha designado a un director ejecutivo. Este grupo se formó en julio pasado con la finalidad de establecer controles en el campo de la IA y mitigar su potencial uso perjudicial para la sociedad.

Sin embargo, el arranque de esta asociación no ha sido completamente auspicioso, ya que la financiación inicial asciende a alrededor de 10 millones de dólares, una cantidad modesta en comparación con las valoraciones e inversiones que estas empresas manejan, como el caso de Microsoft que invirtió 10.000 millones en OpenAI y las negociaciones de Anthropic para recibir más de 3.000 millones de Google y Amazon.

Las empresas consideran que esta suma será suficiente para cumplir con parte de los compromisos que han asumido con la Casa Blanca en relación a la creación de una IA responsable. Estos compromisos voluntarios incluyen la facilitación de la identificación y notificación de vulnerabilidades en sus sistemas de IA por parte de terceros.

LAS 'BIG TECH' DE LA IA DESTINAN 10 MILLONES DE DÓLARES PARA LA SEGURIDAD DE SU INVESTIGACIÓN

El Fondo de Seguridad de la IA se percibe como un elemento crucial para cumplir con este compromiso, al proporcionar financiamiento a la comunidad externa para evaluar y comprender mejor los sistemas de IA más avanzados.

Para liderar esta iniciativa, las compañías tecnológicas han elegido a Chris Meserole, un experto en seguridad de la IA que ha estado trabajando en estas herramientas desde 2018 y que anteriormente se desempeñó como director del centro de investigación Brookings Institution. Meserole ha señalado que si bien los modelos de IA más avanzados ofrecen un gran potencial para la sociedad, es fundamental comprender mejor cómo desarrollarlos y evaluarlos de manera segura.

El objetivo del Forum es abordar el principal problema asociado con los modelos generativos de IA, que es su potencial para ser utilizados de manera inadecuada y que escapa al conocimiento de las empresas que los crean. La intención es prevenir la proliferación de actividades delictivas que ya han comenzado a emerger en línea.

REINO UNIDO APRUEBA LA CONTROVERTIDA LEY DE SEGURIDAD EN LÍNEA

Jeremy Wright, uno de los cinco ministros del Reino Unido encargados de impulsar la legislación histórica del gobierno británico sobre la regulación de Internet, conocida como la Ley de Seguridad en Línea (Online Safety Bill), fue el primero en hacerlo. Aunque el gobierno británico suele promocionar sus iniciativas como líderes a nivel mundial, en este caso, la Ley de Seguridad en Línea podría haber sido pionera en 2019. En ese momento, el proyecto de ley reconocía que las redes sociales ya actuaban como árbitros de facto sobre lo que se consideraba una forma de expresión aceptable en gran parte de la web. Sin embargo, estas plataformas no querían asumir esa responsabilidad por completo.

El proyecto de ley tenía como objetivo definir cómo abordar el contenido "legal pero perjudicial", es decir, material que no era ilegal per se, pero que podía representar un riesgo, como la desinformación médica, publicaciones que promovían el suicidio o trastornos alimentarios, o la desinformación política que podía socavar la democracia. Aunque el proyecto de ley tuvo detractores que temían que otorgara demasiado poder a las grandes empresas tecnológicas, también fue elogiado por abordar un problema que estaba evolucionando más rápido de lo que la política y la sociedad podían seguir.

Después de pasar por las dos cámaras del Parlamento del Reino Unido, el proyecto de ley finalmente recibió la aprobación real. Sin embargo, ya no es considerado pionero a nivel mundial, ya que la Ley de Servicios Digitales de la Unión Europea comenzó a aplicarse en agosto.

Guest, P. (2023, 26 octubre). Reino Unido aprueba la controvertida ley de seguridad en línea. WIRED. https://es.wired.com/articulos/reino-unido-aprueba-controvertida-ley-de-seguridad-en-linea

La nueva Ley de Seguridad en Línea (Online Safety Act) es más amplia y polémica que la versión original defendida por Wright. Contiene más de 200 cláusulas que abarcan una amplia gama de contenidos ilegales que las plataformas deben combatir. También les impone un "deber de diligencia" en lo que respecta a lo que sus usuarios, especialmente los niños, ven en Internet.
Además, la ley establece requisitos para que las plataformas de mensajería revisen los envíos de los usuarios en busca de contenido ilícito, lo cual ha generado controversia ya que algunas empresas tecnológicas y defensores de la privacidad consideran que atenta contra la encriptación. Las compañías, desde las grandes tecnológicas hasta las plataformas más pequeñas y las aplicaciones de mensajería, deberán cumplir con una larga lista de nuevos requisitos, incluyendo la verificación de la edad de sus usuarios. La ley también prohíbe enviar amenazas de violencia, incluyendo la violación, y fomentar la autolesión o difundir pornografía deepfake, y obliga a las empresas a eliminar rápidamente este tipo de contenido de sus plataformas.

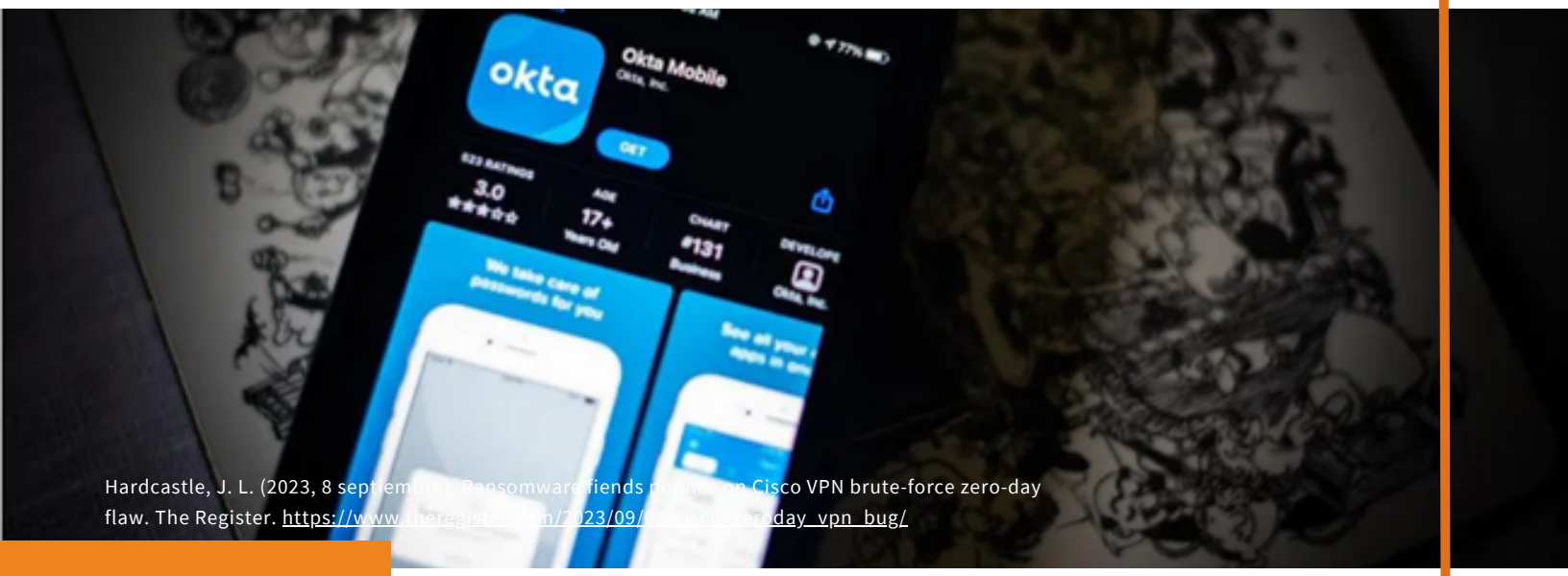
REINO UNIDO APRUEBA LA CONTROVERTIDA LEY DE SEGURIDAD EN LÍNEA

La aplicación de la ley estará a cargo de Ofcom, el regulador de telecomunicaciones del Reino Unido, y las empresas que no cumplan podrían enfrentar multas significativas. Sin embargo, la ley ha generado controversia debido a lo que no aborda, especialmente en lo que respecta a la desinformación en línea. Algunos críticos argumentan que la ley se centra demasiado en contenidos individuales y no aborda de manera adecuada la difusión de desinformación en línea.

Una de las cláusulas más polémicas de la ley es el artículo 122, que podría requerir que las empresas examinen los mensajes de los usuarios para asegurarse de que no compartan material ilegal. Esto plantea preocupaciones sobre la privacidad y la encriptación de extremo a extremo en plataformas de mensajería. A pesar de las preocupaciones, la cláusula se mantuvo en la ley.

En general, la Ley de Seguridad en Línea del Reino Unido es un intento importante de abordar los desafíos en línea, pero su implementación plantea desafíos significativos y controversias en torno a la privacidad y la libertad de expresión.

EL HACKEO A OKTA EXPONE UN PROBLEMA SISTEMÁTICO EN LA INDUSTRIA DE VERIFICACIÓN DE IDENTIDAD ONLINE



Hardcastle, J. L. (2023, 8 septiembre). Ransomware fiends pounce on Cisco VPN brute-force zero-day flaw. The Register. https://www.theregister.com/2023/09/[illegible]/cisco_zero-day_vpn_bug/

Atención: El viernes 20 de octubre, Okta, una plataforma de gestión de identidades anunció que había experimentado una intrusión en su sistema de atención al cliente. Dado que Okta es un servicio de acceso y autenticación, cualquier brecha en su seguridad plantea riesgos para otras organizaciones, y la empresa confirmó que "ciertos clientes" se vieron afectados. La compañía informó a WIRED que notificó a aproximadamente el 1% de los 18,400 usuarios perjudicados por el incidente.

Algunas empresas que son clientes de Okta, como 1Password, BeyondTrust y Cloudflare, detectaron actividad sospechosa relacionada con el incidente antes de que Okta les informara. Okta compartió similitudes con un incidente de seguridad que experimentó en 2022, lo que genera preocupaciones sobre la falta de medidas preventivas.

En este último incidente, los atacantes comprometieron una cuenta de soporte de Okta utilizando credenciales de inicio de sesión robadas y luego robaron cookies y tokens de sesión, que se utilizan para dar acceso a los proveedores de soporte al cliente a los sistemas de los usuarios para resolver problemas. Con estos tokens, los atacantes pudieron acceder directamente a las cuentas de los clientes de Okta.

Aunque algunas empresas como 1Password, BeyondTrust y Cloudflare pudieron detectar y bloquear las intrusiones antes de que afectaran a sus propios clientes, todas destacaron que habían notificado a Okta sobre la situación antes de que la empresa informara públicamente del incidente, en algunos casos semanas antes.

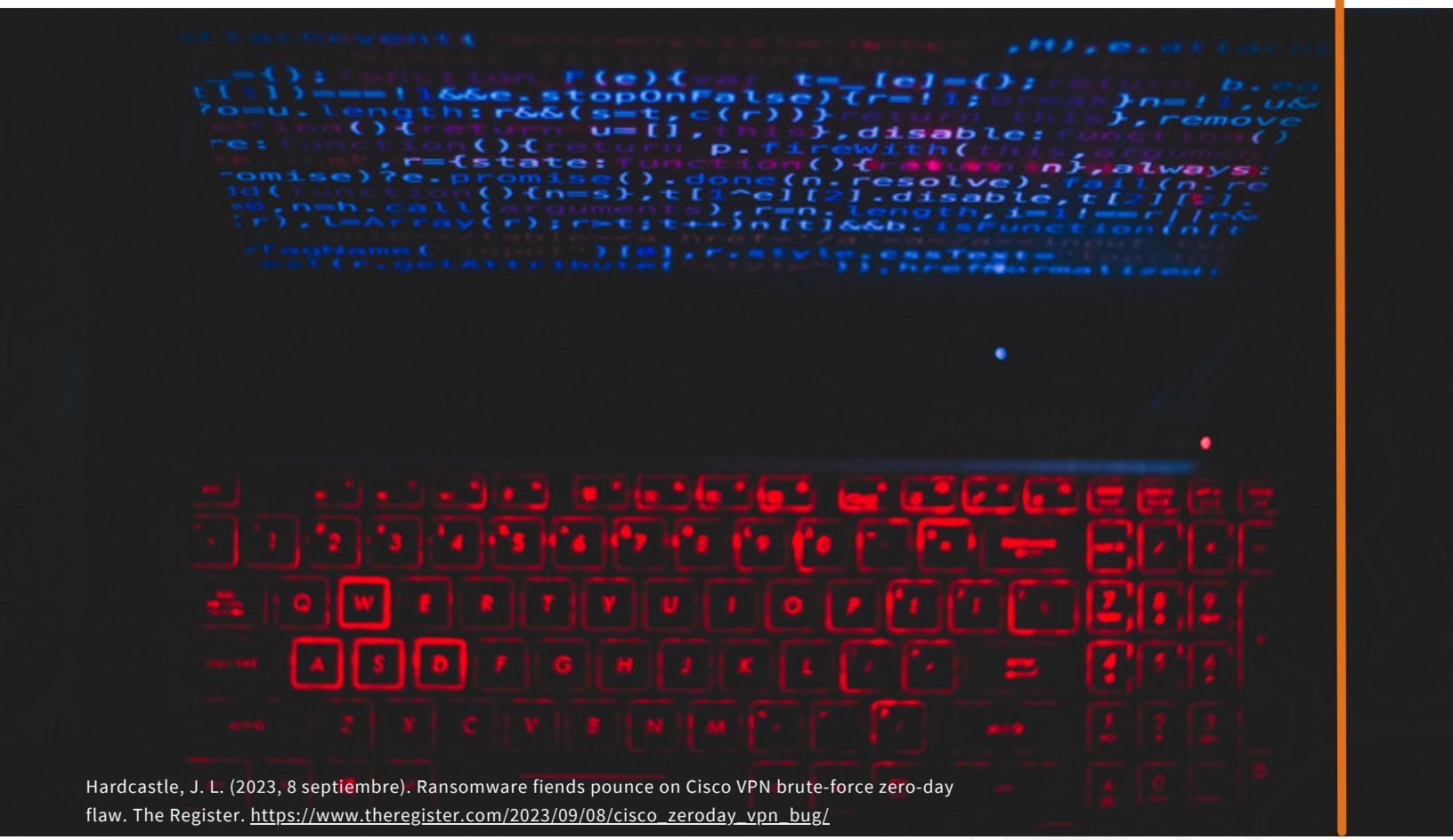
Okta, al ser un proveedor de servicios digitales críticos para muchas organizaciones, siempre es un objetivo principal para los ataques, ya que sirve como un punto de acceso para los hackers que buscan comprometer a numerosas organizaciones. La falta de medidas preventivas y la demora en la notificación de los incidentes plantean preocupaciones sobre la seguridad de Okta y su capacidad para proteger la información de sus clientes.

EL HACKEO A OKTA EXPONE UN PROBLEMA SISTEMÁTICO EN LA INDUSTRIA DE VERIFICACIÓN DE IDENTIDAD ONLINE

A pesar de las preocupaciones y críticas de las empresas afectadas, Okta no proporcionó comentarios sobre las medidas que está tomando para mejorar la seguridad de su servicio de atención al cliente o sobre la aparente falta de urgencia en la empresa al recibir informes de incidentes potenciales. La empresa se limitó a indicar que compartirá más información sobre estos temas en el futuro.

El problema de la seguridad en Okta parece relacionarse con la tercerización de servicios de soporte y con la falta de implementación de medidas de seguridad efectivas, como el uso de llaves de seguridad de hardware. Los expertos señalan que la cadena de suministro de software y la creciente cantidad de ciberataques son desafíos importantes para las empresas en la actualidad.

A pesar de los desafíos, Okta ha experimentado incidentes de seguridad en su cadena de suministro, particularmente en relación con el soporte externo, lo que plantea dudas sobre su capacidad para proteger la información de sus clientes y su respuesta ante incidentes de seguridad.



Hardcastle, J. L. (2023, 8 septiembre). Ransomware fiends pounce on Cisco VPN brute-force zero-day flaw. The Register. https://www.theregister.com/2023/09/08/cisco_zeroday_vpn_bug/

NOTICIAS NACIONALES

CIBERSEGURIDAD EN INSTITUCIONES FINANCIERAS: LA BATALLA MEXICANA CONTRA EL CIBERDELITO

LA SEGURIDAD CIBERNÉTICA SE HA CONVERTIDO EN UN TEMA DE GRAN PREOCUPACIÓN EN EL CONTEXTO FINANCIERO GLOBAL, ESPECIALMENTE EN LAS INSTITUCIONES BANCARIAS.

Con la acelerada transformación digital, la amenaza de ciberataques y las consiguientes pérdidas económicas han aumentado significativamente. México, en particular, ha experimentado el impacto de estos delincuentes cibernéticos.

Ortega, P. (2023, 26 octubre). Ciberseguridad en instituciones financieras: la batalla mexicana contra el ciberdelito. El Economista. https://www.eleconomista.com.mx/los-especiales/Ciberseguridad-en-instituciones-financieras-la-batalla-mexicana-contra-el-ciberdelito-20231025-0162.html

En el período 2021-2022, México sufrió el 66% de todos los ciberataques en América Latina, lo que resultó en pérdidas económicas anuales estimadas entre 3,000 y 5,000 millones de dólares, según datos proporcionados por la Asociación de Bancos de México y la Cámara Americana. Ejemplos concretos de vulnerabilidades se observaron en instituciones como el Buró de Crédito y el Banco de México (Banxico). Aunque estas cifras son alarmantes, también ofrecen una oportunidad para que las instituciones financieras mexicanas reevaluen fortalezcan y transformen sus sistemas de seguridad cibernética. Se enfatiza que la ciberseguridad no solo se trata de tecnología, sino de una combinación de gestión de riesgos, políticas coherentes y educación continua. La adopción de mejores prácticas internacionales, como el estándar ISO/IEC 27701:2019, se considera esencial para reforzar la seguridad de la información y proteger los datos personales.

Sin embargo, los desafíos persisten, ya que el primer semestre de 2023 registró más de 14,000 millones de intentos de ciberataques en México, siendo superado solo por Brasil en la región. Los ciberataques de ransomware y el malware continúan siendo las principales amenazas, y su evolución indica una tendencia hacia operaciones más específicas y dirigidas. La respuesta a esta crisis no depende únicamente de medidas tecnológicas, ya que se destaca la importancia de la colaboración global entre los sectores público y privado, así como la inversión en servicios de seguridad avanzados. Es esencial desalentar la economía de los delincuentes cibernéticos y garantizar que los costos de un ataque superen sus beneficios.

Además, el panorama global presenta desafíos adicionales debido a las tensiones geopolíticas, como los conflictos entre Rusia y Ucrania y entre Israel y Palestina, que han dado lugar a una nueva generación de malware conocidos como "wipers", diseñados para borrar información. Las redes de bots se mantienen en las redes durante períodos más largos, lo que dificulta su detección y eliminación.

Ramón Santoyo, un consultor especializado en banca electrónica, subraya que el panorama actual presenta una complejidad con riesgos económicos, sociales, geopolíticos y tecnológicos interconectados, lo que hace que la ciberseguridad sea aún más crítica. En este contexto, destaca la necesidad de inversión en tecnología, formación y colaboración. Se enfatiza que las instituciones financieras deben entender que la ciberseguridad no es un gasto, sino una inversión en su futuro, ya que implica proteger la integridad de sus sistemas, la confianza de sus clientes y la estabilidad de la economía nacional. Además, se señala que la ciberseguridad no se limita a la tecnología, sino que abarca procesos sólidos, organización, formación de recursos humanos y una gobernanza adecuada.

El consultor destaca que los eventos de ciberseguridad no solo tienen consecuencias económicas, sino que también pueden dañar la reputación de una organización y dar lugar a incumplimientos regulatorios, con sanciones y multas significativas. En ese sentido, la gestión proactiva de la ciberseguridad es esencial para evitar impactos negativos. Además, se enfatiza la importancia de involucrar a los consejeros y la alta dirección en la toma de decisiones estratégicas relacionadas con la ciberseguridad, ya que es uno de los mayores riesgos que enfrentan las instituciones financieras. La formación continua y la promoción de una cultura de ciberhigiene son esenciales para proteger a las organizaciones.

En resumen, la ciberseguridad es un tema que debe abordarse a nivel estratégico, y es responsabilidad del consejo de administración y de un comité de ciberseguridad. La inversión en ciberseguridad es fundamental para proteger el futuro de las instituciones financieras en la era digital actual.

La colaboración y la comunicación son elementos clave en una defensa efectiva, y se destaca la necesidad de compartir inteligencia de amenazas y aprender de incidentes anteriores.

SAT DETECTÓ CORREOS ELECTRÓNICOS Y SITIOS WEB APÓCRIFOS

El Servicio de Administración Tributaria (SAT) ha identificado la existencia de correos electrónicos y páginas web que se hacen pasar por la autoridad fiscal, y por lo tanto, insta a los contribuyentes a evitar caer en engaños con el fin de prevenir la usurpación de identidad.

El organismo federal de recaudación también ha observado la presencia de perfiles falsos relacionados con el SAT en redes sociales, así como en mensajes enviados a través de WhatsApp. Estos perfiles y mensajes falsos tienen como objetivo recopilar información fiscal, datos bancarios o números de seguridad social de los contribuyentes.

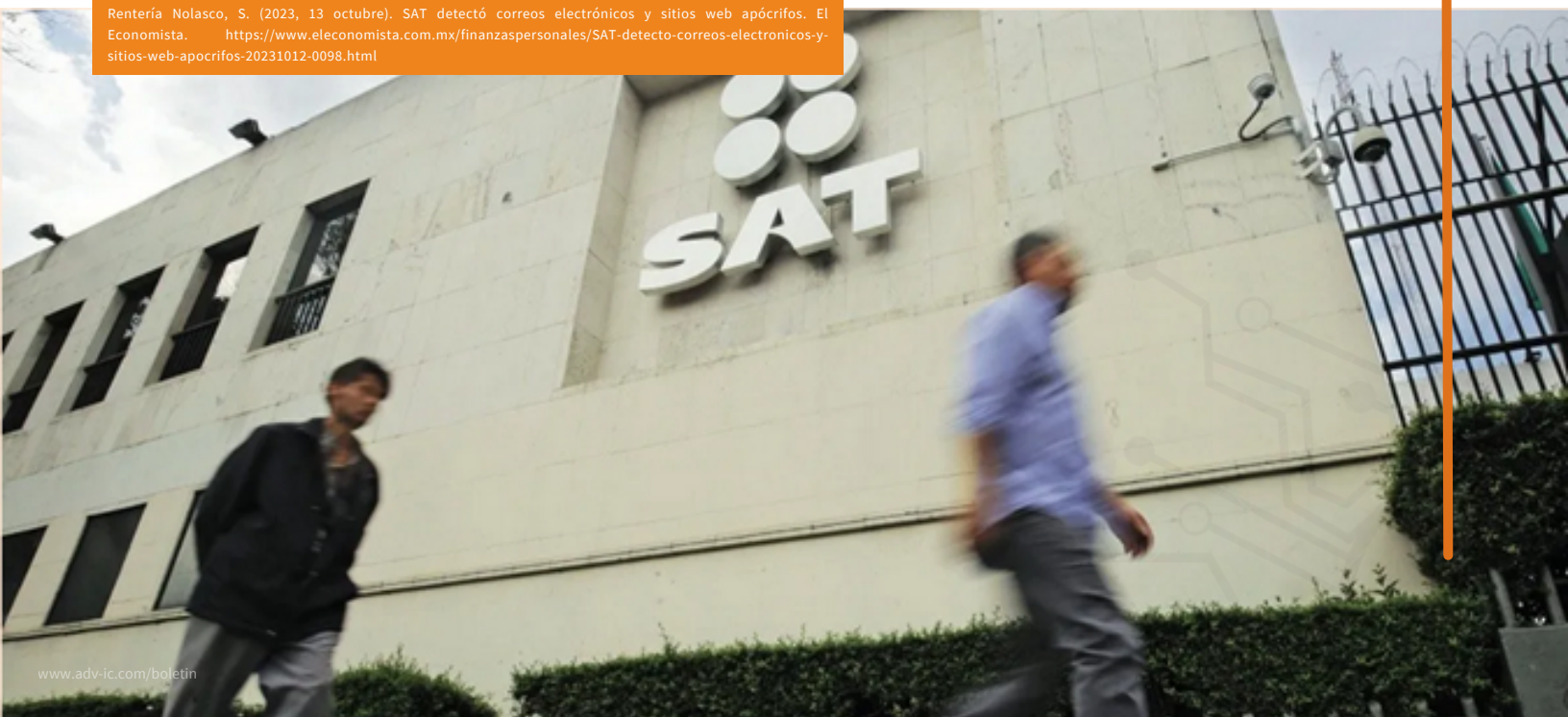
En este contexto, el SAT mencionó que "se han propagado en diversas redes sociales sitios web falsos con propósitos fraudulentos, destinados a suplantar la identidad de la entidad tributaria".

El SAT reafirma su compromiso con la ciberseguridad y subraya que dispone de sólidos mecanismos para prevenir hackeos o la sustracción de información que podría poner en peligro tanto la institución como los datos de los contribuyentes. Además, hace un llamado a los contribuyentes para que, en caso de detectar un sitio web falso, lo reporten a la dirección de correo electrónico denuncias@sat.gob.mx.

En adición, el SAT aclaró que su sitio web oficial no utiliza la terminación ".org", no realiza subastas y no vende bienes, productos, materiales, maquinaria pesada, camiones o vehículos particulares. Por otro lado, los medios de comunicación oficiales del SAT, a través de los cuales se proporcionan información sobre trámites, servicios y temas relevantes, se encuentran alojados en el portal web oficial del SAT.

En una situación relacionada, se ha observado que Petróleos Mexicanos (Pemex) también ha sido blanco de anuncios falsos por parte de estafadores que prometen ganancias de hasta 300,000 pesos por invertir desde 4,500 pesos en la empresa petrolera. Estos anuncios se han generado utilizando Inteligencia Artificial y cuentan con un video en el que el empresario Carlos Slim aparece invitando a las personas a realizar esta inversión ficticia.

Rentería Nolasco, S. (2023, 13 octubre). SAT detectó correos electrónicos y sitios web apócrifos. El Economista. https://www.eleconomista.com.mx/finanzaspersonales/SAT-detecto-correos-electronicos-y-sitios-web-apocrifos-20231012-0098.html



CNBV HACE LLAMADO A FINTECH PARA ATENDER RIESGOS

Estrada, S. (2023b, octubre 5). CNBV hace llamado a Fintech para atender riesgos. El Economista. https://www.eleconomista.com.mx/sectorfinanciero/CNBV-hace-llamado-a-fintech-para-atender-riesgos-20231004-0119.html

LA COMISIÓN NACIONAL BANCARIA Y DE VALORES (CNBV) HA EMITIDO UN LLAMADO A LAS INSTITUCIONES FINANCIERAS QUE OPERAN A TRAVÉS DE PLATAFORMAS TECNOLÓGICAS PARA QUE TOMEN EN CONSIDERACIÓN LOS RIESGOS ASOCIADOS CON LA OPERACIÓN MEDIANTE MEDIOS DIGITALES.

En el marco del Foro "Forjando futuros: Educación, salud e inclusión financiera" realizado en el Senado de la República, Esther Ramírez Bernabé, vicepresidenta de Supervisión de Banca de Desarrollo y Finanzas Populares de la CNBV, destacó que con la incursión de entidades digitales en el sector financiero, se han incrementado ciertos riesgos. Ramírez Bernabé reconoció que "han surgido riesgos emergentes, es decir, riesgos que anteriormente no habían sido ampliamente contemplados o explorados, pero que ahora son una preocupación con la que debemos lidiar".

Dada la evolución del sector financiero, la vicepresidenta de la CNBV señaló que las amenazas persisten en áreas como la ciberseguridad y el fraude, y también mencionó la identificación de riesgos relacionados con el cumplimiento regulatorio. Ramírez resaltó que "estos son tres riesgos emergentes a los que debemos hacer frente. Por lo tanto, aunque busquemos un crecimiento sostenible y avances financieros, también debemos hacerlo de manera responsable".

En ese sentido, la funcionaria instó a las instituciones de tecnología financiera a evolucionar con una cultura que promueva el cumplimiento regulatorio para abordar los riesgos previamente mencionados. "Desde este momento, debemos crecer con una mentalidad orientada al cumplimiento regulatorio, a la gestión integral de riesgos y dentro de un marco de control interno", enfatizó. Cabe mencionar que la CNBV actualmente supervisa a 5,211 entidades financieras, y en general, estos sectores cuentan con una sólida capitalización.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-46747	10/26/2023	Undisclosed requests may bypass configuration utility authentication	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-46747

Descripción: Allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-36434	10/10/2023	Windows IIS Server Elevation of Privilege Vulnerability	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-36434

Descripción: In a network-based attack, an attacker could brute force user account passwords to log in as that user. Microsoft encourages the use of strong passwords that are more difficult for an attacker to brute force. The attacker would be able to login as another user successfully.

TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-35349	10/10/2023	Microsoft Message Queuing Remote Code Execution Vulnerability	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-35349

Descripción: Successful exploitation of this vulnerability could allow an unauthenticated attacker to remotely execute code on the target server and Thunderbird.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5730	10/25/2023	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-5730

Descripción: Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.

TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5700	10/22/2023	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-5700

Descripción: Affected is an unknown function of the file /protocol/iscgwtunnel/uploadiscgwrouteconf.php. The manipulation of the argument GWLinkId leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-243138 is the identifier assigned to this vulnerability.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-4488	10/20/2023	The Dropbox Folder Share for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 1.9.7 via the editor-view.php file.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-4488

Descripción: This allows unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.

TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-39332	10/18/2023	Various `node:fs` functions allow specifying paths as either strings or `Uint8Array` objects. In Node.js environments, the `Buffer` class extends the `Uint8Array` class.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-39332

Descripción: Node.js prevents path traversal through strings (see CVE-2023-30584) and `Buffer` objects (see CVE-2023-32004), but not through non-`Buffer` `Uint8Array` objects. This is distinct from CVE-2023-32004 ([report 2038134](https://hackerone.com/reports/2038134)), which only referred to `Buffer` objects. However, the vulnerability follows the same pattern using `Uint8Array` instead of `Buffer`. Impacts: This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-38545	10/18/2023	This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-38545

Descripción: When curl is asked to pass along the host name to the SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that host name can be is 255 bytes. If the host name is detected to be longer, curl switches to local name resolving and instead passes on the resolved address only. Due to this bug, the local variable that means "let the host resolve the name" could get the wrong value during a slow SOCKS5 handshake, and contrary to the intention, copy the too long host name to the target buffer instead of copying just the resolved address there. The target buffer being a heap based buffer, and the host name coming from the URL that curl has been told to operate with.

TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2023

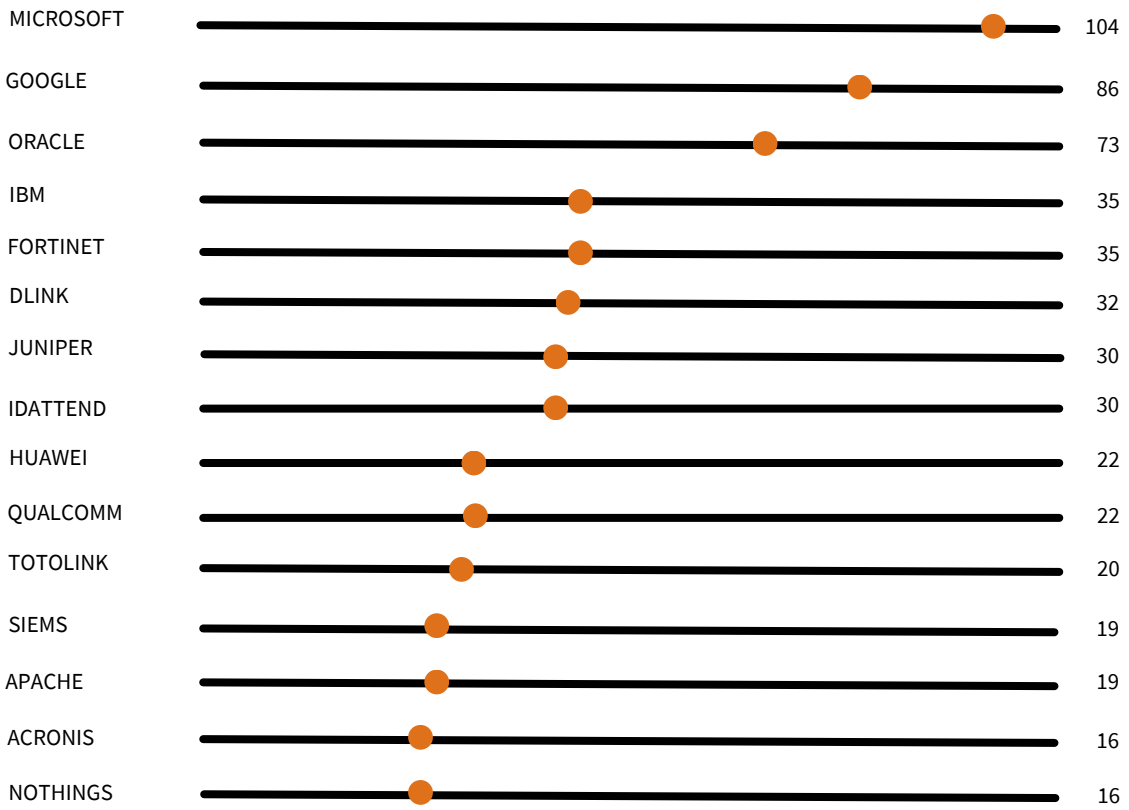
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-22069	10/17/2023	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core).	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-22069

Descripción: Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

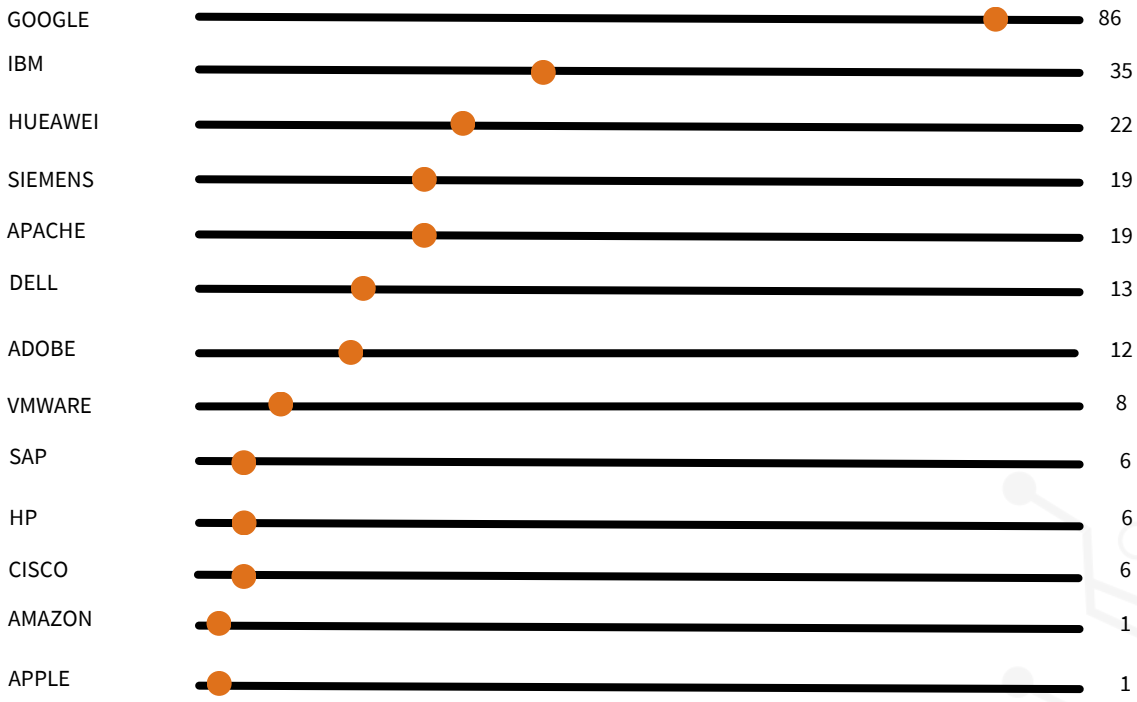
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-20198	10/16/2023	Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks.	CVSS v3.1:10 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-20198

Descripción: This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system. For steps to close the attack vector for this vulnerability, see the Recommendations section of this advisoryCisco will provide updates on the status of this investigation and when a software patch is available.

FABRICANTES CON VULNERABILIDADES RELEVANTES: OCTUBRE DE 2023



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: OCTUBRE DE 2023



CULTURA DE CIBERSEGURIDAD

INDICADORES DE COMPROMISO.

DEFINICIÓN.

Los Indicadores de Compromiso (IOCs, por sus siglas en inglés, Indicators of Compromise) son atributos o pistas específicas que indican la presencia de una brecha de seguridad o una actividad maliciosa en un sistema o red. Estos indicadores pueden variar en forma y tipo, y algunos ejemplos comunes de IOCs incluyen:

1. Direcciones IP maliciosas: Las direcciones IP que se han asociado previamente con actividades maliciosas, como servidores de comando y control.
2. Nombres de dominio sospechosos: Los nombres de dominio que se utilizan en ataques de phishing o que están vinculados a malware.
3. Hash de archivos maliciosos: Los valores hash (como MD5 o SHA-256) de archivos que se sabe que son malware.
4. Patrones de comportamiento sospechoso: Actividades inusuales en registros de eventos, como intentos de inicio de sesión fallidos o actividades de red inusuales.
5. Firmas de malware: Secuencias de bytes específicas que identifican la presencia de malware en un archivo o memoria.
6. Huellas dactilares de malware: Características únicas que permiten identificar ciertas variantes de malware.
7. Indicadores de redes comprometidas: Información relacionada con la infraestructura de red utilizada por un atacante, como direcciones IP, nombres de dominio y puertos.
8. Indicadores de phishing: URLs, direcciones de correo electrónico y contenido de phishing.
9. Cadenas de texto sospechosas: Secuencias de texto que pueden indicar la presencia de malware en un archivo o en el tráfico de red.
10. Indicadores de infiltración: Datos que sugieren que un atacante ha ganado acceso no autorizado a un sistema.

COMO FUNCIONA.

Hay algunos comunes que las organizaciones empresariales deberían conocer para detectarlos e investigarlos. A continuación, se exponen algunos indicadores de compromiso más comunes para que los recordemos:

1. Tráfico inusual de salida de la red

- Las anomalías en los patrones y volúmenes de tráfico de la red son uno de los signos más comunes de una brecha de seguridad.
- No obstante, mantener a los intrusos fuera de su red es cada vez más difícil. Algunos expertos afirman que podría ser más fácil supervisar el tráfico saliente en busca de posibles indicadores de compromiso.
- Cuando un intruso intenta extraer datos de su red o cuando un sistema infectado transmite información a un servidor de comando y control, se puede detectar en la red un inusual tráfico saliente.

2. Actividad de zonas geográficas ajenas

- Si, por ejemplo, toda la operación de su empresa tiene su sede en Los Ángeles (Estados Unidos), debería sorprenderse al ver que un usuario se conecta a su red desde otro lugar, especialmente desde otro país con mala reputación por la ciberdelincuencia a nivel internacional.

PASOS DE BÚSQUEDA DE AMENAZAS.

- Benjamin Caudill, consultor principal de Rhino Security, afirma que: «En cuanto a los indicios de brechas de datos, una de las partes más útiles que he encontrado son los registros que muestran una cuenta que se conecta desde múltiples IPs en un corto período de tiempo, particularmente cuando se combina con el etiquetado de geolocalización. La mayoría de las veces, esto es un síntoma de que un atacante utiliza un conjunto de credenciales vulneradas para entrar en sistemas confidenciales.»
- La vigilancia de las direcciones IP en la red y su procedencia es una forma sencilla de detectar los ciberataques antes de que puedan causar un daño real a su organización.

Múltiples conexiones a sus cuentas desde lugares inesperados podrían ser un buen indicador de compromiso

3. Actividad inexplicable en las cuentas de usuario con privilegios

- En los ciberataques complejos, como las amenazas persistentes avanzadas, un método común es comprometer cuentas de usuarios con pocos privilegios antes de escalar sus privilegios y autorizaciones o exponer el vector de ataque a cuentas con más privilegios.
- Cuando los operadores de seguridad observan un comportamiento sospechoso de las cuentas de usuarios con privilegios, esto puede ser evidencia de ataques internos o externos a los sistemas y a los datos de la organización.

4. Frecuentes fallos de autentificación

En los casos de apropiación de cuentas, los atacantes utilizan la automatización para autentificarse utilizando credenciales falsificadas. Un alto índice de intentos de autenticación podría indicar que alguien ha robado las credenciales y está intentando encontrar una cuenta que le dé acceso a la red.

5. Muchas solicitudes en archivos importantes

- Sin una cuenta con privilegios elevados, un atacante se ve obligado a explorar diferentes recursos y encontrar la vulnerabilidad adecuada para acceder a los archivos.
- Cuando los atacantes encuentran indicios de que un exploit puede tener éxito, suelen utilizar diferentes variaciones para lanzarlo.

6. Cambios de configuración sospechosos

Puede que ni siquiera lo sepamos, pero cambiar las configuraciones de los archivos, servidores y dispositivos podría dar al atacante una segunda entrada («backdoor») a la red. Los cambios también podrían añadir vulnerabilidades para que el malware las aproveche.

7. Indicadores de ataques DDoS (Denegación de Servicio Distribuida)

- Estos ataques se producen cuando un operador malintencionado intenta cerrar un servicio inundándolo de tráfico y peticiones desde una red de máquinas controladas, llamada botnet.
- Los DDoS se utilizan con frecuencia como cortinas de humo para camuflar otros ataques más dañinos.
- Las señales deDDoS: rendimiento lento de la red, indisponibilidad de los sitios web, fallo del cortafuegos, sistemas de back-end trabajando al máximo de su capacidad por razones desconocidas.

RIESGOS.

No tomar en cuenta los Indicadores de Compromiso (IOCs) en la ciberseguridad puede tener graves consecuencias para una organización o individuo. Aquí hay algunas de las posibles repercusiones:

1. Brecha de seguridad no detectada: Los IOCs actúan como señales de alerta temprana de actividades maliciosas. Si no se les presta atención, es probable que las brechas de seguridad pasen desapercibidas. Esto significa que los atacantes pueden continuar sus actividades y potencialmente causar daño significativo antes de ser detectados.
2. Pérdida de datos sensibles: La falta de detección de IOCs puede llevar a la exposición y la pérdida de datos sensibles o confidenciales. Esto puede tener un impacto significativo en la privacidad y la integridad de los datos, así como en la reputación de la organización.
3. Daño financiero: Las brechas de seguridad pueden resultar en costos financieros significativos, incluyendo la recuperación de sistemas, el costo de notificación y respuesta a incidentes, y posibles multas por incumplimiento de regulaciones de privacidad.
4. Daño a la reputación: Las organizaciones que no responden eficazmente a las amenazas cibernéticas pueden dañar su reputación y la confianza de sus clientes, socios y empleados.
5. Tiempo y recursos adicionales: No tomar en cuenta los IOCs puede llevar a una respuesta tardía y costosa a los incidentes de seguridad una vez que se descubren. La recuperación puede requerir más tiempo y recursos de lo que hubiera sido necesario si se hubieran detectado y abordado temprano.
6. Amenazas persistentes avanzadas (APTs): Las APTs suelen ser difíciles de detectar y pueden operar de manera sigilosa en un entorno durante largos períodos. Ignorar los IOCs puede permitir que estas amenazas avanzadas permanezcan activas durante mucho tiempo.
7. Incumplimiento de regulaciones y leyes de privacidad: Dependiendo de la industria y la ubicación geográfica, no atender adecuadamente los IOCs puede llevar al incumplimiento de regulaciones y leyes de privacidad, lo que puede resultar en sanciones legales y financieras.

No tomar en cuenta los IOCs puede tener graves consecuencias en términos de seguridad, privacidad, reputación y costos financieros. La detección temprana y la respuesta efectiva a las amenazas cibernéticas son fundamentales para mitigar riesgos y proteger sistemas, datos y la reputación de una organización. Por lo tanto, es esencial prestar atención a los IOCs y tomar medidas adecuadas en caso de detección.

UN CASO CONOCIDO.

Stuxnet es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares.

La compañía rusa de seguridad digital Kaspersky Lab describía a Stuxnet en una nota de prensa como "un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial". Kevin Hogan, un ejecutivo de Symantec, advirtió que el 60% de los ordenadores contaminados por el gusano se encuentran en Irán, sugiriendo que sus instalaciones industriales podrían ser su objetivo. Kaspersky concluye que los ataques sólo pudieron producirse "con el apoyo de una nación soberana", convirtiendo a Irán en el primer objetivo de una guerra cibernética real.

Nombre Técnico	Win32/Stuxnet.A.Down
Método de Propagación	Vía USB, Internet y mediante Vulnerabilidades del Sistema
Sistema Operativo Afectado	Microsoft Windows
Tipo	Gusano y Rootkit
Fecha de descubrimiento	junio de 2010

DE DONDE SE OBTIENEN.

Los Indicadores de Compromiso (IOCs) se obtienen de diversas fuentes y técnicas de investigación en el campo de la ciberseguridad. A continuación, se mencionan algunas de las fuentes y métodos comunes para obtener IOCs:

1. Análisis de malware: El análisis de muestras de malware, como virus, troyanos y gusanos, puede proporcionar información sobre los IOCs utilizados por los atacantes. Esto incluye direcciones IP, nombres de dominio, hashes de archivos y patrones de comportamiento malicioso.
2. Registros de eventos de seguridad: Los registros generados por sistemas de seguridad, servidores, dispositivos de red y aplicaciones pueden contener información valiosa sobre IOCs. Los registros pueden incluir intentos de inicio de sesión fallidos, actividades inusuales de usuarios y patrones de tráfico sospechoso.

3.Inteligencia de amenazas: Los servicios de inteligencia de amenazas recopilan y analizan datos de fuentes abiertas y privadas para identificar y compartir IOCs relacionados con amenazas cibernéticas conocidas.
4.Sensores y sondas de seguridad: Los sensores y sondas de seguridad en una red pueden identificar y registrar IOCs, como patrones de tráfico malicioso, conexiones a direcciones IP sospechosas y actividades inusuales en la red.
5.Detección de intrusiones: Los sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) pueden generar IOCs basados en reglas que identifican comportamientos maliciosos o patrones de ataque en el tráfico de red.
6.Análisis de registros de firewall: Los registros de cortafuegos (firewalls) pueden contener información sobre intentos de conexión no autorizados, direcciones IP bloqueadas y patrones de tráfico no permitido.
7.Correo electrónico y análisis de phishing: Los correos electrónicos de phishing y los sitios web maliciosos suelen incluir URLs y nombres de dominio que se pueden utilizar como IOCs.
8.Investigación forense: Durante una investigación forense de incidentes de seguridad, se pueden recopilar y analizar evidencia digital que incluye IOCs, como registros de sistema y registros de actividad de usuarios.
9.Colaboración en la comunidad de ciberseguridad: La comunidad de ciberseguridad comparte IOCs entre organizaciones, gobiernos y grupos de investigación. Esto permite una detección y respuesta más rápida y efectiva a las amenazas cibernéticas.
10.Análisis de redes sociales y foros de hackers: La observación de comunidades en línea de ciberdelincuentes y grupos de hacking a veces proporciona información sobre IOCs y tácticas utilizadas en ataques.

La obtención de IOCs y su análisis es esencial para detectar y mitigar amenazas cibernéticas. Los profesionales de la ciberseguridad utilizan herramientas y técnicas avanzadas para recopilar y utilizar IOCs en la protección de sistemas y redes contra ataques cibernéticos.

COMO SE INTEGRAN LOS INDICADORES DE COMPROMISO

Los Indicadores de Compromiso (IOCs) se integran en el proceso de ciberseguridad de una organización para fortalecer la detección y respuesta a amenazas cibernéticas. La integración efectiva de los IOCs implica la incorporación de estos indicadores en las herramientas y procesos utilizados para monitorear, analizar y proteger sistemas y redes. A continuación, se describe cómo se integran los IOCs:

1. Definición y recolección de IOCs: En primer lugar, los IOCs deben ser definidos y recolectados a partir de diversas fuentes, como análisis de malware, inteligencia de amenazas, registros de eventos de seguridad y otras fuentes relevantes.
2. Creación de reglas y firmas: Los IOCs se utilizan para crear reglas y firmas que permiten a las herramientas de seguridad identificar comportamientos maliciosos. Por ejemplo, se pueden crear reglas basadas en direcciones IP, nombres de dominio, hashes de archivos y patrones de tráfico.

3. Integración en sistemas de seguridad: Las reglas y firmas basadas en IOCs se integran en los sistemas de seguridad, como sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), firewalls, sistemas antivirus y soluciones de seguridad de endpoints.
4. Monitoreo y análisis en tiempo real: Los sistemas de seguridad monitorean en tiempo real el tráfico de red, el comportamiento del sistema y las actividades de usuarios en busca de coincidencias con los IOCs. Si se detecta una coincidencia, se genera una alerta o notificación.
5. Investigación y análisis de alertas: Los analistas de seguridad investigan las alertas generadas por las coincidencias con IOCs. Esto incluye la evaluación de la gravedad del incidente y la determinación de si se trata de una amenaza legítima.
6. Respuesta a incidentes: Si se confirma un incidente de seguridad, se implementan medidas de respuesta, que pueden incluir el aislamiento de sistemas comprometidos, la eliminación de malware y la corrección de vulnerabilidades.
7. Gestión de la base de datos de IOCs: Las organizaciones mantienen una base de datos de IOCs actualizada con información sobre los indicadores utilizados y sus detalles. Esto facilita la detección de futuras amenazas basadas en IOCs similares.
8. Intercambio de información: Las organizaciones comparten IOCs con otras organizaciones, la comunidad de ciberseguridad y agencias de inteligencia para mejorar la protección contra amenazas cibernéticas.
9. Automatización de la respuesta: En algunos casos, se implementa la automatización de la respuesta a incidentes basada en IOCs para responder de manera más rápida y efectiva a las amenazas.

CÓMO PUEDE AYUDAR ADV-IC

1. **Supervisión continua:** El SOC supervisa continuamente la infraestructura de TI y las redes de la organización en busca de actividades inusuales o maliciosas que puedan generar IOCs. Esto incluye la monitorización de registros de eventos de seguridad, tráfico de red y comportamiento del sistema.
2. **Detección temprana:** El SOC utiliza herramientas de seguridad avanzadas para identificar posibles amenazas basadas en IOCs. La detección temprana es clave para responder de manera proactiva a amenazas cibernéticas.
3. **Análisis y evaluación:** Los analistas de seguridad del SOC analizan las alertas generadas por las coincidencias con IOCs. Evalúan la gravedad del incidente, determinan la naturaleza de la amenaza y evalúan el impacto potencial en la organización.
4. **Investigación de incidentes:** Si se confirma un incidente de seguridad, el SOC lleva a cabo investigaciones más profundas para comprender cómo ocurrió, cuál fue el vector de ataque y qué sistemas o datos se vieron comprometidos.
5. **Gestión de la base de datos de IOCs:** El SOC mantiene y gestiona una base de datos de IOCs actualizada. Esto incluye la incorporación de nuevos IOCs a medida que se descubren y la actualización de las reglas de seguridad en función de esta información.
6. **Capacitación y concienciación:** El SOC proporciona capacitación y concienciación en materia de seguridad a empleados y otros miembros de la organización para ayudar a prevenir incidentes basados en IOCs.

REFERENCIAS

REFERENCIAS

- Popa, A. (2022, 2 marzo). 8 Tipos de indicadores de compromiso (IOC) y cómo reconocerlos - ATTACK Simulator. ATTACK Simulator. https://attacksimulator.es/blog/8-tipos-de-indicadores-de-compromiso-ioc-y-como-reconocerlos/
- Herraez, A. (2022, 25 noviembre). Indicadores de Compromiso (IOC): el termómetro de tus sistemas. Micromouse. https://www.micromouse.com/2022/11/24/indicadores-de-compromiso-ioc-el-termometro-de-tus-sistemas/
- colaboradores de Wikipedia. (2023, 16 septiembre). Stuxnet. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Stuxnet

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 81 2011 8604

contacto@adv-ic.com

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