BOLETÍN DE CIBERSEGURIDAD

SEPTIEMBRE 2023

ÍNDICE

NOTICIAS INTERNACIONALES

LA CORTE PENAL INTERNACIONAL REPORTA UN “INCIDENTE DE CIBERSEGURIDAD”

LA CORTE PENAL INTERNACIONAL DIJO EL MARTES QUE DETECTÓ “ACTIVIDAD ANÓMALA QUE AFECTA SUS SISTEMAS INFORMÁTICOS” LA SEMANA PASADA Y TOMÓ MEDIDAS URGENTES.

Associated Press & By Associated Press. (2023, 19 septiembre). La Corte Penal Internacional reporta un «incidente de ciberseguridad» - San DiEgo Union-Tribune en español. San Diego Union-Tribune en Español. https://www.sandiegouniontribune.com/en-espanol/noticias/story/2023-09-19/la-corte-penal☒internacional-reporta-un-incidente-de-ciberseguridad

CEl vocero de la corte, Fadi El Abdallah, dijo en un comunicado que “están en marcha medidas de respuesta y seguridad” con ayuda de las autoridades de Holanda, donde se encuentra su sede.

“En lo sucesivo, la corte aprovechará el trabajo en curso para reforzar su marco de ciberseguridad, que incluye acelerar su uso de la tecnología de la nube”, añadió.

La corte se negó a difundir más detalles de lo sucedido, pero dijo que a medida que “sigue analizando y mitigando el impacto de este incidente, da más prioridad a garantizar que continúa el trabajo de la corte”. La CPI, que tiene en marcha varias investigaciones de gran repercusión en distintos países del mundo, ha sido blanco de espionaje en el pasado.

El año pasado, una agencia de inteligencia holandesa dijo que frustró el intento de un espía ruso que usaba una identidad falsa brasileña de trabajar como pasante en la corte, que investiga denuncias de crímenes de guerra rusos en Ucrania y ha emitido una orden de arresto por crímenes de guerra contra el presidente Vladimir Putin, al que acusa de tener responsabilidad personal por el secuestro de niños en Ucrania.

Las autoridades holandesas no respondieron de inmediato a pedidos de declaraciones sobre el incidente.

EL AYUNTAMIENTO DE SEVILLA SUSPENDE TODOS LOS SERVICIOS TELEMÁTICOS POR UN SECUESTRO INFORMÁTICO: "NO SE NEGOCIARÁ"

Los hackers han reclamado hasta un millón y medio de dólares (1.396.642 euros) al gobierno municipal, aunque este ha asegurado que "en ningún caso negociará con ciberdelincuentes". Es el segundo ataque con éxito a la web municipal en tres años.

Todos los servicios se han visto afectados. Entre los más importantes para las gestiones ciudadanas se encuentran los de solicitud de cita previa y el pago de tributos (acaba de comenzar el segundo plazo para abonar el Impuesto de Bienes Inmuebles), que los funcionarios han pedido que se efectúe de forma presencial en las sucursales bancarias autorizadas. También los dispositivos de emergencias, como Policía Local y Bomberos, se han visto obligados a las anotaciones en papel para registrar y ordenar las actuaciones. Los atacantes calculan que el daño causado se eleva a cinco millones de euros.

El delegado de Transformación Digital, Juan Bueno, ha explicado que "los responsables técnicos del Ayuntamiento y personal externo especializado están trabajando de manera continua y conjunta para determinar el origen y alcance del ataque y poder establecer la normalidad lo antes posible". "Actuaremos con cautela para no cometer errores", ha matizado. La partida municipal para prevenir ciberataques fue en 2022 de 200.000 euros dentro del presupuesto global de 1.072 millones, precisan fuentes municipales del nuevo equipo de Gobierno.

El Centro Criptológico Nacional (CCN-CERT) y el Cuerpo Nacional de Policía han comenzado a investigar el secuestro y creen haber identificado el equipo desde el que se inició el ataque, del total de 4.000 ordenadores de que

Limón, R., Martín-Arroyo, J., Limón, R., Martín-Arroyo, J., Limón, R., & Martín-Arroyo, J. (2023, 6 septiembre). El Ayuntamiento de Sevilla suspende todos los servicios telemáticos por un secuestro informático: "No se negociará". El País. https://elpais.com/tecnologia/2023-09-06/el-ayuntamiento-de-sevilla-suspende-todos-los-servicios-telematicos-por-un-secuestro-informatico-no-se-negociara.html

dispone el Consistorio. Mientras, el Ayuntamiento, como medida preventiva, ha interrumpido todos los servicios "hasta conocer el alcance concreto del ciberataque". De momento, no hay constancia de que los datos personales de los ciudadanos hayan sido alterados por los piratas informáticos, según Bueno.

El ataque se ha realizado con LockBit, un programa de extorsión identificado en 2019 y conocido también como ABCD. Esta herramienta es una subclase de virus de cifrado para exigir un rescate a cambio de la descodificación de archivos y se centra, principalmente, en empresas e instituciones oficiales más que en particulares. El Ministerio de Interior alertó hace solo dos semanas de una "campaña de distribución masiva" de este virus.

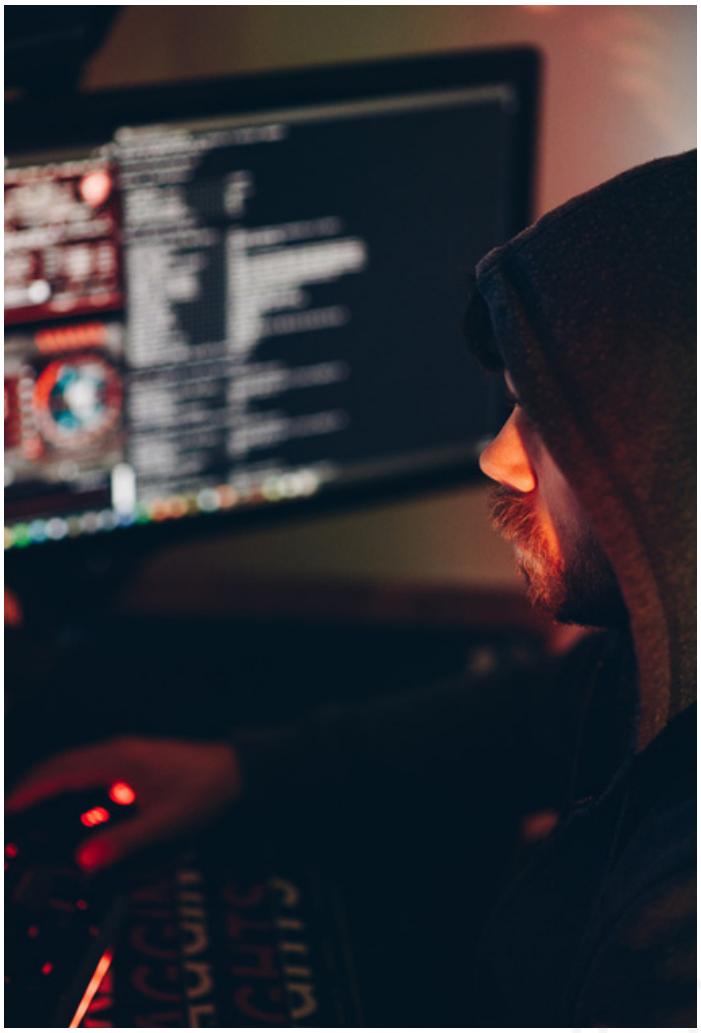
LockBit está dirigido por procesos automatizados diseñados previamente, a diferencia de los ataques que se ejecutan manualmente a través de la red. Una de sus características es su gran capacidad de propagación y su dificultad para ser localizado de forma inmediata. A veces, actúan durante semanas antes de ejecutar el ataque definitivo que causa la denegación de servicios.

DESARTICULACIÓN DE PIILOPUOTI: UN GOLPE GLOBAL A LA COMERCIALIZACIÓN ILÍCITA EN LA DARK WEB

OFICIALES DE LA LEY EN FINLANDIA, EN COLABORACIÓN CON EUROPOL, AUTORIDADES DE ALEMANIA, LITUANIA Y OTROS PAÍSES, ASÍ COMO LA FIRMA DE CIBERSEGURIDAD BITDEFENDER, HAN LOGRADO DESMANTELAR PIILOPUOTI, UN MERCADO ILÍCITO QUE OPERABA EN LA DARK WEB.

En una operación coordinada, oficiales de la ley en Finlandia, en colaboración con Europol, autoridades de Alemania, Lituania y otros países, así como la firma de ciberseguridad Bitdefender, han logrado desmantelar Piilopuoti, un mercado ilícito que operaba en la Dark Web. La plataforma se había erigido como un punto neurálgico para el contrabando y venta de drogas, dirigido principalmente al territorio finlandés.

Esta operación marca un hito en la lucha contra el ciberdelito y resalta la importancia de la colaboración internacional para enfrentar a aquellos que buscan el amparo del anonimato en la red para llevar a cabo actividades ilegales. La intervención en Piilopuoti envía un mensaje claro a los criminales en el ciberespacio: el alcance de la justicia va más allá de los recovecos oscuros de la web, y la unión de fuerzas globales trabaja incansablemente para garantizar la seguridad digital.



Operación contra Piilopuoti

Según informó la Aduana de Finlandia, Piilopuoti había estado activo en la Red Tor desde mayo de 2022, funcionando como un medio para el contrabando y venta de estupefacientes en Finlandia. La investigación criminal aún se encuentra en curso, y las autoridades han decidido no proporcionar más detalles en este momento. «Por el momento, las aduanas finlandesas y nuestros socios de cooperación internacional no facilitarán más información sobre el asunto», se informa en el comunicado de las Aduanas de Finlandia.

La operación contra Piilopuoti es la última de una serie de acciones destinadas a combatir plataformas de internet utilizadas para fines ilegales. El mes pasado, agencias de EE. UU. colaboraron con oficiales en Polonia para desmantelar la plataforma de alojamiento Lolek, y

Cyware. (s. f.). Cyber Security News Today | Articles on cyber security, malware attack updates | Cyware. Cyware Labs. https://cyware.com/cyber-dcr/daily-cybersecurity-roundup-august-25-2023-b07b

en abril, el mercado Genesis, que funcionaba como un centro para criminales vendiendo credenciales robadas y herramientas para su utilización, fue confiscado en una operación liderada por el FBI y más de una docena de socios internacionales.

El nuevo éxito de la operación contra Piilopuoti demuestra la creciente eficacia de los esfuerzos internacionales para frenar actividades ilegales en línea y envía un mensaje claro a aquellos que buscan perpetrar delitos en el anonimato del ciberespacio.

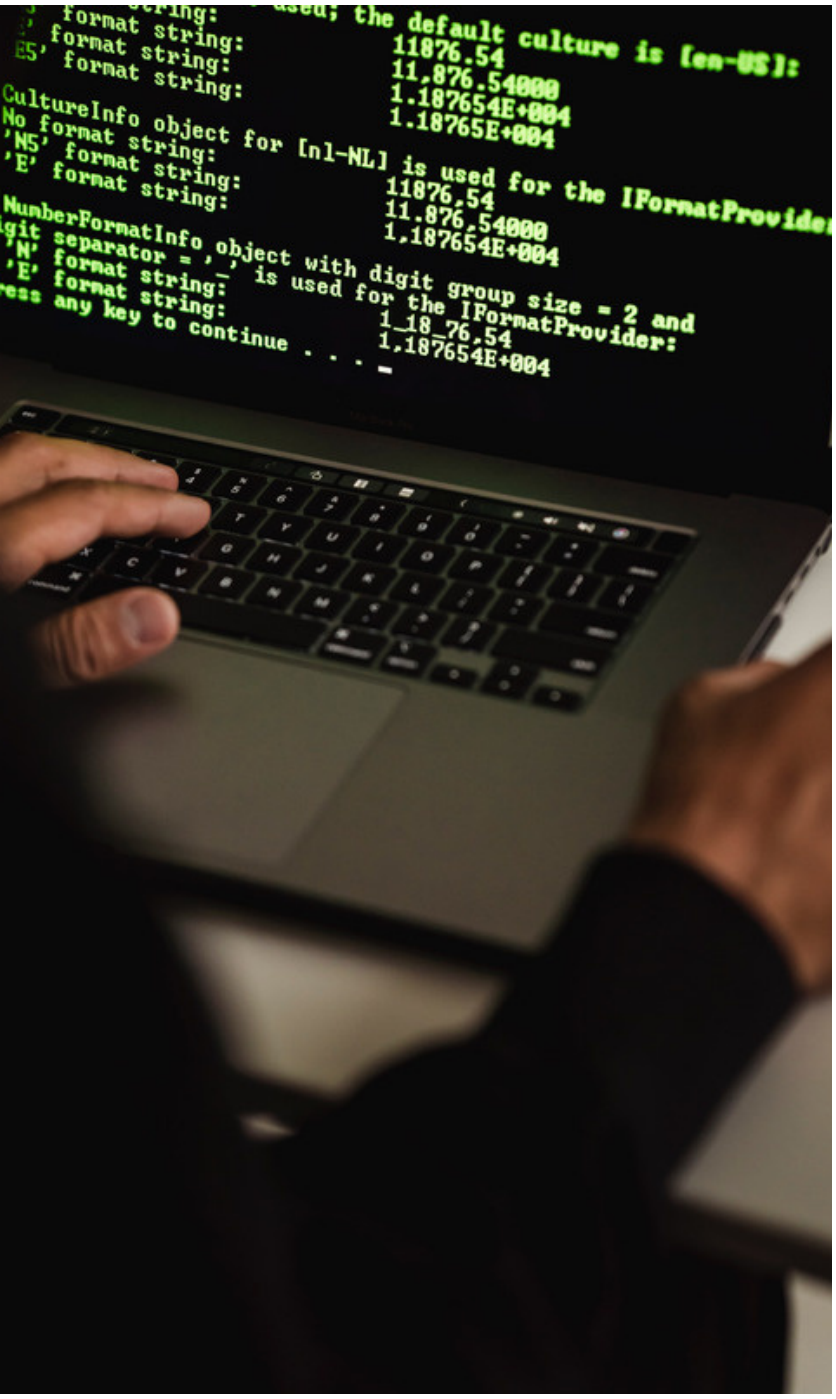
Colaboración de una empresa de ciberseguridad

Bitdefender, una reconocida firma de ciberseguridad participó en el operativo brindando asesoramiento técnico al grupo de investigación. Alexandru Catalin Cosoi, director senior de la unidad de investigación y forense de Bitdefender, destacó la importancia de la colaboración público-privada en este tipo de operaciones y advirtió que este éxito debería servir de llamada de atención para los criminales que creen erróneamente que están completamente protegidos por la Dark Web.

Nos complace descubrir que nuestra información ayudó en la actuación. Esta operación es un excelente ejemplo de cómo los sectores público y privado aúnan recursos y colaboran para desbaratar actividades ilegales en línea», declaró Cosoi.Según un estudio de Emsisoft, la campaña MOVEit del grupo de ransomware Cl0p ha afectado a casi 1,000 organizaciones y 60 millones de personas, con más del 80% de las entidades afectadas ubicadas en Estados Unidos.

Los actores de amenazas de ransomware están pasando menos tiempo en las redes comprometidas, con un tiempo de permanencia mediano que ha disminuido a cinco días en la primera mitad de 2023, según informó Sophos. También afirmó que los ataques de ransomware representaron el 68.75% de todos los ataques.

DESARTICULACIÓN DE PIILOPUOTI: UN GOLPE GLOBAL A LA COMERCIALIZACIÓN ILÍCITA EN LA DARK WEB

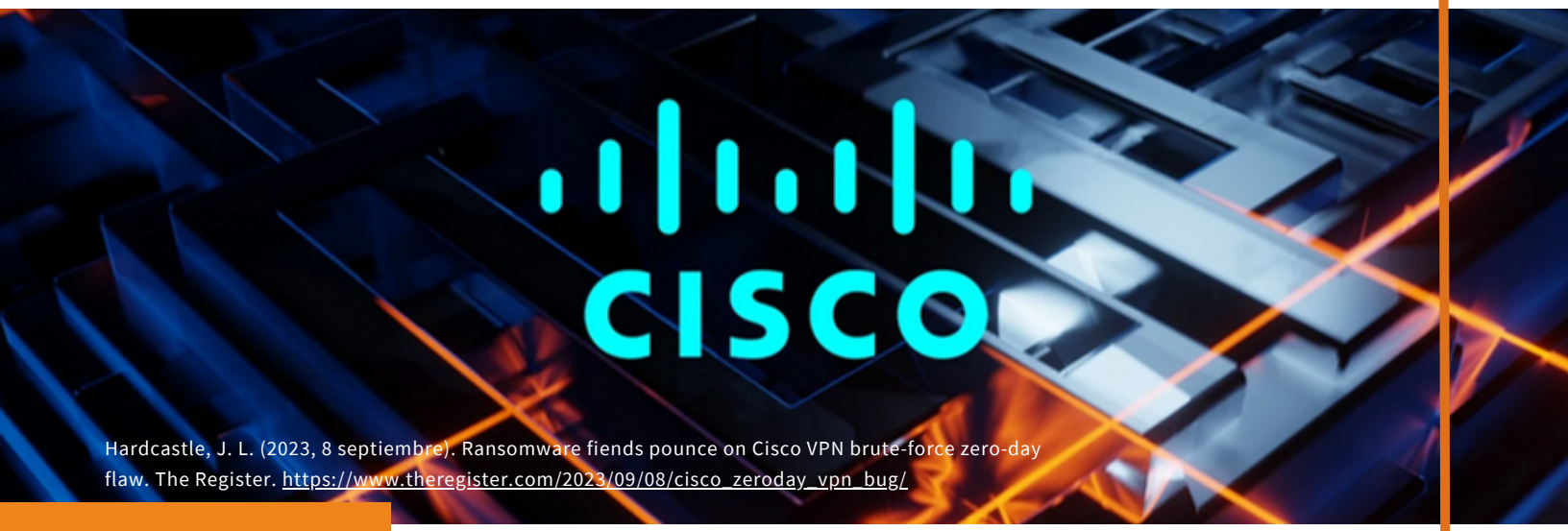


Los investigadores descubrieron una nueva cepa de ransomware llamada TZW, que se dirige a individuos y pequeñas empresas y exige rescates más bajos en comparación con otros ransomware. Esta cepa pertenece a la familia de ransomware Adhubllka. El NIST publicó un borrador de estándares de Criptografía Post-Cuántica (PQC) para uso global, con el objetivo de proteger a las organizaciones de posibles ciberataques habilitados por futuros ordenadores cuánticos. El HSCC CWG publicó una versión actualizada de la guía Mejores Prácticas de Compartir Información de Ciberseguridad de la Industria de la Salud que tiene como objetivo ayudar a las organizaciones de atención médica a establecer y mantener programas efectivos de intercambio de información sobre amenazas de ciberseguridad.

La plataforma de automatización de ciberseguridad GRC basada en SaaS, Cypago, recaudó $13 millones en financiamiento inicial y $2 millones en financiamiento de deuda de Entrée Capital, Axon Ventures y Jump Capital.

Malwarebytes anunció la adquisición del proveedor de soluciones de privacidad en línea Cyrus, con el objetivo de fortalecer su compromiso con la privacidad y dar a los usuarios más control sobre su información. Los términos del acuerdo no fueron revelados.

RANSOMWARE FIENDS SE ABALANZAN SOBRE EL FALLO DE DÍA CERO DE FUERZA BRUTA DE LA VPN DE CISCO



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/

Los creadores de ransomware se aprovechan de un fallo de día cero de Cisco en algunos de sus productos VPN. El gigante de las redes ha publicado una solución provisional para solucionar el problema mientras trabaja en un parche completo.

El fallo de gravedad media, identificado como CVE-2023-20269, se produce en la función VPN de acceso remoto de los paquetes de software Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD) de Cisco.

Básicamente, resulta que no hay nada que impida a los atacantes forzar su entrada en un dispositivo vulnerable, pasando por todas las combinaciones posibles o probables de nombre de usuario y contraseña. Si tienes configurada la autenticación multifactor y utilizas credenciales de inicio de sesión seguras, no deberías tener problemas. Cisco dice que todo se debe a una separación incorrecta de la autenticación, autorización y contabilidad entre la función de VPN remota, la gestión HTTPS y las funciones de VPN de sitio a sitio.

Como señaló el fabricante "Esta vulnerabilidad no permite a un atacante saltarse la autenticación. Para establecer con éxito una sesión VPN de acceso remoto, se requieren credenciales válidas, incluyendo un segundo factor válido si está configurada la autenticación multifactor (MFA)".

Por básico que sea, no parece disuadir a los ciberdelincuentes que, según Cisco, llevan intentando explotar esta vulnerabilidad in the wild desde agosto.

El software puede "permitir a un atacante remoto no autenticado llevar a cabo un ataque de fuerza bruta en un intento de identificar combinaciones válidas de nombre de usuario y contraseña", dice el informe. Hasta que Cisco desarrolle un parche completo para el software ASA y FTD, recomienda a los administradores implementar una serie de soluciones para protegerse de los ataques.

Para la situación de VPN SSL sin cliente, esto incluye configurar una política de acceso dinámico (DAP) para terminar el establecimiento del túnel VPN cuando se utiliza el perfil de conexión/grupo de túnel DefaultADMINGroup o DefaultL2LGroup.

Además, si no estás utilizando la política de grupo predeterminada (DfltGrpPolicy) para el acceso VPN remoto, y si no esperas que los usuarios de la base de datos de usuarios LOCAL establezcan túneles VPN de acceso remoto, es una buena idea establecer la opción vpn-simultaneous-logins a cero. Cisco proporciona instrucciones sobre cómo hacerlo en ambos escenarios.

Asegúrese de activar los registros para detectar los intentos de fuerza bruta antes de que se produzca una intrusión.

NOTICIAS NACIONALES

CAJA POPULAR MEXICANA SUFRIÓ ATAQUE CIBERNÉTICO; FUE UN SECUESTRO DE DATOS

LA COMISIÓN NACIONAL BANCARIA Y DE VALORES (CNBV) INFORMÓ QUE LAS INTERMITENCIAS EN LOS SERVICIOS DE CAJA POPULAR MEXICANA (CPM) SE DEBIERON A UN ATAQUE CIBERNÉTICO DE SECUESTRO DE DATOS (RANSOMWARE), SEGÚN LO QUE INDICÓ EL PASADO VIERNES.

La Comisión Nacional Bancaria y de Valores (CNBV) informó que las intermitencias en los servicios de Caja Popular Mexicana (CPM) se debieron a un ataque cibernético de secuestro de datos (ransomware), según lo que indicó el pasado viernes.

La Comisión Nacional Bancaria y de Valores (CNBV) informó que las intermitencias en los servicios de Caja Popular Mexicana (CPM) se debieron a un ataque cibernético de secuestro de datos (ransomware), según lo que indicó el pasado viernes.

Estrada, S. (2023, 4 septiembre). Caja Popular Mexicana sufrió ataque cibernético; fue un secuestro de datos. El Economista. https://www.eleconomista.com.mx/empresas/Caja-Popular-Mexicana-sufrio-ataque-cibernetico-fue-un-secuestro-de-datos-20230903-0037.html

El cierre de sucursales, el tiempo en que tardó la entidad en restablecer sus servicios y las operaciones que se detuvieron son indicadores de que diversos sistemas de CPM fueron secuestrados, de acuerdo con el experto en Hiram Camarillo, director ejecutivo de Seekurity, una firma consultora de seguridad informática.el saldo en el momento de la infección).

El secuestro sucedió desde el ransomware denominado “BlackCat”, de acuerdo con los registros del Banco de México (Banxico).

“La mayoría de los ransomware siempre se realizan para obtener un rescate, hay otro tipo que se llaman wipers, éstos llegan con la intención de eliminar y destruir todo. En este caso sí fue un secuestro, los atacantes pudieron darse cuenta de la cantidad de equipos de información, de los sistemas y que son una institución financiera que puede pagar un rescate”, señaló Camarillo.

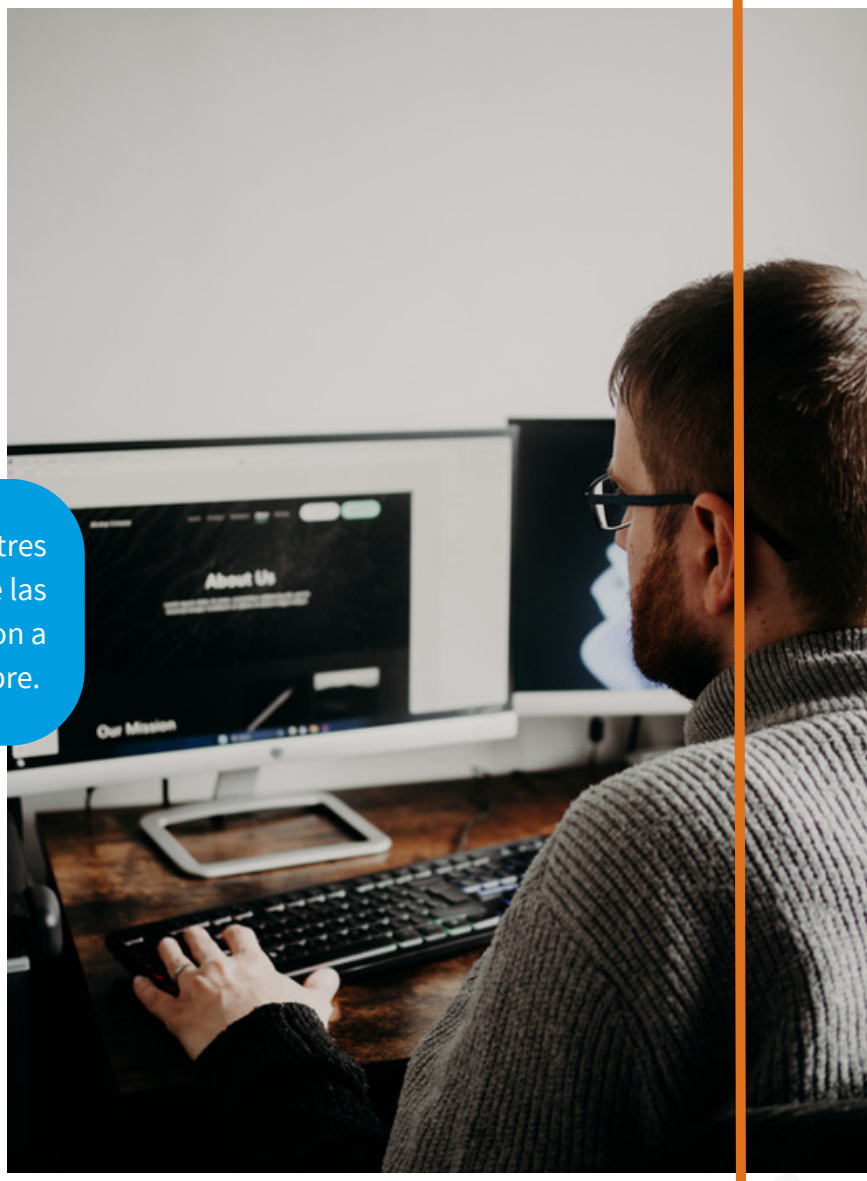
Este tipo de ataques generalmente son realizados por grupos, aunque ninguno se atribuyó la acción hasta el momento de la redacción de esta nota. También se desconoce qué tipo de datos y cuánta información se vio comprometida en el incidente.

Caja Popular Mexicana tiene 3 millones 370,196 asociados, quienes no pudieron realizar operaciones de forma física y en línea; sin embargo, Banxico indica que no existe afectación monetaria para los socios y aún se desconoce cuánto pudo costarle el incidente a la entidad.

CAJA POPULAR MEXICANA SUFRIÓ ATAQUE CIBERNÉTICO; FUE UN SECUESTRO DE DATOS

Fue alto el nivel de secuestro que tuvo la entidad, pudo haber llegado hasta el nivel de sistemas operativos de los equipos es posible que no tuvieran un nivel de seguridad madura o que no sea la adecuada", comentó Camarillo.

Según lo indicado por la CNBV, el viernes pasado, aún continúa realizando labores de contención para mantener las afectaciones al mínimo y se están realizando las acciones necesarias para el restablecimiento total de los servicios de CPM.



En lo que va del 2023 Banxico ha registrado otros tres incidentes en materia de ciberseguridad de las instituciones financieras, todos ellos afectaron a bancos, de los que no se revela el nombre.

SENADO URGE EN LEGISLAR EN MATERIA DE CIBERSEGURIDAD ANTE AVANCE DE IA

Durante la mesa de discusión "Ciberseguridad y Gestión de Riesgos" organizada por la Alianza Nacional de Inteligencia Artificial (ANIA), enfatizaron que existen desafíos significativos, tanto tecnológicos como legales, para proteger los datos personales de los usuarios de Internet.

Senadores, académicos y expertos en el campo de la inteligencia artificial coincidieron en la importancia de fortalecer la legislación en relación con la ciberseguridad, la protección de datos personales en Internet y la gestión de riesgos, dada la rápida evolución de la tecnología.

También señalaron que los sistemas normativos en México y en todo el mundo suelen ser reactivos, es decir, responden a los problemas después de que surgen. Sin embargo, en el ámbito digital, todo cambia rápidamente, lo que requiere un cambio hacia leyes proactivas.

Explicaron que, aunque las leyes existentes pueden necesitar actualizaciones para abordar las necesidades actuales, el marco de derechos humanos que debe protegerse en el entorno digital ya está establecido en la Constitución. Las garantías que existen en el mundo analógico deben preservarse de la misma manera en el mundo digital.

La senadora Alejandra Lagunes Soto del Partido Verde resaltó que uno de los aspectos más críticos de la inteligencia artificial es la ciberseguridad, ya que es fundamental para proteger la infraestructura y evitar el tráfico no autorizado de datos personales en Internet. El organizador del evento anunció que las opiniones expresadas durante el foro se tendrán en cuenta para fortalecer la iniciativa destinada a regular el uso de la inteligencia artificial en nuestro país.

El senador Gustavo Madero Muñoz del Grupo Plural señaló la necesidad de herramientas para combatir nuevos tipos de delitos impulsados por la inteligencia artificial, especialmente cuando ocurren en otros países con diferentes jurisdicciones legales. También destacó la urgencia de examinar la legislación de otros países y adaptarla al contexto mexicano, ya que las tecnologías pueden proporcionar medios para ocultar la identidad de los ciberdelincuentes.

Mientras tanto, Javier Joaquín López Casarín, presidente de la Comisión de Ciencia, Tecnología e Innovación de la Cámara de Diputados, afirmó que el mundo digital tiene un impacto diario en nuestras vidas. Por lo tanto, los legisladores tienen el deber de situar a nuestro país a la vanguardia en este campo. También destacó que el Parlamento mexicano está dando ejemplo a nivel mundial al fomentar la participación ciudadana en la regulación de la inteligencia artificial y las tecnologías en constante evolución, afirmando que "somos pioneros" en este sentido.

Arellano, S. (2023, 22 septiembre). Senado urge en legislar en materia de ciberseguridad ante avance de IA. Grupo Milenio. https://www.milenio.com/politica/senado-llaman-a-legislar-en-materia-de-ciberseguridad

REPORTAN HACKEO A SEDENA POR EL GRUPO INTERNACIONAL DENOMINADO “GUACAMAYA”

Web, C. 2. (2022). Reportan hackeo a Sedena por el grupo internacional denominado “Guacamaya”. NOTICIAS | Capital 21. https://www.capital21.cdmx.gob.mx/noticias/?p=33434

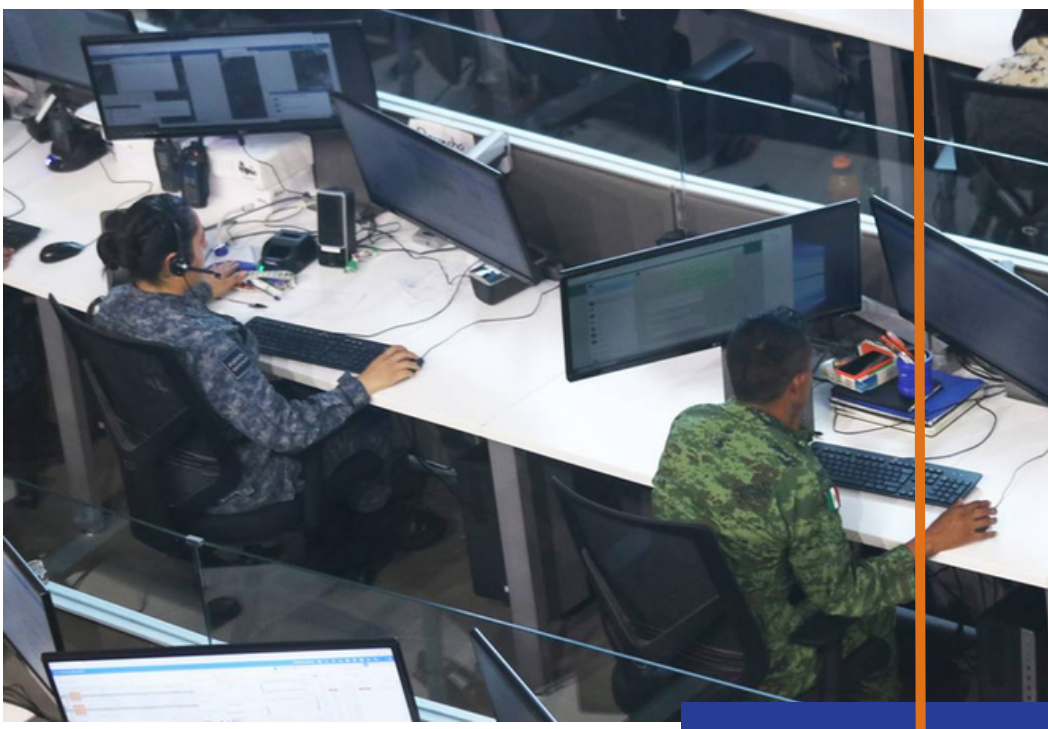
LA NOCHE DE ESTE JUEVES SE INFORMÓ QUE EL GOBIERNO DE MÉXICO EXPERIMENTÓ UN ATAQUE MASIVO POR PARTE DEL GRUPO INTERNACIONAL DE ACTIVISTAS CONOCIDO COMO "GUACAMAYA".

Según la información proporcionada por el periodista Carlos Loret de Mola en la plataforma de Latinus, un medio de comunicación privado que ha sido crítico con el gobierno del presidente Andrés Manuel López Obrador, este grupo de hackers habría logrado vulnerar el sistema informático de la Secretaría de la Defensa Nacional (Sedena).

De acuerdo con Loret de Mola, este incidente constituye el mayor ciberataque en la historia del país, ya que habría resultado en la exposición de miles de documentos confidenciales del gobierno federal, abarcando el período desde 2016 hasta septiembre de 2022. Se estima que los hackers accedieron a seis terabytes de material.

El periodista también informó que entre la información comprometida se encuentran supuestos detalles sobre la salud del presidente López Obrador, quien habría enfrentado complicaciones médicas en Palenque, Chiapas, el 2 de enero. Esto habría llevado a su traslado en una ambulancia aérea del Ejército al Hospital Central Militar de la Ciudad de México, siendo diagnosticado con angina inestable de alto riesgo, una condición cardíaca que puede desencadenar infartos. Además, se menciona que una semana después se anunció que el presidente tenía Covid-19.

El comunicador también indicó que hay información relacionada con el operativo en el que fue capturado y luego liberado Ovidio Guzmán, hijo de Joaquín "El Chapo" Guzmán Loera, hecho conocido como el



Culiacanazo', que tuvo lugar el 17 de octubre de 2019. Según Loret de Mola, esta información incluye detalles sobre los delitos imputados a Ovidio Guzmán en Estados Unidos.

Además, se mencionan supuestas diferencias entre los líderes de la Defensa Nacional y la Secretaría de la Marina (Semar), así como preocupaciones sobre la seguridad en las aduanas. El periodista destaca que esto revela el considerable poder y mando del Ejército en el actual gobierno.

En cuanto a "Guacamaya", se trata de un grupo de activistas de origen centroamericano que se identifica como defensores de la naturaleza. El nombre del grupo se inspira en el ave guacamaya, nativa de América Central y del Sur, como símbolo ambientalista. Según Latinus, su objetivo principal ha sido exponer información de ejércitos latinoamericanos, incluyendo el de Chile, El Salvador, Perú, Colombia y México. Los ataques de este grupo se han centrado en empresas mineras y petroleras, así como en fuerzas policiales y agencias reguladoras de la región.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5201	09/29/2023	The OpenHook plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 4.3.0 via the 'php' shortcode.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-3162

Descripción: This allows authenticated attackers with subscriber-level permissions or above, to execute code on the server. This requires the [php] shortcode setting to be enabled on the vulnerable site.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-43192	09/27/2023	SQL injection can exist in a newly created part of the JFinalcms background, and the parameters submitted by users are not filtered.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-43192

Descripción: As a result, special characters in parameters destroy the original logic of SQL statements. Attackers can use this vulnerability to execute any SQL statement.

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5176	09/27/2023	Memory safety bugs present in Firefox 117, Firefox ESR 115.2, and Thunderbird 115.2.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-5176

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 < 118, Firefox ESR < 115.3, and Thunderbird < 115.3.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-41320	09/27/2023	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. UI layout preferences management can be hijacked to lead to SQL injection.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-41320

Descripción: This injection can be use to takeover an administrator account. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-39347	09/27/2023	Cilium is a networking, observability, and security solution with an eBPF-based dataplane.	CVSS v3.1:9.0 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-39347

Descripción: An attacker with the ability to update pod labels can cause Cilium to apply incorrect network policies. This issue arises due to the fact that on pod update, Cilium incorrectly uses user-provided pod labels to select the policies which apply to the workload in question. This can affect Cilium network policies that use the namespace, service account or cluster constructs to restrict traffic, Cilium clusterwide network policies that use Cilium namespace labels to select the Pod and Kubernetes network policies.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-4521	09/25/2023	The Import XML and RSS Feeds WordPress plugin before 2.1.5 contains a web shell, allowing unauthenticated attackers to perform RCE.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-4521

Descripción: The plugin/vendor was not compromised and the files are the result of running a PoC for a previously reported issue (https://wpscan.com/vulnerability/d4220025-2272-4d5f-9703-4b2ac4a51c42) and not deleting the created files when releasing the new version.

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5143	09/24/2023	A vulnerability, which was classified as critical, has been found in D-Link DAR-7000 up to 20151231.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-5143

Descripción: This issue affects some unknown processing of the file /log/webmailattach.php. The manipulation of the argument table_name leads to an unknown weakness. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240239. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-1260	09/23/2023	An authentication bypass vulnerability was discovered in kube-apiserver.	CVSS v3.1:9.1[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-1260

Descripción: This issue could allow a remote, authenticated attacker who has been given permissions "update, patch" the "pods/ephemeralcontainers" subresource beyond what the default is. They would then need to create a new pod or patch one that they already have access to. This might allow evasion of SCC admission restrictions, thereby gaining control of a privileged pod.

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2023

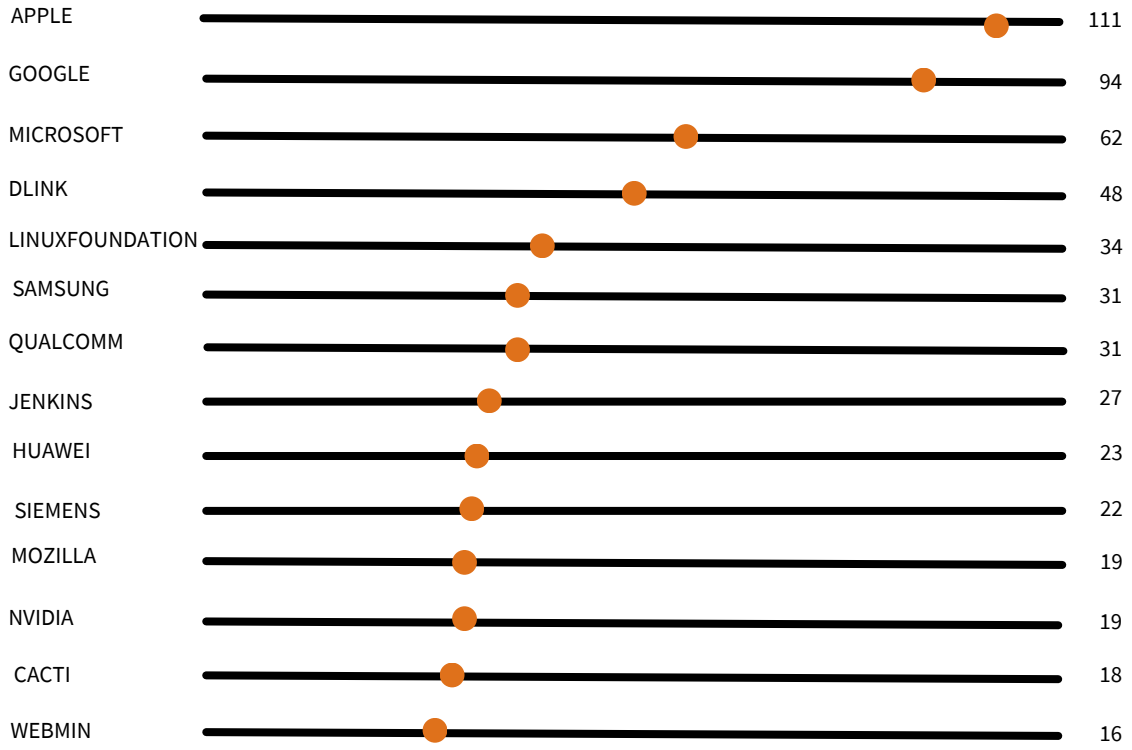
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-42798	09/22/2023	AutomataCI is a template git repository equipped with a native built-in semi-autonomous CI tools.	CVSS v3.1:9.1[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-42798

Descripción: An issue in versions 1.4.1 and below can let a release job reset the git root repository to the first commit. Version 1.5.0 has a patch for this issue. As a workaround, make sure the `PROJECT_PATH_RELEASE` (e.g. `releases/`) directory is manually and actually `git cloned` properly, making it a different git repostiory from the root git repository.

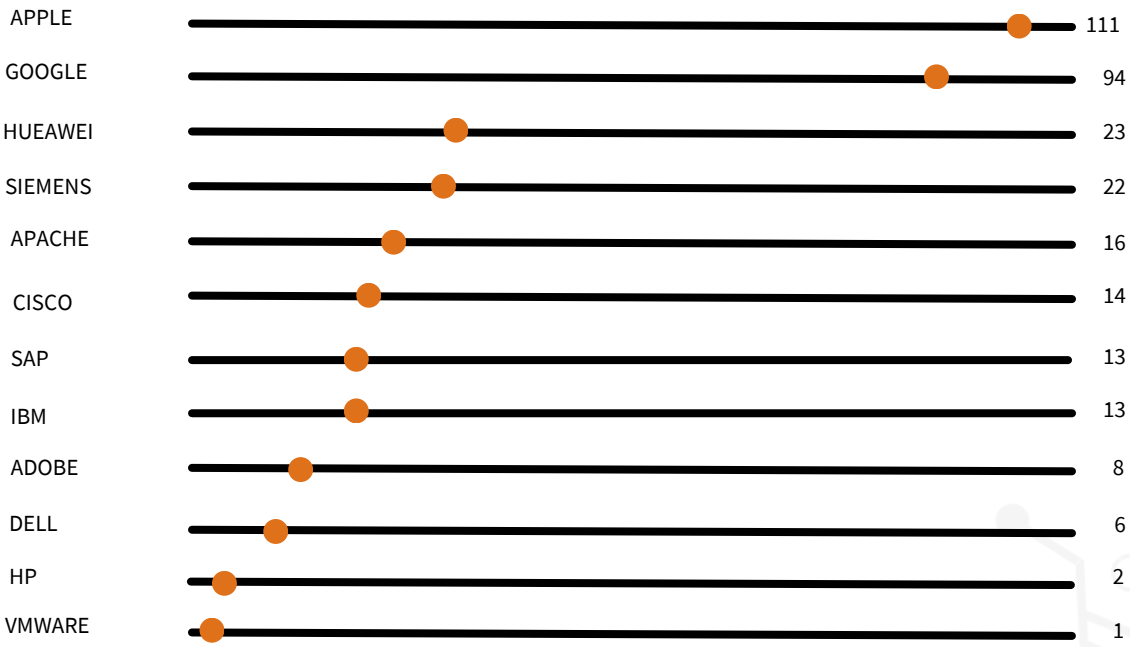
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-42464	09/20/2023	A Type Confusion vulnerability was found in the Spotlight RPC functions in afpd in Netatalk 3.1.x before 3.1.17.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-42464

Descripción: When parsing Spotlight RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the underlying protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a malicious actor may be able to fully control the value of the pointer and theoretically achieve Remote Code Execution on the host. This issue is similar to CVE-2023-34967.

FABRICANTES CON VULNERABILIDADES RELEVANTES: SEPTIEMBRE DE 2023



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: SEPTIEMBRE DE 2023



CULTURA DE CIBERSEGURIDAD

THREAT HUNTING

¿QUÉ ES?

Es la búsqueda activa de amenazas potenciales que pongan en riesgo la seguridad de una red cibernética, por lo que es un componente esencial de cualquier estrategia de defensa.

La búsqueda de amenazas es cada vez más importante a medida que las empresas buscan mantenerse a la vanguardia de las últimas amenazas cibernéticas y responder rápidamente a cualquier ataque potencial.

METODOLOGÍAS DE BÚSQUEDA DE AMENAZAS.

Los cazadores de amenazas asumen que los adversarios ya están en el sistema e inician una investigación para encontrar un comportamiento inusual que pueda indicar la presencia de actividad maliciosa.

1. Investigación basada en hipótesis

Las investigaciones basadas en hipótesis a menudo se desencadenan por una nueva amenaza que se ha identificado a través de un gran conjunto de datos de ataque de crowdsourcing, lo que brinda información sobre las últimas tácticas, técnicas y procedimientos (TTP) de los atacantes.

2. Investigación basada en indicadores conocidos de compromiso o indicadores de ataque.

Este enfoque de búsqueda de amenazas implica aprovechar la inteligencia táctica de amenazas para catalogar IOC y IOA conocidos asociados con nuevas amenazas

3. Análisis avanzado e investigaciones de aprendizaje automático.

El tercer enfoque combina un potente análisis de datos y aprendizaje automático para examinar una gran cantidad de información con el fin de detectar irregularidades que puedan sugerir una posible actividad maliciosa.

PASOS DE BÚSQUEDA DE AMENAZAS.

Paso 1: El disparador

Un disparador apunta a los cazadores de amenazas a un sistema o área específica de la red para una mayor investigación cuando las herramientas de detección avanzadas identifican acciones inusuales que pueden indicar actividad maliciosa.

Paso 2: Investigación

Durante la fase de investigación, el cazador de amenazas utiliza tecnología como EDR (Endpoint Detection and Response) para profundizar en el posible compromiso malicioso de un sistema.

Paso 3: Resolución

La fase de resolución implica comunicar inteligencia de actividad maliciosa relevante a los equipos de operaciones y seguridad para que puedan responder al incidente y mitigar las amenazas.

¿DÓNDE ENCAJA LA CAZA DE AMENAZAS?

La búsqueda de amenazas es altamente complementaria al proceso estándar de detección, respuesta y corrección de incidentes.

REFERENCIAS

REFERENCIAS

- Durán, M. (2023, 16 mayo). Threat hunting: qué es hunting en ciberseguridad y cómo funciona. HubSpot. https://blog.hubspot.es/website/hunting-ciberseguridad

- CrowdStrike. (2023, 9 agosto). What is cyber threat hunting? [Proactive Guide] - CrowdStrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 55 6178 9397

contacto@adv-ic.com

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