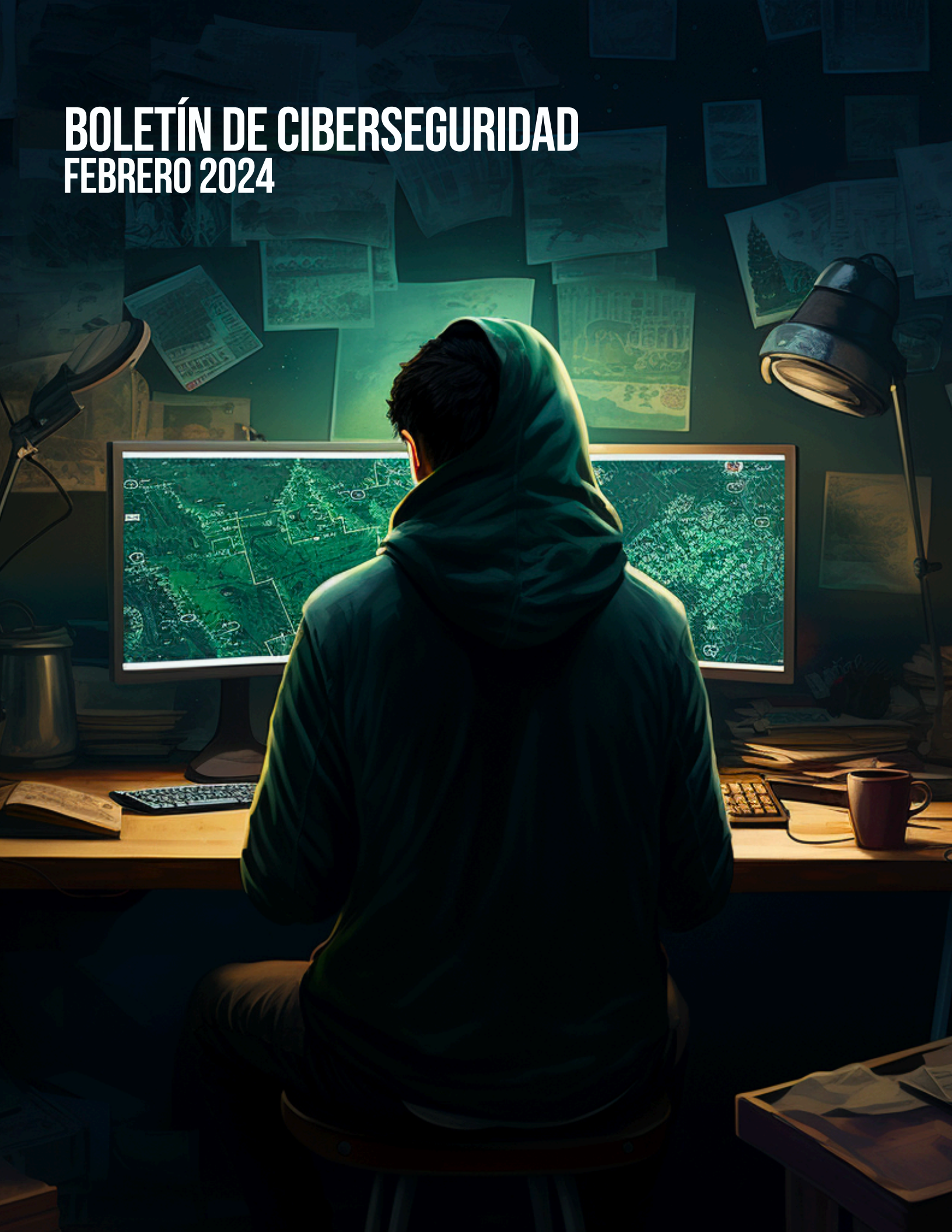
BOLETÍN DE CIBERSEGURIDAD
FEBRERO 2024



ÍNDICE

NOTICIAS INTERNACIONALES

EL GOBIERNO DE EE. UU. DESMANTELA UNA BOTNET VINCULADA A RUSIA DEDICADA AL CIBERESPIONAJE.

GOBIERNO DE LOS ESTADOS UNIDOS DERRIBÓ UNA BOTNET DE CIENTOS DE ENRUTADORES DE PEQUEÑAS OFICINAS Y OFICINAS DOMÉSTICAS EN EL PAÍS UTILIZADOS POR EL ATACANTE APT28 VINCULADO A RUSIA PARA OCULTAR SUS ACTIVIDADES MALICIOSAS, SEGÚN EL INFORME.

The Hacker News. (s. f.). U.S. Government Disrupts Russia-Linked Botnet Engaged in Cyber Espionage. https://thehackernews.com/2024/02/us-government-disrupts-russian-linked.html

"Estas actividades criminales incluyen campañas de phishing a gran escala y credenciales similares dirigidas a los intereses de inteligencia de las autoridades rusas, como los gobiernos de Estados Unidos y extranjeros, así como de organizaciones militares, de seguridad y corporativas", dijo el Departamento de Justicia de Estados Unidos en un comunicado.

Se cree que APT28, que también se conoce con los alias BlueDelta, Fancy Bear, Fighting Ursa, Forest Blizzard (anteriormente Strontium), FROZENLAKE, Iron Twilight, Pawn Storm, Sednit, Sofacy y TA422, está vinculado a la Unidad 61652 de la Dirección General de Rusia. Unidad de Estado Mayor (GRU). Se cree que ha estado activo desde al menos 2007.

Los atacantes se basaron en MooBot, una botnet basada en Mirai que utilizaba enrutadores fabricados por Ubiquiti y los integraba en una red de dispositivos que podían modificarse para actuar como servidores proxy, según documentos judiciales. Reenvíe tráfico malicioso mientras protege su dirección IP real.

El Departamento de Justicia dijo que la botnet permitió a los actores de amenazas enmascarar su verdadera ubicación y recopilar credenciales y hashes de NT LAN Manager (NTLM) v2 utilizando scripts personalizados, así como alojar páginas de inicio de phishing y otras herramientas personalizadas de piratería de fuerza bruta. Roba contraseñas de usuarios de enrutadores y propaga el malware MooBot a otros dispositivos.

En una declaración redactada presentada ante el FBI, la agencia dijo que MooBot utilizó enrutadores Ubiquiti vulnerables y disponibles públicamente utilizando credenciales estándar e implantó malware SSH, este proporcionó acceso remoto constante al dispositivo.

SOPHOS PARTNER CARE ES UN NUEVO SERVICIO DE ATENCIÓN PERSONALIZADA PARA SOCIOS CORPORATIVOS QUE NOS LO PRESENTARON EN MUYCANAL

SOPHOS PARTNER CARE, NUEVO SERVICIO DEL FABRICANTE DE CIBERSEGURIDAD.

Como resultado, los proveedores de ciberseguridad han ampliado su ecosistema para satisfacer todas sus necesidades de seguridad gestionadas.

Sophos Partner Care ofrece un único punto de contacto para cotizaciones, exploración de portales de socios, preguntas sobre licencias, solicitudes de no reventa (NFR) y más. Con este alto nivel de servicio, los socios que trabajan con pequeñas y medianas empresas pueden aumentar la productividad y aumentar la rentabilidad.

El servicio es parte de su programa global de socios y está diseñado para acelerar los tiempos de respuesta para los socios de Sophos y proveedores de servicios gestionados (MSP) que necesitan ayuda con tareas administrativas y operativas. Con este enfoque, los libera para centrarse en las ventas y la protección del cliente utilizando la tecnología del fabricante.

«Basándonos en nuestras décadas de experiencia apoyando con éxito a los partners que venden a pequeñas y medianas empresas, sabemos que los problemas administrativos y operativos restan un tiempo valioso, necesario para establecer relaciones con los clientes, buscar otros potenciales y cerrar nuevos acuerdos comerciales. Partner Care refuerza la estrategia a largo plazo de Sophos de ser ‘channel-best’, centrada en nuestro compromiso con proporcionar a los partners oportunidades de ingresos y rentabilidad óptimas y sin conflicto, formación especializada, soporte y soluciones de seguridad avanzadas que defienden a los clientes de las violaciones de datos, del ransomware y de otros ciberataques debilitantes”, afirma la vicepresidenta senior de canales globales y ventas a pequeñas empresas de Sophos, Kendra Krause.

Redaccion. (2024, 28 febrero). Sophos Partner Care, nuevo servicio del fabricante de ciberseguridad - MuyPymes. MuyPymes. https://www.muypymes.com/2024/02/28/sophos-partner-care-servicio-fabricante-ciberseguridad

HACKERS CHINOS APROVECHAN LAS FALLAS DE IVANTI VPN PARA IMPLEMENTAR NUEVO MALWARE.

AL MENOS DOS PRESUNTOS GRUPOS DE CIBERESPIONAJE VINCULADOS A CHINA, CONOCIDOS COMO UNC5325 Y UNC3886, HAN SIDO ACUSADOS DE EXPLOTAR VULNERABILIDADES DE SEGURIDAD EN LOS DISPOSITIVOS IVANTI CONNECT SECURE VPN.

Mandiant dijo que UNC5325 utilizó CVE-2024-21893 para difundir una nueva familia de malware llamada LITTLELAMB.WOOLTEA, PITSTOP, PITDOG, PITJET y PITHOOK e intentó mantener un acceso constante a los dispositivos infectados.

Google Threat Intelligence estima con confianza media que UNC5325 está relacionado con UNC3886 porque el código fuente de LITTLELAMB.WOOLTEA y PITHOOK se superpone con este último malware. Actualmente, no está claro qué información se accedió en el incidente.

En particular, UNC3886 ha aprovechado las vulnerabilidades de día cero de las soluciones Fortinet y VMware para implementar varios implantes como VIRTUALPITA, VIRTUALPIE, THINCRUST y CASTLETAP.

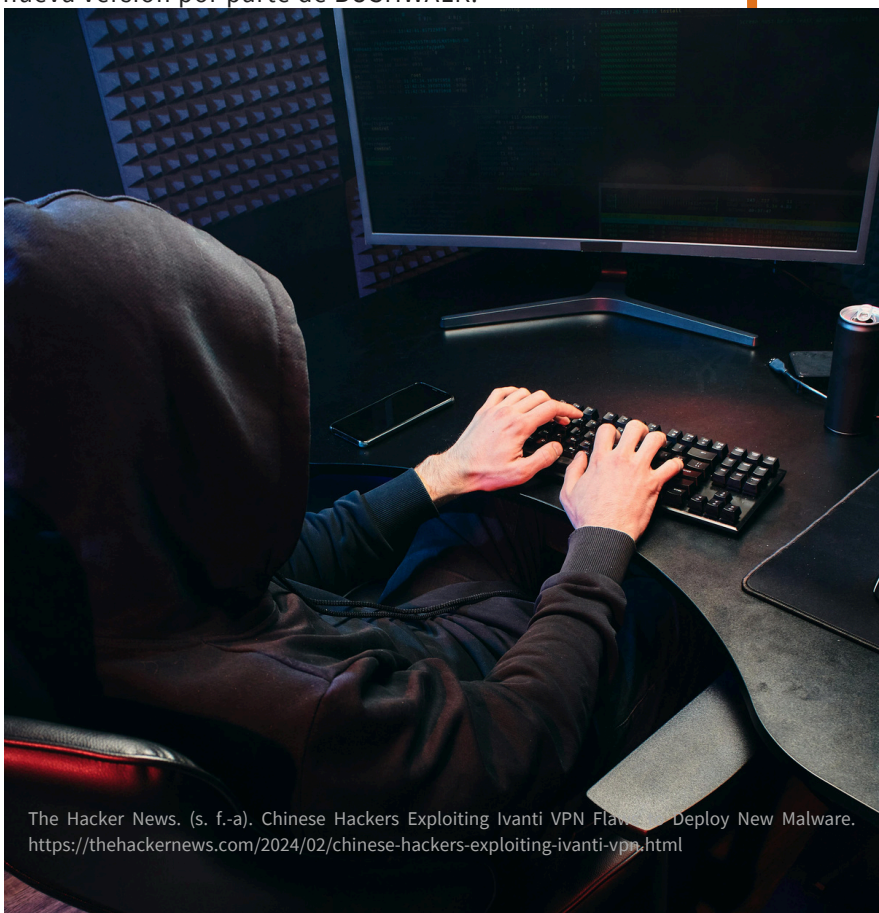
“El UNC3886 está destinado principalmente a la base industrial de defensa, las organizaciones de tecnología y telecomunicaciones en los Estados Unidos. y [Asia-Pacífico]”, dijeron los investigadores de Mandiant.

En enero, se informó que UNC5325 explotó activamente CVE-2024-21893, una vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF) en el elemento Ivanti Connect Secure, Ivanti Policy Secure e Ivanti Neurons para ZTA SAML. 19 de septiembre de 2024 dispositivos.nología limitada para fabricantes.

La cadena de ataque implicó combinar CVE-2024-21893 con una vulnerabilidad de inyección de comandos previamente revelada y rastreada como CVE-2024-21887 para obtener acceso no autorizado a dispositivos vulnerables, lo que llevó a la implementación de una nueva versión por parte de BUSHWALK.

En algunos casos, también se abusa de los componentes legítimos de Ivanti, como el complemento SparkGateway, para eliminar cargas útiles adicionales. Estos incluyen el complemento PITFUEL, que se utiliza para cargar objetos compartidos maliciosos con nombre en código LITTLELAMB.WOOLTEA, que tienen la capacidad de persistir en eventos de actualización del sistema, parches y restablecimientos de fábrica.

"Si bien los intentos limitados de persistencia vistos hasta ahora han fracasado debido a una falta de lógica en el código de malware para tener en cuenta las diferencias en las claves de cifrado, esto es una prueba más de que UNC5325 contribuirá en gran medida a mantener el acceso a objetivos prioritarios y objetos críticos.". Es importante que los equipos de red tengan las últimas actualizaciones y parches”, dijo la empresa.



The Hacker News. (s. f.-a). Chinese Hackers Exploiting Ivanti VPN Flaw[illegible] Deploy New Malware. https://thehackernews.com/2024/02/chinese-hackers-exploiting-ivanti-vpn.html

WORDPRESS BRICKS BAJO ATAQUE ACTIVO: FALLA CRÍTICA AFECTA A MÁS DE 25,000 SITIOS.

LOS ACTORES DE AMENAZAS ESTÁN EXPLOTANDO ACTIVAMENTE UNA VULNERABILIDAD DE SEGURIDAD CRÍTICA EN EL TEMA BRICKS DE WORDPRESS PARA EJECUTAR CÓDIGO PHP ARBITRARIO EN INSTALACIONES VULNERABLES.

Registrada como CVE-2024-25600 (puntuación CVSS: 9,8), esta vulnerabilidad permite a un atacante no autorizado realizar la ejecución remota de código. Esto afecta a todas las versiones de Bricks 1.9.6 y anteriores.

Los desarrolladores de temas parchearon la vulnerabilidad en la versión 1.9.6.1, que se lanzó el 13 de febrero de 2024, pocos días después de que el proveedor de seguridad de WordPress, Snicco informara la vulnerabilidad el 10 de febrero.

Si bien la vulnerabilidad de prueba de concepto (PoC) aún no se ha publicado, tanto Snicco como Patchstack publicaron detalles técnicos y señalaron que existe un código potencialmente vulnerable en la función prepare_query_vars_from_settings().

Específicamente, implica el uso de un token de seguridad llamado "nonce" para verificar los permisos, que luego puede usarse para ejecutar comandos arbitrarios, permitiendo que un actor de amenazas tome el control de un sitio web objetivo. Patchstack dijo que los valores aleatorios estaban disponibles públicamente en la interfaz del sitio de WordPress y agregó que no se realizaron pruebas de funcionalidad adecuadas.

"Nunca debes confiar en números únicos para autenticación, autorización o control de acceso", advierte WordPress en su documentación. "Utilice current_user_can() para proteger sus funciones y acepte siempre que los números nonce pueden verse comprometidos". La empresa de seguridad de WordPress, Wordfence, anunció el 19 de febrero de 2024 que había descubierto más de tres docenas de intentos de ataque para explotar la vulnerabilidad. Según los informes, los intentos de ataque comenzaron el 14 de febrero, un día después de la liberación.

Donde La mayoría de los ataques provienen de las siguientes direcciones IP:

200.251.23[.]57
92.118.170[.]216
103.187.5[.]128
149.202.55[.]79
5.252.118[.]211
91.108.240[.]52

Se estima que Bricks cuenta actualmente con unas 25.000 instalaciones activas. Se recomienda a los usuarios del complemento que apliquen los parches más recientes para mitigar posibles amenazas.

NOTICIAS NACIONALES

MÉXICO, SEGUNDO LUGAR EN AMÉRICA LATINA CON MÁS CIBERATAQUES.

MÉXICO FUE BLANCO DE MÁS DE 14 MIL MILLONES DE INTENTOS DE CIBERATAQUES EN EL PRIMER SEMESTRE DE 2023

México, segundo lugar en América Latina con más ciberataques | Municipios Puebla | Información del estado de Puebla. 14 febrero) https://municipiospuebla.mx/nota/2023-02-14/cdmx/m%C3%A9xico-segundo-lugar-en-am%C3%A9rica-latina-con-m%C3%A1s-ciberataques

Ocupando el segundo lugar entre las regiones de América Latina en este tipo de ataques, según el informe Global Threat Outlook de FortiGuard Labs.

Esto demuestra que todos somos o podemos ser víctimas de los ciberdelincuentes, que no excluyen a las organizaciones públicas y privadas e incluso afectan a las instituciones educativas de cualquier nivel.

Ante lo anterior, la Universidad Autónoma de Guadalajara (UAG) en colaboración con otras instituciones educativas de la región metropolitana impulsa la creación del Comité de Cooperación Interuniversitaria de Occidente en Ciberseguridad. El ingeniero Humberto Gutiérrez Zamorano, coordinador del Consejo de Ciberseguridad Empresarial de la UAG, explicó que debido a la alta frecuencia de incidentes de ciberdelitos a nivel global, nacional y local, esto ha ocurrido en Guadalajara. Esto es en respuesta a ciberataques como robo de identidad, secuestro de aplicaciones e intentos de acceso a servidores que afectan la vida de la comunidad universitaria, desde proveedores hasta personal directivo.

Red colaborativa

“Esta es una colaboración en ciberseguridad destinada a compartir experiencias, prácticas, errores y oportunidades para protegernos. y concientizar a la comunidad universitaria sobre los peligros que existen en línea y lo vulnerables que somos a ataques si no protegemos nuestros dispositivos, redes, etc.”, dijo el Ing. Gutiérrez. Universidades participantes en la primera selección: UAG, ITESO; Próximamente se sumarán la Universidad del Valle de Atmayaque (UNIVA), la Universidad de Guadalajara (UdeG) y varias instituciones educativas. A la primera reunión asistieron líderes de ciberseguridad de varias agencias. en beneficio de la sociedad

POLICÍA CIBERNÉTICA DE CDMX Y JAPÓN SE REÚNEN PARA FORTALECER ESTRATEGIAS DE CIBERSEGURIDAD.

Personal del Departamento de Policía Cibernética de la Secretaría de Seguridad Civil (SSC) de la Ciudad de México y el Departamento de Investigación Cibernética del Negociado de la Policía Nacional de Japón sostuvieron una reunión para fortalecer y compartir conocimientos en temas de seguridad cibernética.

La reunión se llevó a cabo en las instalaciones de la Policía Cibernética ubicada en la Alcaldía Cuahtémoc en la comunidad de Juárez; es parte de una estrategia para fortalecer los vínculos internacionales en materia de ciberseguridad.

Además de crear reciprocidad en las áreas de buenas prácticas y oportunidades que existen para cada lugar de trabajo individual, el objetivo es luchar contra el cibercrimen a nivel internacional.

El director de Investigación y Operaciones Técnicas de la Red CSE, Didier Domínguez Castellans, destacó la importancia de fortalecer las capacidades a través de la cooperación internacional.

Al encuentro asistieron el subjefe de la Policía Cibernética, Jesús Alfredo Hernández Olvera, y la directora de Asuntos Internacionales, Pamela Reducindo Pérez.

La Embajada de Japón estuvo representada por el Agregado de Seguridad y Cónsul Nobuaki Takahashi y el Asesor y Coordinador de Seguridad Diplomática Gogoya Arie.
Como representantes de la Agencia Nacional de Policía de Japón, Yutaka Ogawa y Hajime Kamata son del Departamento de Investigación de Internet.

Se asegura que: “tan solo en el 2023, la Policía Cibernética atendió 31 mil 849 denuncias recibidas a través de llamadas telefónicas, dos mil 265 denuncias por medio de la App Mi Policía y 76 mil 322 correos electrónicos, además se impartieron mil 118 pláticas preventivas a 74 mil 862 ciudadanos”.

Policía Cibernética de CdMx y Japón se reúnen para fortalecer estrategias de ciberseguridad (2024, 22 febrero). https://www.milenio.com/policia/mexico-y-japon-reunen-para-fortalecer-policia-cibernetica

SONICWALL, EMPRESA ESPECIALIZADA EN SEGURIDAD CIBERNÉTICA, DIJO QUE MÉXICO OCUPA EL SEXTO LUGAR A NIVEL MUNDIAL EN TÉRMINOS DE ATAQUES TOTALES DE RANSOMWARE.

MÉXICO, PUESTO 6 EN TOTAL DE ATAQUES DE RANSOMWARE A NIVEL MUNDIAL.

En su informe anual sobre ciberamenazas 2024, dijo que el año pasado se descubrió la amenaza de ciberataques más estructurados. "En comparación con esta época del año pasado, el número de ataques globales aumentó a más de mil millones", dice el informe.

El análisis registra un aumento del 659 % en los ataques de cifrado globales y un aumento del 117 % en las amenazas de cifrado a medida que los ciberdelincuentes optan por formas de actividad maliciosa más sigilosas y menos riesgosas.

"Estos datos ilustran el estado constante y en constante cambio de las amenazas cibernéticas, subrayan la necesidad de que las empresas adapten continuamente sus estrategias de seguridad y alientan a las organizaciones a confiar en los MSP (proveedores de servicios gestionados) para identificar y remediar rápidamente las amenazas", informó SonicWall. Explica.

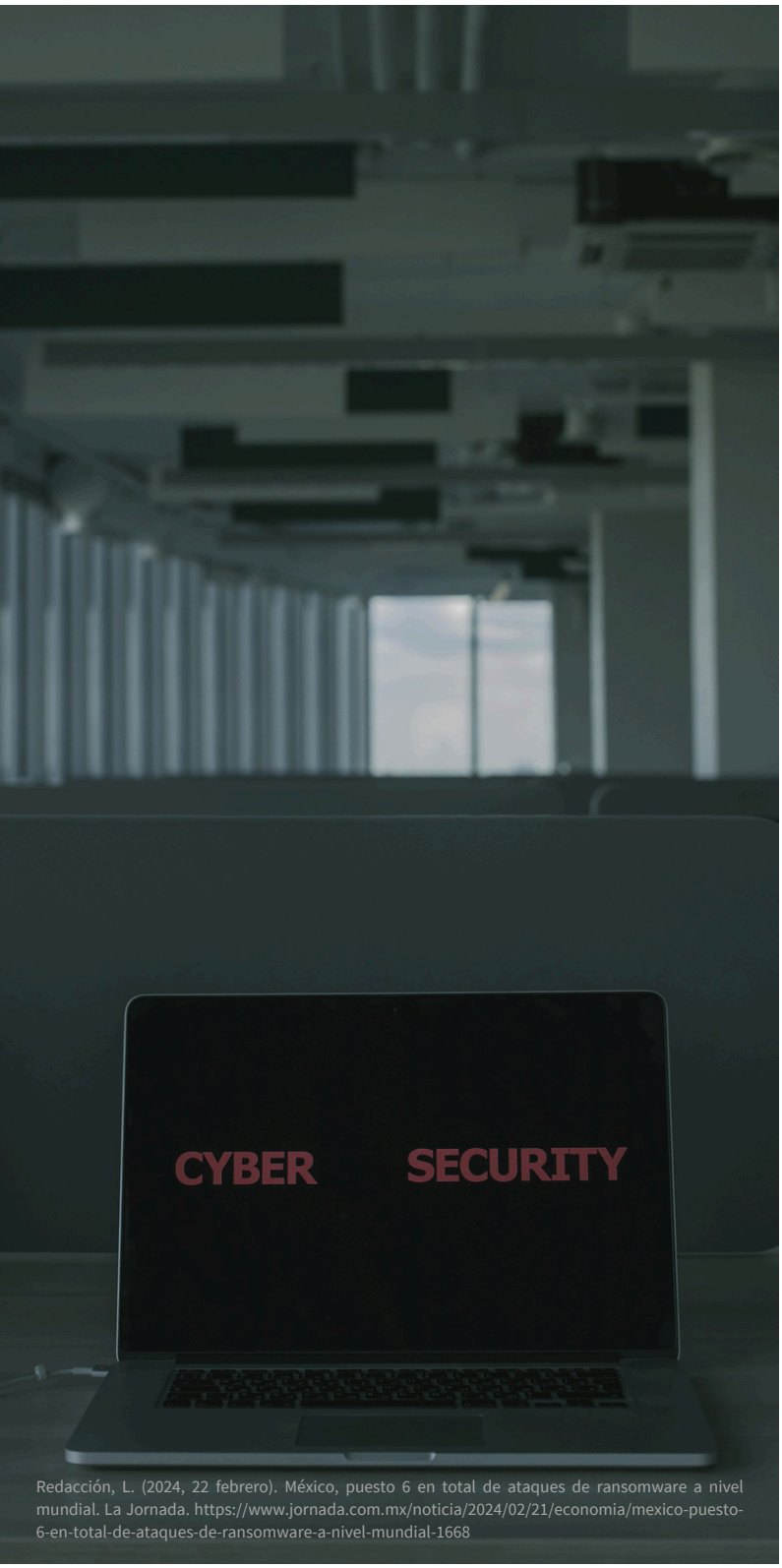
Se detectan más de 19.000 amenazas cada día

Los investigadores de SonicWall Capture Labs identifican y bloquean más de 19.000 amenazas cada día, y esperan más en 2024 específicamente para las pequeñas y medianas empresas (PYME), los gobiernos y las empresas.

Dijo que sus investigadores recopilan, analizan y verifican información sobre una red de amenazas que consta de dispositivos y activos en todo el mundo,
incluidos más de 1 millón de sensores de seguridad en casi 215 países y territorios.

Los documentos muestran que los intentos de amenazas de malware aumentaron un 11% en 2023, mientras que América Latina y EE.UU. fueron las regiones con mayor incidencia, creciendo un 30% y un 15% respectivamente. En comparación, Europa cayó un 2%, pero el Reino Unido tuvo la mayor caída, un 28%.

MÉXICO, PUESTO 6 EN TOTAL DE ATAQUES DE RANSOMWARE A NIVEL MUNDIAL.



Redacción, L. (2024, 22 febrero). México, puesto 6 en total de ataques de ransomware a nivel mundial. La Jornada. https://www.jornada.com.mx/noticia/2024/02/21/economia/mexico-puesto-6-en-total-de-ataques-de-ransomware-a-nivel-mundial-1668

El malware es la introducción de software malicioso con el que los ciberdelincuentes se infiltran en un dispositivo sin el conocimiento del usuario y causan daños e interrupciones en el sistema o robo de datos. Cuando se trata de ataques de ransomware, que es malware o código malicioso que bloquea el uso de un dispositivo o sistema infectado, el informe señala que México ocupa el sexto lugar a nivel mundial en términos de ataques en América Latina.

Mientras tanto, las amenazas globales han aumentado en un 15% a medida que la cantidad de dispositivos conectados continúa disparándose y los ciberdelincuentes apuntan a los puntos de entrada débiles como posibles vectores de ataque para las organizaciones.

Otra forma en que operan los delincuentes es a través de amenazas cifradas, un método más silencioso, que aumentó un 117% en todo el mundo el año pasado.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: FEBRERO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-20720	02/15/2024	Fallas de seguridad en productos Adobe	CVSS v3.1: 9.1 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-20720

Descripción: Las versiones 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 y anteriores de Adobe Commerce se ven afectadas por una neutralización inadecuada de elementos especiales utilizados en una vulnerabilidad de comando del sistema operativo ('inyección de comando del sistema operativo') que podría generar código arbitrario. ejecución por parte de un atacante. La explotación de este problema no requiere la interacción del usuario.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-23113	15/02/2024	Fallas de seguridad en productos Fortinet	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-23113

Descripción: Un uso de cadena de formato controlada externamente en Fortinet FortiOS versiones 7.4.0 a 7.4.2, 7.2.0 a 7.2.6, 7.0.0 a 7.0.13, FortiProxy versiones 7.4.0 a 7.4.2, 7.2.0 a 7.2.8, 7.0.0 a 7.0.14, versiones de FortiPAM 1.2.0, 1.1.0 a 1.1.2, 1.0.0 a 1.0.3, versiones de FortiSwitchManager 7.2.0 a 7.2.3, 7.0.0 a 7.0. 3 permite al atacante ejecutar código o comandos no autorizados a través de paquetes especialmente diseñados.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5155	15/02/2024	Fallas de seguridad en productos SQL	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-5155

Descripción: La neutralización inadecuada de elementos especiales utilizados en una vulnerabilidad de comando SQL ("Inyección SQL") en la aplicación móvil SoliPay de Utarit Information Technologies permite la inyección SQL. Este problema afecta a la aplicación móvil SoliPay: versiones anteriores a 5.0.8.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-7081	15/02/2024	Fallas de seguridad en productos SQL	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-7081

Descripción: La neutralización inadecuada de elementos especiales utilizados en una vulnerabilidad de comando SQL ("Inyección SQL") en el sistema de pago en línea POSTAHSİL permite la inyección de SQL. Este problema afecta al sistema de pago en línea: antes del 14.02.2024.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-23477	15/02/2024	Fallas de seguridad en productos SolarWinds	CVSS v3.1: 9.6 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-23477

Descripción: Se descubrió que SolarWinds Access Rights Manager (ARM) era susceptible a una vulnerabilidad de ejecución remota de código transversal de directorio. Si se explota, esta vulnerabilidad permite a un usuario no autenticado lograr una ejecución remota de código.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-20719	15/02/2024	Fallas de seguridad en productos Adobe	CVSS v3.1: 9.1 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-20719

Descripción: Las versiones 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 y anteriores de Adobe Commerce se ven afectadas por una vulnerabilidad de secuencias de comandos entre sitios (XSS) almacenada que podría ser aprovechada por un atacante administrador para inyectar secuencias de comandos maliciosas en cada administrador. página. Se puede ejecutar JavaScript malicioso en el navegador de la víctima cuando navega a la página que contiene el campo vulnerable, que podría aprovecharse para obtener acceso de administrador.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21413	13/02/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-23477

Descripción: Vulnerabilidad de ejecución remota de código de Microsoft Outlook

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-43609	08/02/2024	Fallas de seguridad en productos Emerson	CVSS v3.1: 9.1 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-43609

Descripción: En los productos Emerson Rosemount GC370XA, GC700XA y GC1500XA, un usuario no autenticado con acceso a la red podría obtener acceso a información confidencial o provocar una condición de denegación de servicio.

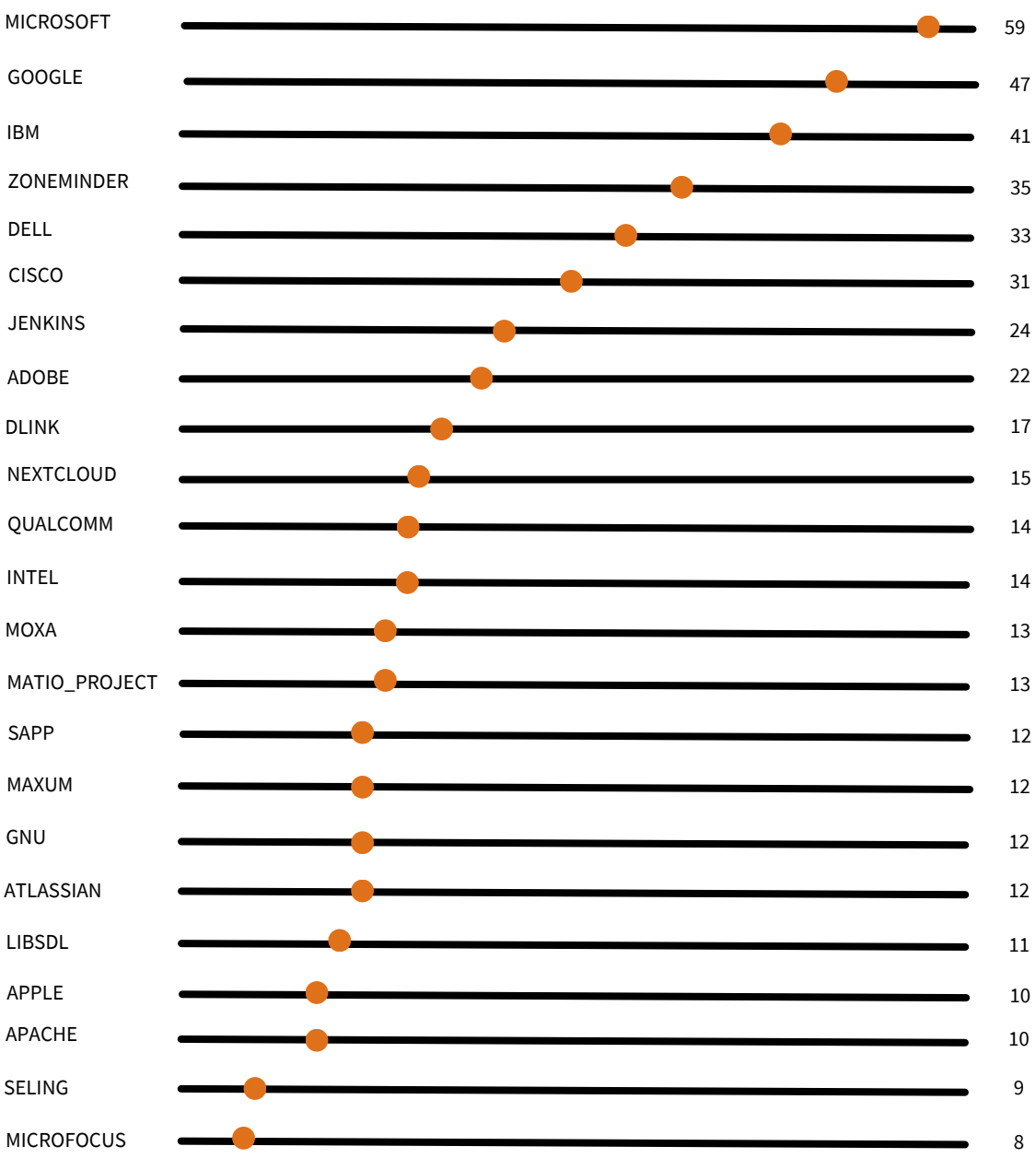
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-32328	07/02/2024	Fallas de seguridad en productos IBM	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-32328

Descripción: IBM Security Verify Access 10.0.0.0 a 10.0.6.1 utiliza protocolos inseguros en algunos casos que podrían permitir que un atacante en la red tome el control del servidor. Identificación de IBM X-Force: 254957.

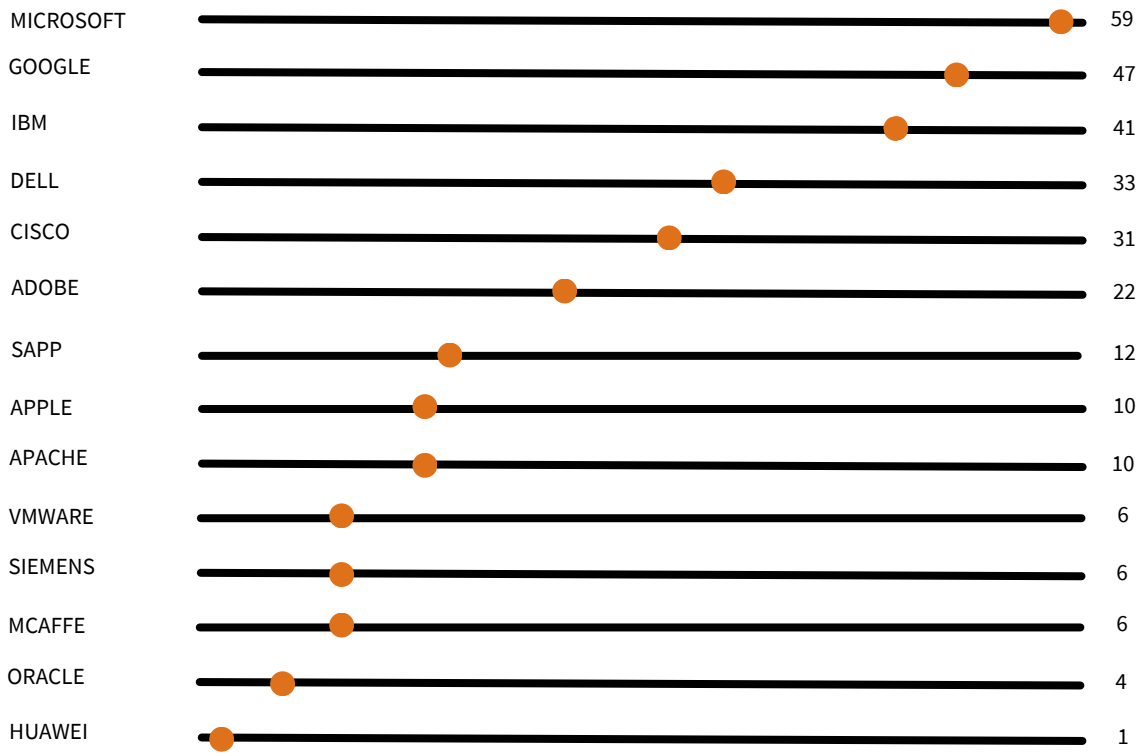
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-6989	05/02/2024	Fallas de seguridad en productos WordPress	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-6989

Descripción: El complemento Shield Security – Smart Bot Blocking & Intrusion Prevention Security para WordPress es vulnerable a la inclusión de archivos locales en todas las versiones hasta la 18.5.9 inclusive a través del parámetro render_action_template. Esto hace posible que un atacante no autenticado incluya y ejecute archivos PHP en el servidor, permitiendo la ejecución de cualquier código PHP en esos archivos.

FABRICANTES CON VULNERABILIDADES RELEVANTES: FEBRERO DE 2024



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: FEBRERO DE 2024



CULTURA DE CIBERSEGURIDAD

SPAM Y LAS ESTAFAS DE PHISHING

¿QUÉ ES EL SPAM Y LAS ESTAFAS DE PHISHING?

El spam es el equivalente electrónico de "correo basura" que llega a tu buzón o pasa por debajo de tu puerta. El spam, sin embargo, es más que algo molesto. Puede ser peligroso, especialmente si es parte de un phishing fraudulento.

Los correos electrónicos de spam se envían a una gran cantidad de especialistas en esta forma de engaño y ciberdelincuentes que buscan uno de los siguientes objetivos:

- Ganar dinero con la pequeña cantidad de personas que finalmente responden al mensaje.
- Realizar estafas de phishing para obtener contraseñas, números de tarjetas de crédito y detalles de cuentas bancarias.
- Infectar las computadoras de los destinatarios con código malicioso.

CÓMO PROTEGERTE DEL CORREO ELECTRÓNICO DE SPAM Y LAS PRÁCTICAS DE PHISHING

Para reducir la cantidad de correo electrónico de spam que recibe, estos son algunos consejos útiles del equipo de expertos en seguridad de Internet de Kaspersky Lab:

·Configura varias direcciones de correo electrónico
Es recomendable contar con al menos dos direcciones de correo electrónico.

·Dirección de correo electrónico privada
Esta dirección es solo para correspondencia personal. Las personas que envían spam crean listas de direcciones de correo electrónico posibles utilizando combinaciones obvias de nombres, palabras y números. Por lo tanto, debe hacer que la dirección sea difícil de adivinar. Además de tu nombre y apellido, debe proteger tu dirección privada con los siguientes elementos:

Nunca compartas tu dirección de correo electrónico privada con sitios web públicos.

Si necesita publicar su dirección de correo electrónico privado, intente enmascararla para evitar que los agentes de spam la obtengan. Para los que envían spam, por ejemplo, una dirección fácil de encontrar es "pedro.paredes@gmail.com". Trata de enviar un mensaje a la dirección "pedro-punto-paredes-arroba-gmail.com".

En caso de necesitar publicar tu dirección privada en un sitio web es más seguro como archivo gráfico ya que como enlace es más vulnerable al spam.
Si los spammers detectan su dirección privada, deberá de cambiarla. Aunque puede resultar molesto, cambiar tu dirección de correo electrónico te ayudará a evitar el spam.

·Dirección de correo electrónico pública
Utilice esta dirección cuando se registre en foros públicos y salas de chat o cuando se suscriba a listas de correo y otros servicios de Internet. Los siguientes consejos también pueden ayudarle a reducir la cantidad de spam que recibe de direcciones de correo electrónico públicas.

·Utilice filtros antispam
Abra únicamente cuentas de correo electrónico de proveedores que incluyan filtrado de spam. Elija entre soluciones antivirus y de seguridad de Internet que también incluyen funciones avanzadas antispam.

RHYSIDA RANSOMWARE

Rhysida es un ransomware dirigido a múltiples industrias, este ataque se hace pasar como un equipo especializado de ciberseguridad los cuales ofrecen su ayuda para identificar debilidades de seguridad en las redes y sistemas de las victimas, las cuales se ven presionadas mediante tácticas de doble extorsión donde se les exigen pagos exuberantes en bitcoins por el rescate.

Teniendo como motivación las ganancias financieras, Rhysida utiliza ataques de phishing como medio para obtener el acceso, posterior emplean Cobalt Strike para realizar movimiento lateral en las maquinas infectadas, siguiendo este patrón de ataque, emplean PsExec para entregar un Script llamado SILENTKILL, acabando con los programas de antivirus.

Mediante el phishing, Rhysida envía correos electrónicos fraudulentos que aparentan ser legítimos de manera persuasiva, su cuartada mas efectiva fue fingir ser un equipo de profesionales de la ciberseguridad generando confianza en las victimas.

Una vez las victimas muerden el cebo, Rhysida comienza el ataque con el uso de PsExec para obtener acceso de manera remota a los sistemas, lo que les permite a los atacantes realizar la ejecución remota de comandos, la ejecución de programas, ambos realizados con las credenciales de usuarios de confianza, teniendo total interacción con los servicios. Una vez tienen esta libertad, emplean el uso de Cobalt Strike realizando pruebas de penetración las cuales por su naturaleza sigilosa se vuelven desafiantes de detectar.

De la misma manera Qakbot comienza a robar informacion confidencial como credenciales bancarias, datos de inicio de sesión, etc. infectado el sistema Qakbot se propaga dentro de la red de la empresa y abre una puerta trasera para permitir el acceso remoto la cual es explotada por SystemBC.

De esta forma Rhysida ha logrado su cometido, teniendo todo lo que necesita, se emiten los mensajes de extorsión y se cifran los archivos, de esta forma solicitan pagos en criptomonedas.

Ransomware Spotlight: Rhysida - Security News - Trend Micro ID. (s. f.). https://www.trendmicro.com/vinfo/id/security/news/ransomware-spotlight/ransomware-spotlight-rhysida

REFERENCIAS

REFERENCIAS

- Ransomware Spotlight: Rhysida - Security News - Trend Micro ID. (s. f.). https://www.trendmicro.com/vinfo/id/security/news/ransomware-spotlight/ransomware-spotlight-rhysida
- Redacción, L. (2024, 22 febrero). México, puesto 6 en total de ataques de ransomware a nivel mundial. La Jornada. https://www.jornada.com.mx/noticia/2024/02/21/economia/mexico-puesto-6-en-total-de-ataques-de-ransomware-a-nivel-mundial-1668
- Policía Cibernética de CdMx y Japón se reúnen para fortalecer estrategias de ciberseguridad (2024, 22 febrero). https://www.milenio.com/policia/mexico-y-japon-reunen-para-fortalecer-policia-cibernetica
- México, segundo lugar en América Latina con más ciberataques | Municipios Puebla | Noticias del estado de Puebla. (2024, 14 febrero). https://municipiospuebla.mx/nota/2024-02-14/naci%C3%B3n/m%C3%A9xico-segundo-lugar-en-am%C3%A9rica-latina-con-m%C3%A1s-ciberataques

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