GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °1523

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERSEGURIDAD

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	4		
MALWARE	2	1	1
BRECHAS DE SEGURIDAD		2	1
NOTICIAS DE CIBERSEGURIDAD		1	4

VULNERABILIDADES

Vulnerabilidades críticas en SAP con puntaje cvss > 9.5

En su Security Patch Day de marzo de 2023 , el fabricante alemán de software corporativo SAP anunció un total de 19 nuevas notas de seguridad, cinco de las cuales fueron designadas como “críticas”.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
- https://noticiasseguridad.com/vulnerabilidades/vulnerabilidades-criticas-en-sap-con-puntaje-cvss-9-5/

Boletín mensual de Microsoft – Abril 2023

El boletín de abril de Microsoft detalla 124 vulnerabilidades, de las cuales 7 son de severidad crítica, 90 de severidad importante, 2 de severidad moderada, 4 de severidad baja y 21 sin severidad asignada.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/04/microsoft-parchea-97-cve-incluidos.html
- https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr?ranMID=43674&ranEAID=FE4O7wtxe6g&ranSiteID=FE4O7wtxe6g-u2tXEPxYoNOsvorctXk.uA&epi=FE4O7wtxe6g-u2tXEPxYoNOsvorctXk.uA&irgwc=1&OCID=AID2200057_aff_7795_1243925&tduid=%28ir__sg223zle2wkfbkljuvcdk9mugv2x6idfj3ahaiv900%29%287795%29%281243925%29%28FE4O7wtxe6g-u2tXEPxYoNOsvorctXk.uA%29%28%29&irclickid=_sg223zle2wkfbkljuvcdk9mugv2x6idfj3ahaiv900
- https://www.darkreading.com/vulnerabilities-threats/microsoft-patches-97-cves-including-zero-day-wormable-bugs
- https://www.incibe.es/protege-tu-empresa/avisos-seguridad/boletin-mensual-microsoft-abril-2023

Mozilla publica avisos de seguridad para varios productos

Mozilla ha publicado avisos de seguridad sobre vulnerabilidades que afectan a varios productos de Mozilla. Un actor de amenazas cibernéticas podría explotar estas vulnerabilidades para tomar el control de un sistema afectado.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/

Fortinet publica avisos de vulnerabilidad de abril de 2023

Fortinet ha publicado sus Avisos de vulnerabilidad de abril de 2023 para abordar las vulnerabilidades que afectan a múltiples productos. Un atacante podría explotar una de estas vulnerabilidades para tomar el control de un sistema afectado.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.fortiguard.com/psirt-monthly-advisory/april-2023-vulnerability-advisories

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.
- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

MALWARE

Más de un millón de sitios WordPress infectados por el malware Balada Injector

Se estima que, desde 2017, más de un millón de sitios web de WordPress han sido infectados por una campaña en curso para desplegar malware llamado Balada Injector.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.sucuri.net/2023/04/balada-injector-synopsis-of-a-massive-ongoing-wordpress-malware-campaign.html
- https://blog.segu-info.com.ar/2023/04/mas-de-un-millon-de-sitios-wordpress.html
- https://thehackernews.com/2023/04/over-1-million-wordpress-sites-infected.html

---

0-day en Windows es explotado por el ransomware Nokoyawa

Microsoft ha parcheado una vulnerabilidad Zero-Day en *Windows Common Log File System (CLFS)*, explotada activamente por ciberdelincuentes para escalar privilegios y desplegar cargas útiles de ransomware Nokoyawa.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/04/windows-zero-day-es-explotado-por.html

- https://www.bleepingcomputer.com/news/security/windows-zero-day-vulnerability-exploited-in-ransomware-attacks/

El nuevo programa espía quadream es un reemplazo del pegasus utilizado para hackear iphones de forma remota

Los investigadores de seguridad han descubierto nuevo malware con capacidades de hacking comparables a las de Pegasus, que fue desarrollado por NSO Group. El software, que es vendido por una empresa israelí llamada QuaDream, ha sido utilizado anteriormente por clientes para atacar a periodistas, líderes de la oposición política y un empleado de una ONG. La empresa que fabrica y vende el spyware se llama QuaDream.

Prioridad: 3 Importante.

Ampliar información:

- https://noticiasseguridad.com/seguridad-movil/el-nuevo-programa-espia-quadream-es-un-reemplazo-del-pegasus-utilizado-para-hackear-iphones-de-forma-remota/

El nuevo ransomware "Rorschach" se propaga a través de un producto comercial

Los actores de amenazas han desplegado una nueva y única cepa de ransomware utilizando la herramienta Palo Alto Cortex XDR Dump Service Tool, un producto de seguridad comercial.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/04/08/el-nuevo-ransomware-rorschach-se-propaga-a-traves-de-un-producto-comercial/

Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíba las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.
- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma Cyberacademy ©.
- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.
- Mantener actualizadas sus soluciones de ciberseguridad.
- Descargar aplicaciones solo de fuentes de confianza, como la tienda oficial de aplicaciones de Google Play Store.
- Revisar las calificaciones y opiniones de otras personas antes de descargar cualquier aplicación, especialmente si es una aplicación bancaria o financiera.
- No responder a llamadas telefónicas de números desconocidos o sospechosos, especialmente si solicitan información personal o financiera.
- No compartir información personal o financiera a través del teléfono o correo electrónico, a menos que esté seguro de la identidad del destinatario.

BRECHAS DE SEGURIDAD

Datos de conductores de Uber, expuestos en una brecha en los servidores de un bufete de abogados

Un bufete de abogados de tamaño medio que representa a Uber ha notificado a un número desconocido de sus conductores que los datos sensibles han sido expuestos y robados debido a un ciberataque. Genova Burns, con sede en Nueva Jersey, reveló la brecha en un correo electrónico a los clientes obtenido por primera vez por The Register.
"Hemos determinado que un tercero no autorizado obtuvo acceso a nuestros sistemas, y ciertos archivos limitados fueron accedidos o exfiltrados entre el 23 de enero de 2023, y el 31 de enero de 2023", reza el aviso.

Prioridad: 3 Importante.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/04/07/datos-de-conductores-de-uber-expuestos-en-una-brecha-en-los-servidores-de-un-bufete-de-abogados/
- https://noticiasseguridad.com/hacking-incidentes/uber-entrego-datos-confidenciales-de-los-conductores-a-un-bufete-de-abogados-y-filtraron-todos-los-datos/

Revelan en EE.UU. una masiva filtración de datos de inteligencia de la guerra en Ucrania

Los documentos, que en parte parecen provenir del Pentágono y están marcados como *"altamente clasificados"*, contienen información táctica sobre la guerra en Ucrania, incluso sobre las capacidades bélicas de ese país. Según un funcionario del Pentágono, muchos de esos archivos parecen haber sido preparados durante los últimos meses por el general Mark A. Milley, jefe del Estado Mayor Conjunto y otros altos militares norteamericanos, pero también tenían acceso a ellos otros militares y empleados contratados autorizados.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.lanacion.com.ar/el-mundo/revelan-en-eeuu-una-masiva-filtracion-de-datos-de-inteligencia-de-la-guerra-en-ucrania-nid09042023/

Una vez más Hyundai y Toyota filtran datos personales de clientes

Los piratas informáticos pudieron acceder a la información personal de las personas después de que Hyundai anunciara una violación de datos que afectó a los propietarios de vehículos en Italia y Francia, así como a aquellos que habían programado pruebas de manejo con el fabricante de automóviles.

Prioridad: 2 Urgente.

Ampliar información:

- https://noticiasseguridad.com/hacking-incidentes/una-vez-mas-hyundai-y-toyota-filtran-datos-personales-de-clientes/
- https://computerhoy.com/ciberseguridad/hyundai-sufre-ciberataque-espana-compromete-datos-miles-clientes-1228530
- https://cybersecuritynews.es/hyundai-victima-de-un-ciberataque-que-ha-expuesto-datos-de-miles-de-clientes/

NOTICIAS DE CIBERSEGURIDAD

SONDA, una de las mayores empresas de tecnología de América Latina, víctima de un ataque ransomware

SONDA, empresa líder en tecnología de América Latina, confirmó recientemente que sufrió un ataque ransomware el pasado 29 de marzo. Los ciberdelincuentes exigieron un rescate de $2 millones de dólares para liberar la información cifrada. Aunque la empresa afirma haber contenido la situación de manera ágil y oportuna, los delincuentes lograron extraer información sensible, incluyendo órdenes de compra, cotizaciones, propuestas, inventarios, facturas e información administrativa.

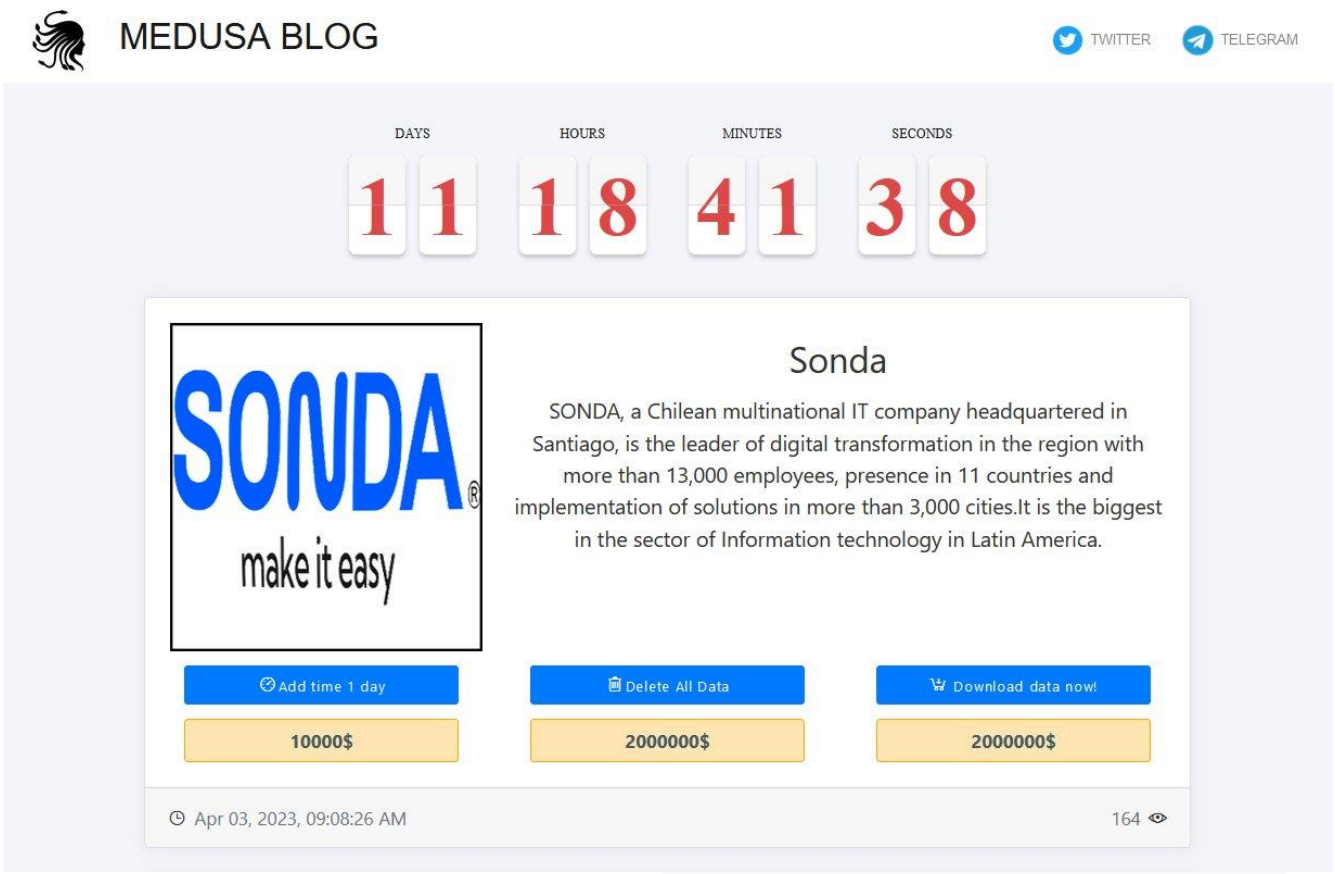

Imagen Darkweb blog Medusa Ransomware

Prioridad: 2 Urgente.

Ampliar información:

- https://www.trendtic.cl/2023/04/sonda-confirma-ataque-de-ransomware-en-chile/
- https://www.ciberseguridadlatam.com/2023/04/12/sonda-una-de-las-mayores-empresas-de-tecnologia-de-america-latina-victima-de-un-ataque-ransomware/

La empresa taiwanesa de PC, MSI, es víctima de un ataque de ransomware

La empresa taiwanesa de PC MSI (abreviatura de Micro-Star International) ha confirmado oficialmente que ha sido víctima de un ciberataque contra sus sistemas.
La compañía dijo que "rápidamente" inició la respuesta a incidentes y medidas de recuperación después de detectar "anomalías en la red." También dijo que alertó a las fuerzas de seguridad sobre el asunto.

Prioridad: 3 Importante.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/04/10/la-empresa-taiwanesa-de-pc-msi-es-victima-de-un-ataque-de-ransomware/

Gartner presenta sus ocho principales predicciones de ciberseguridad para 2023-2024

El futuro de la ciberseguridad se discutió en el Gartner Security & Risk Management Summit, celebrado en Sídney el 28 y 29 de marzo. Allí, Richard Addiscott y Lisa Neubauer, analistas senior de Gartner, presentaron las ocho predicciones más destacadas de la compañía en ciberseguridad para ayudar a los líderes de seguridad y gestión de riesgos a tener éxito en la era digital.

Prioridad: 3 Importante.

Ampliar información:

- https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024

Emisoras de Caracol Radio sufrieron ataque cibernético y daños en varios sistemas

Con el dial afectado amanecieron las emisoras que pertenecen a la cadena Caracol Radio, que informó a través de un comunicado que varias de sus plataformas fueron víctimas de un ataque cibernético por inescrupulosos, lo que complicó un poco la operación en el inicio de la jornada periodística de este viernes 14 de abril.

CARACOL RADIO

COMUNICADO OFICIAL

PRISA MEDIA COLOMBIA

Bogotá, Abril 14, 2022

Desde las 3:00 a.m., del día de hoy, el grupo de medios Caracol S.A., sus emisoras (W Radio, Caracol Radio, Tropicana, Bésame, Radioacktiva, Los 40 Urban y Los 40) y sus activos digitales han sufrido un ataque cibernético.

Actualmente, los sistemas de emisión de publicidad, operaciones, de gestión de contenido en radio, publicación digital y streaming son los principalmente afectados.

Estamos trabajando para resolver este problema lo más rápido posible y poder normalizar la operación.

Imagen Comunicado Caracol Radio

Prioridad: 3 Importante.

Ampliar información:

- https://www.pulzo.com/nacion/emisoras-caracol-radio-sufrieron-ataque-cibernetico-PP2750018
- https://www.pulzo.com/nacion/reaccion-hernan-pelaez-por-ataque-cibernetico-caracol-radio-PP2750540
- https://caracol.com.co/2023/04/14/grupo-de-medios-de-caracol-radio-fue-victima-de-ciberataque/?outputType=amp

---

Darktrace: la investigación no encontró evidencia de violación de LockBit

La firma de seguridad cibernética Darktrace dice que no encontró evidencia de que la pandilla de ransomware LockBit haya violado su red después de que el grupo agregó una entrada a su plataforma de fugas en la web oscura, lo que implica que robaron datos de los sistemas de la compañía.
Horas después de que la pandilla reclamara a DarkTrace como víctima en su sitio de fuga de datos, la compañía realizó una investigación y no encontró evidencia de una violación de sus sistemas.

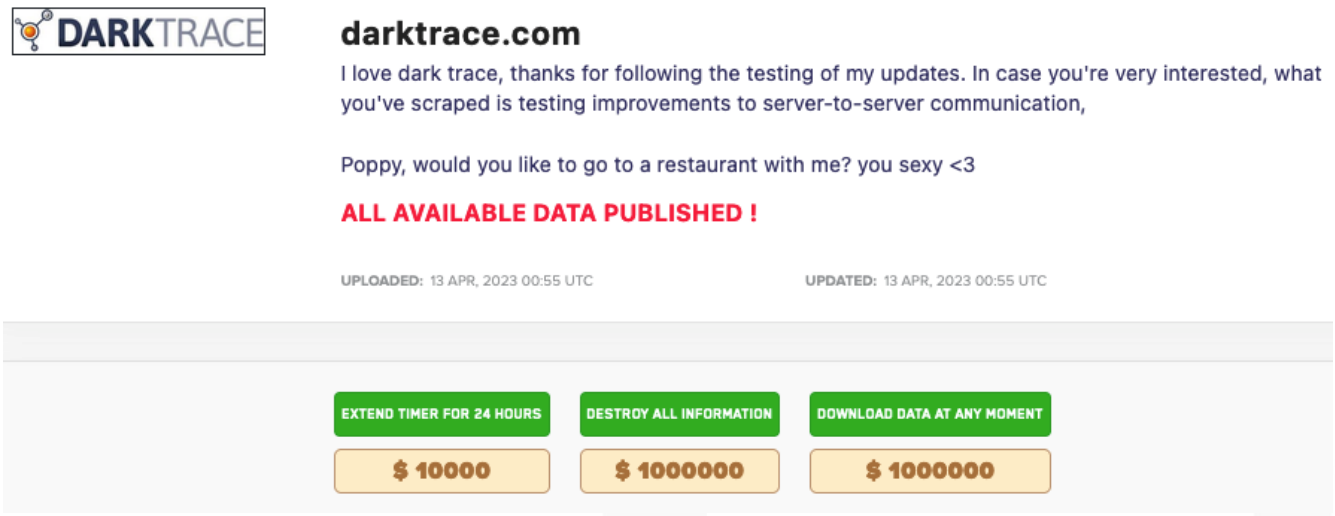

Imagen de fuga de datos falsa que puso Lockbit en su blog en Darkweb

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/darktrace-investigation-found-no-evidence-of-lockbit-breach/
- https://es.darktrace.com/statement-darktrace