GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1324

En alianza con

TD SYNNEX FORTINET

BOLETÍN DE CIBERINTELIGENCIA DE AMENAZAS

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	1	1	2
MALWARE	0	0	5
NOTICIAS DE CIBERSEGURIDAD	0	1	9

VULNERABILIDADES

Aiohttp Group Vulnerabilidad (CVE-2024-23334)

En la última semana de enero de 2024, se lanzó un parche para abordar una vulnerabilidad detectada en aiohttp. Este problema de seguridad afecta a las versiones de aiohttp anteriores a la 3.9.2. La vulnerabilidad de seguridad, identificada como CVE-2024-23334, consiste en una vulnerabilidad de directorios en aiohttp que permite a atacantes remotos no autenticados, acceder a información de archivos arbitrarios en el servidor si es explotada.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/hackers-exploit-aiohttp-bug-to-find-vulnerable-networks

---

Jenkins Args4j CVE-2024-23897

Se descubrió que Jenkins, un popular servidor de automatización de código abierto, se veía afectado por una vulnerabilidad de lectura de archivo, identificada como CVE-2024-23897. Jenkins utiliza una interfaz de línea de comandos (CLI) incorporada para facilitar la interacción desde entornos de script o shell, y emplea la biblioteca args4j para analizar los argumentos de los comandos y opciones en el controlador Jenkins durante el procesamiento de comandos CLI.

Prioridad: 2 Urgente.

Ampliar información:

https://www.trendmicro.com/en_us/research/24/c/cve-2024-23897.htm

---

Vulnerabilidad de deserialización de PHP sin parches en Artica Proxy

El equipo de investigación de amenazas de SonicWall Capture Labs identificó una vulnerabilidad de deserialización en Artica Proxy. Tras evaluar su impacto, se han desarrollado medidas de mitigación. Artica Proxy es una solución integral de proxy que lleva a cabo funciones como filtrado y categorización web, inspección SSL y gestión del ancho de banda. Según el proveedor, esta solución cuenta con más de 100 mil servidores instalados en todo el mundo.

Prioridad: 3 Importante.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/03/unpatched-php-deserialization-vulnerability-in-artica-prox

---

Exploit lanzado para el error RCE de fortinet utilizado en ataques

Investigadores de seguridad han publicado un exploit de prueba de concepto (PoC) para una vulnerabilidad crítica en el software FortiClient Enterprise Management Server (EMS) de Fortinet, que actualmente está siendo activamente explotada en ataques. Identificada como CVE-2023-48788, esta vulnerabilidad de seguridad consiste en una inyección SQL en el componente de administración de la base de datos (DAS) de DB2, descubierta y reportada por el Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unido.

Prioridad: 1 Critico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/exploit-released-for-fortinet-rce-bug-used-in-attacks-patch-now

---

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se pueden aplicar las actualizaciones de inmediato.
- Establecer una política y un plan periódico de mitigación de vulnerabilidades.
- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.

- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.
- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

Una campaña evasiva de Azorult de contrabando a través de Google Sites

Netskope Threat Labs ha detectado una campaña evasiva de Azorult en la naturaleza que emplea múltiples técnicas de evasión de la defensa, desde la entrega hasta la ejecución, con el objetivo de pasar desapercibido para el defensor y robar datos confidenciales. Azorult, descubierto por primera vez en 2016, es un ladrón de información que se especializa en la obtención de datos sensibles, incluidas credenciales de usuario, información del navegador y datos de billeteras criptográficas. Clasificado con una puntuación de 4/8, Azorult actualmente representa una de las principales familias de malware observadas por Netskope Threat Labs.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/hackers-using-sneaky-html-smuggling-to.html

Malware para Android

El malware dirigido a dispositivos móviles es un desafío recurrente con el que nos enfrentamos constantemente. En el año 2023, se bloquearon 33.8 millones de ataques de malware, adware y riskware en dispositivos móviles. Uno de los incidentes más destacados fue la Operación Triangulación, que afectó a dispositivos iOS, aunque fue un caso bastante singular.

Prioridad: 3 Importante.

Ampliar información:

https://securelist.com/crimeware-report-android-malware/112121

Malware Sign1: análisis, historial de campañas e indicadores de compromiso

La aparición de ventanas emergentes aparentemente aleatorias en su sitio web. Aunque estaba claro que algo no iba bien con el sitio web, resultaba difícil reproducir el problema. Sin embargo, al inspeccionar los registros del escáner del lado del servidor, se pudo localizar la fuente del inconveniente, que resultó ser una inyección de JavaScript notablemente interesante relacionada con una campaña de malware que internamente se conoce como Sign1.

Prioridad: 3 Importante.

Ampliar información:

https://blog.sucuri.net/2024/03/sign1-malware-analysis-campaign-history-indicators-of-compromise.html

---

Un nuevo ataque de phishing utiliza un ingenioso truco de Microsoft Office para implementar NetSupport RAT

Una nueva campaña de phishing está dirigida a organizaciones de EE. UU. con la intención de implementar un control remoto troyano de acceso llamado NetSupport RAT. La empresa israelí de ciberseguridad Perception Point está haciendo un seguimiento de la campaña bajo el nombre de Operación PhantomBlu. "La operación PhantomBlu introduce un matiz novedoso en el método de explotación, divergiendo del mecanismo de entrega típico de NetSupport RAT al aprovechar la manipulación de plantillas OLE (Object Linking and Embedding), explotando las plantillas de documentos de Microsoft Office.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/new-phishing-attack-uses-clever.html

---

Los nuevos ataques de phishing de strelastealer afectan a más de 100 organizaciones en la UE y los EE. UU.

Los investigadores de ciberseguridad han detectado una nueva ola de ataques de phishing que tienen como objetivo entregar un ladrón de información en constante evolución conocido como StrelaStealer. Estas campañas afectan a más de 100 organizaciones en la Unión Europea y los Estados Unidos, según informan los investigadores de la Unidad 42 de Palo Alto Networks en un nuevo informe publicado hoy. "Estas campañas se presentan en forma de correos electrónicos no deseados con archivos adjuntos que eventualmente ejecutan la carga útil de la DLL de StrelaStealer", declararon los investigadores Benjamin Chang, Goutam Tripathy y Pranay Kumar Chhapar.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/new-strelastealer-phishing-attacks-hit.html

---

Recomendaciones generales sobre malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.
- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.
- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.
- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.
- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

El apetito del ransomware por la atención médica de EE. UU. hace que los ataques conocidos se dupliquen al año

Tras el ataque del 21 de febrero a Change Healthcare, decenas de personas en Estados Unidos han experimentado los impactantes efectos del ransomware en el mundo real. Descrito por el presidente y director ejecutivo de la Asociación Americana de Hospitales (AHA, por sus siglas en inglés), Rick Pollack, como "el incidente más significativo y consecuente de su tipo contra el sistema de salud de Estados Unidos en la historia", el ataque ha interrumpido el flujo de miles de millones de dólares en pagos entre médicos, hospitales, farmacias y aseguradoras.

Prioridad: 3 Importante.

Ampliar información:

https://www.malwarebytes.com/blog/ransomware/2024/03/ransomwares-appetite-for-us-healthcare-sees-known-attacks-double-in-a-yeaR

Evaluación de INTERPOL sobre el fraude financiero

Una nueva evaluación de INTERPOL sobre el fraude financiero en el mundo destaca cómo el aumento del uso de la tecnología permite a los grupos de delincuencia organizada dirigirse de manera más efectiva a las víctimas en todo el mundo. La utilización de inteligencia artificial (IA), grandes modelos de lenguaje y criptomonedas, combinados con el phishing y modelos de negocio de ransomware como servicio, ha dado lugar a campañas de fraude más sofisticadas y profesionales sin la necesidad de habilidades técnicas avanzadas, a un costo relativamente bajo.

Prioridad: 3 Importante.

Ampliar información:

https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/INTERPOL-inancial-Fraud-assessment-A-global-threat-boosted-by-technology

---

Rastrear todo en la dark web es de misión crítica

Una de las prácticas estándar en ciberseguridad hoy en día es monitorear de manera constante la Dark Web, el lugar de operaciones para los actores malintencionados en todo

el mundo, en busca de cualquier indicio de que los secretos de su empresa u otra propiedad intelectual han sido exfiltrados.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/vulnerabilities-threats/tracking-everything-on-dark-web-is-mission-critica

---

Los sectores de la Aviación y Aeroespacial se enfrentan a amenazas cibernéticas que se disparan

Resecurity destaca los recientes incidentes cibernéticos dirigidos a los sectores aeroespacial y de la aviación, y enfatiza la importancia de realizar evaluaciones rigurosas de los riesgos de ciberseguridad para los aeropuertos. Es crucial tener en cuenta las diferentes definiciones técnicas que distinguen entre las industrias aeroespacial y aeronáutica.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/160664/uncategorized/aviation-and-aerospace-sectors-cyber-threats.html

---

Una inmersión profunda en el informe de inteligencia de amenazas de 2023 de ATO: navegando el complejo panorama de la ciberseguridad

En el acelerado mundo de la ciberseguridad, anticiparse a las amenazas emergentes no es solo un objetivo, sino una necesidad. A medida que los atacantes cibernéticos

evolucionan y se vuelven más sofisticados, las organizaciones deben equiparse con la inteligencia y las defensas más recientes para proteger sus activos. El equipo de Operaciones de Amenazas Avanzadas (ATO) ha lanzado su Informe de Inteligencia de Amenazas 2023.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/it-construction-sectors-ransomware

---

Guerra cibernética

En las últimas décadas, la naturaleza de la guerra entre naciones ha evolucionado sustancialmente con la integración de tácticas cibernéticas ofensivas. A finales de 2023, el jefe de ciberdefensa de Israel, Yigal Unna, expresó su preocupación por el aumento de la intensidad de los ataques cibernéticos por parte de Irán contra la infraestructura y las agencias gubernamentales israelíes. Esto ejemplifica la nueva realidad en la que vivimos, donde la guerra cibernética se ha convertido en un dominio crítico junto con tácticas terrestres, aéreas y marítimas en conflictos armados en todo el mundo.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/cyberattacks-data-breaches/cyber-warfare-understanding-new-frontiers-in-global-conflicts

---

CISA, FBI y MS-ISAC publican una actualización de la guía conjunta sobre la distribución técnicas de denegación de servicio

CISA, el FBI y el Centro de Análisis Multiestatal de Intercambio de Información (MS-ISAC) han publicado conjuntamente una guía actualizada titulada "Comprender y responder a los ataques distribuidos de denegación de servicio (DDoS)", destinada a abordar las necesidades y desafíos específicos que enfrentan las organizaciones en la defensa contra ataques DDoS.

Prioridad: 3 Importante.

Ampliar información:

https://www.cisa.gov/news-events/alerts/2024/03/21/cisa-fbi-and-ms-isac-release-update-joint-guidance-distributed-denial-service-techniques

---

Aumenta la ansiedad pública por la resistencia de las infraestructuras críticas a los ciberataques

Con el aumento de las fallas temporales en la infraestructura crítica en los últimos años, el 81% de los residentes están preocupados por la seguridad que puede tener la infraestructura crítica, según una encuesta realizada por MITRE y The Harris Poll. El público considera que los ciberataques representan el mayor riesgo para las infraestructuras críticas (el 78% mencionó los ciberataques), y el 51% no confía en que se esté preparado parala recuperación frente a un ataque.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/03/18/critical-infrastructure-cyberattacks-risk/

Cuentas de correo electrónico del Fondo Monetario Internacional comprometidas

El Fondo Monetario Internacional (FMI) reveló una brecha de seguridad en la que las cuentas de correo electrónico se vieron comprometidas a principios de este año. La agencia descubrió el incidente el 16 de febrero de 2024 y se inició una investigación inmediatamente con la ayuda de expertos en ciberseguridad. El FMI es uno de los principales organismos financieros de las Naciones Unidas y una institución financiera internacional financiada por 190 países miembros. Su misión declarada es "trabajar para fomentar la cooperación monetaria global".

Prioridad: 2 Urgente.

Ampliar información:

https://securityaffairs.com/160641/hacking/international-monetary-fund-email-compromise.html

---