GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0924

En alianza con

TD SYNNEX FORTINET

BOLETÍN DE CIBERSEGURIDAD SEMANAL

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

VULNERABILIDADES

Solar Winds corrige errores críticos de RCE

SolarWinds ha lanzado parches para cinco vulnerabilidades de ejecución remota de código (RCE) en su solución Access Rights Manager (ARM), incluyendo tres que se consideran críticas, las cuales pueden ser explotadas sin autenticación. Access Rights Manager permite a las empresas gestionar y auditar los derechos de acceso en toda su infraestructura de TI, lo que ayuda a minimizar el impacto de las amenazas internas y garantizar la seguridad de los sistemas.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/solarwinds-fixes-critical-rce-bugs-in-access-rights-audit-solution/

Alerta de VMware: desinstale EAP ahora

VMware ha emitido una recomendación urgente instando a los usuarios a desinstalar el obsoleto Enhanced Authentication Plugin (EAP) después de descubrir una falla de seguridad crítica. La vulnerabilidad, identificada como CVE-2024-22245 (con una puntuación CVSS de 9.6), se describe como un error de retransmisión de autenticación arbitrario. Según la compañía, "un actor malicioso podría engañar a un usuario de dominio objetivo con EAP instalado en su navegador web para que solicite y retransmita tickets de servicio para nombres principales de servicio (SPN) arbitrarios de Active Directory.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/02/vmware-alert-uninstall-eap-now-critical.html

---

Vulnerabilidades explotadas en campañas de ransomware desde 2017 a 2023

La explotación de vulnerabilidades por parte de grupos de ransomware se divide en dos categorías: vulnerabilidades que solo han sido explotadas por uno o dos grupos y aquellas que han sido ampliamente explotadas por varios grupos. Cada una de estas categorías requiere un enfoque diferente para la defensa y la mitigación. Este informe de Recorded Future profundiza en estos aspectos. Los grupos de actores de amenazas que son los únicos que atacan ciertas vulnerabilidades tienden a seguir preferencias específicas de

orientación y uso de armas, lo que permite a las empresas priorizar las defensas de la red y las auditorías de los proveedores.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/02/vulnerabilidades-explotadas-en-campanas.html

---

Vulnerabilidades críticas en Jenkins

El equipo de investigación de vulnerabilidades de Sonar ha identificado vulnerabilidades de seguridad en Jenkins, el destacado software de integración e implementación continua (CI/CD) de código abierto. Es crucial que los administradores y desarrolladores parcheen sus servidores Jenkins de manera urgente, dado que dos vulnerabilidades críticas ya cuentan con exploits públicos.

Prioridad: 1 Crítico.

Ampliar información:

https://blog.segu-info.com.ar/2024/02/vulnerabilidades-criticas-en-jenkins.html

---

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

Las APT iraníes se disfrazan de hacktivistas

Los grupos respaldados por el estado iraní, bajo el disfraz de hacktivistas, han reclamado la responsabilidad de ataques dirigidos contra infraestructuras críticas y sistemas de defensa aérea en Israel. A pesar del silencio de los actores de amenazas en Gaza, la mayoría de los recientes ataques cibernéticos contra Israel han sido perpetrados por estas entidades.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/threat-intelligence/iranian-apts-dress-up-as-hacktivists-for-disruption-influence-ops

---

Nuevo ransomware "Alpha"

Alpha, un ransomware recientemente identificado, surgió por primera vez en febrero de 2023 y ha intensificado sus actividades en las últimas semanas. Este ransomware presenta notables similitudes con el ya desaparecido ransomware NetWalker, el cual cesó sus operaciones en enero de 2021 tras una exitosa operación internacional de aplicación de la ley.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/alpha-ransomware-linked-to-netwalker-operation-dismantled-in-2021/

Cómo convertir los LLM en armas para secuestrar sitios web automáticamente

Los modelos de inteligencia artificial (IA), que han suscitado inquietudes persistentes sobre la seguridad debido a resultados nocivos y sesgados, representan un riesgo que va más allá de la mera generación de contenidos. Al combinarse con herramientas que posibilitan la interacción automatizada con otros sistemas, estos modelos pueden comportarse de manera autónoma como agentes maliciosos.

Prioridad: 2 Urgente.

Ampliar información:

https://www.theregister.com/2024/02/17/ai_models_weaponized/

El troyano "Anatsa"

En el entorno dinámico de la banca móvil, la seguridad se encuentra en constante evolución, lo que presenta continuos desafíos para los bancos y las instituciones financieras. Por tanto, es crucial anticiparse a las amenazas emergentes. Los últimos descubrimientos sobre la campaña de troyanos bancarios "Anatsa" resaltan la naturaleza cambiante de estas amenazas, subrayando la importancia de contar con una sólida inteligencia de amenazas móviles.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/anatsa-android-malware-downloaded-150-000-times-via-google-play/

VietCreaCare dirigida a anunciantes de Facebook en Vietnam

Los anunciantes de Facebook en Vietnam han sido el blanco de un ladrón de información, conocido como VietCredCare, al menos desde agosto de 2022. Este malware es notable por su capacidad para filtrar automáticamente las cookies de sesión de Facebook y las credenciales robadas de dispositivos comprometidos. Además, evalúa si estas cuentas administran perfiles comerciales y mantienen un saldo positivo de crédito publicitario de Meta. Estos hallazgos provienen de un nuevo informe compartido con The Hacker News por parte de Group-IB, con sede en Singapur.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/02/new-vietcredcare-stealer-targeting.html

---

Actividades maliciosas con SSH-Snake

Una herramienta de mapeo de red de código abierto llamada SSH-Snake ha sido utilizada por actores de amenazas para llevar a cabo actividades maliciosas. Según el investigador de Sysdig, Miguel Hernández, SSH-Snake es un gusano automodificable que aprovecha las credenciales SSH descubiertas en un sistema comprometido para propagarse por toda la red. Esta herramienta busca a través de ubicaciones de credenciales conocidas y archivos de historial de shell para determinar su próximo movimiento de forma automática.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/02/cybercriminals-weaponizing-open-source.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

Formas de simplificar la gobernanza de identidades de SaaS

Dado que las aplicaciones SaaS ahora representan la mayoría de tecnología utilizada por colaboradores en la muchas organizaciones, la gestión de identidades se ha vuelto una tarea crucial. Sin embargo, esta tarea conlleva un gran desafío, ya que implica gestionar y proteger el acceso a una gran cantidad de aplicaciones SaaS individuales. Esto pone a prueba a los equipos de TI centralizados, que son responsables de esta tarea, pero que enfrentan dificultades para convertirse en expertos en la configuración de seguridad nativa, así como los controles de acceso para cientos (o miles) de aplicaciones.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/02/6-ways-to-simplify-saas-identity.html

---

Ciberseguridad para el cuidado de la salud

Los ciberdelincuentes están adoptando estrategias más audaces que nunca, enfocándose en las organizaciones sanitarias más pequeñas con el objetivo de obtener grandes pagos. Aunque sería reconfortante creer que los delincuentes alguna vez

respetaron un código de conducta, si alguna vez existió, ha sido desechado por completo. Los grupos de hackers sofisticados ahora están dispuestos a lanzar ataques cibernéticos contra clínicas médicas, residencias de ancianos y otros proveedores de servicios de salud. Lamentablemente, las organizaciones de atención médica tipo PYME se han convertido en objetivos vulnerables, sujetas a robo de datos confidenciales, extorsión de grandes rescates o, lo que es aún más preocupante, interrupción de la atención crítica a pacientes.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/02/cybersecurity-for-healthcarediagnosing.html

---

Operación de inteligencia para ransomware LockBit

La Agencia Nacional contra el Crimen del Reino Unido (NCA) confirmó el martes que ha obtenido el código fuente de LockBit, junto con una amplia cantidad de inteligencia relacionada con sus actividades y afiliados. Este logro se realizó como parte de un grupo de trabajo conocido como “Operación Cronos”.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/02/lockbit-ransomware-operation-shut-down.html

---

Resurgimiento del grupo de ransomware LockBit

Los actores de amenazas detrás de la operación de ransomware LockBit han resurgido en la web oscura utilizando una nueva infraestructura, apenas días después de que un ejercicio internacional de aplicación de la ley tomara el control de sus servidores. En este sentido, el grupo ha trasladado su portal de fuga de datos a una nueva dirección ".onion" en la red TOR, y al momento de redactar este artículo, se han enumerado 12 nuevas víctimas.

En un mensaje de seguimiento detallado, el administrador responsable de LockBit, admitió que algunos de sus sitios web fueron confiscados, probablemente debido a la explotación de una vulnerabilidad crítica de PHP identificada como CVE-2023-3824. Además, reconoció que no se realizó la actualización de PHP debido a lo que describió como "negligencia personal e irresponsabilidad".

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/02/lockbit-ransomware-group-resurfaces.html

---

VMware pide eliminar un complemento de autenticación vulnerable y obsoleto

Una coalición de países, entre los que se encuentran Francia, el Reino Unido y Estados Unidos, junto con empresas tecnológicas como Google, MDSec, Meta y Microsoft, han firmado el acuerdo conjunto conocido como "Proceso de Pall Mall". Este esfuerzo tiene como objetivo frenar el abuso de software espía comercial para violaciones de los derechos humanos. La iniciativa busca abordar la proliferación con el uso irresponsable de herramientas de intrusión cibernéticas comerciales, estableciendo principios rectores, así como políticas para los estados, la industria y la sociedad civil relacionados con su desarrollo, facilitación, compra o uso.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/02/vmware-pide-eliminar-un-complemento-de.html

---

Fuga de software espía de China

Una filtración en GitHub ha expuesto un programa de vigilancia global dirigido por una empresa en colaboración con el gobierno chino. Esta fuga masiva revela registros de conversaciones confidenciales del Ministerio de Seguridad Pública de China (MPS).

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/02/vmware-pide-eliminar-un-complemento-de.html