GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0124

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	1	3	
MALWARE	2	3	2
NOTICIAS DE CIBERSEGURIDAD		2	1

VULNERABILIDADES

Nueva técnica maliciosa Bypass en Windows 10 y 11

Investigadores de seguridad han identificado una nueva variante de la técnica de hijacking de búsqueda de bibliotecas dinámicas (DLL) que podría ser utilizada por ciberdelincuentes para ejecutar código malicioso en sistemas con Windows 10 y 11. Esta técnica aprovecha archivos comunes en la carpeta confiable WinSxS y explota la técnica clásica de hijacking de DLL. Permite a los atacantes ejecutar código malicioso sin privilegios elevados y potencialmente introducir binarios vulnerables en la cadena de ataque. Las organizaciones deben tomar precauciones para mitigar esta explotación.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/new-variant-of-dll-search-order.html

---

Vulnerabilidad crítica en Apache OFBiz en la mira de los atacantes

La Fundación Shadowserver informa sobre intentos de explotación en la naturaleza de la vulnerabilidad crítica CVE-2023-49070 en Apache OFBiz, utilizado en proyectos como Atlassian Jira. La falla permite la elusión de autenticación o falsificación de solicitudes en el servidor, con potencial para obtener datos sensibles y ejecutar código arbitrario.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/critical-apache-ofbiz-vulnerability-in-attacker-crosshairs/

Vulnerabilidades en Google Kubernetes Engine podrían permitir la toma de control del clúster

Palo Alto Networks informa sobre dos fallos en Google Kubernetes Engine (GKE) que, cuando se combinan, podrían permitir a un atacante escalar privilegios y tomar el control del clúster Kubernetes. Las vulnerabilidades se encuentran en FluentBit, el agente de registro predeterminado en GKE, y en Anthos Service Mesh (ASM), un complemento opcional para controlar la comunicación entre servicios. Aunque no representan un riesgo significativo por sí mismas, cuando se explotan en conjunto, podrían conducir a la ejecución remota de código y al control total del clúster. Google ha lanzado parches para abordar estos problemas.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/vulnerabilities-in-google-kubernetes-engine-could-allow-cluster-takeover/

Operación triangulación: ataque a iPhones con 0-Clics y 4 Zero-Days

Investigadores descubrieron la operación "Triangulación", donde atacantes utilizan un exploit de iMessage de 0-clics con cuatro zero-days para comprometer iPhones. Los zero-days, incluyendo CVE-2023-41990 y CVE-2023-32434, permiten ejecución remota de código y escalada de privilegios. Aprovechando vulnerabilidades en JavaScriptCore y XNU, se logra el control total del dispositivo. Aunque Apple lanzó parches, el incidente destaca la complejidad de defenderse contra ataques avanzados incluso con medidas de seguridad hardware.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/operation-triangulation-0-click-imessage/

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

Malware abusa del endpoint OAuth de Google para secuestrar cuentas

Familias de malware están utilizando un punto final no documentado de OAuth de Google llamado "MultiLogin" para reactivar cookies de autenticación caducadas. Este exploit permite a los atacantes acceder a cuentas incluso después de restablecer contraseñas. Manipulando este punto final, los actores de amenazas regeneran cookies de servicio de Google caducadas, manteniendo un acceso persistente a cuentas comprometidas.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/malware-abuses-google-oauth-endpoint-to-revive-cookies-hijack-accounts/

Nuevo JinxLoader dirigido a usuarios con malware Formbook y XLoader

Un nuevo cargador de malware denominado JinxLoader está siendo empleado por ciberdelincuentes para distribuir amenazas como Formbook y XLoader. Este malware, que rinde homenaje al personaje Jinx de League of Legends, se propaga a través de correos electrónicos de phishing disfrazados de la empresa Abu Dhabi National Oil Company (ADNOC). Los correos instan a los destinatarios a abrir archivos adjuntos protegidos por contraseña, desencadenando la ejecución del JinxLoader. Este actúa como puerta de enlace para instalar Formbook o XLoader en el sistema comprometido.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/new-jinxloader-targeting-users-with.html

---

Nuevo cargador de malware Rugmi experimenta un aumento en las detecciones diarias

Se ha identificado un nuevo cargador de malware llamado Rugmi utilizado por actores de amenazas para distribuir varios programas de robo de información, como Lumma Stealer, Vidar, RecordBreaker y Rescoms. Rugmi funciona como un cargador con tres tipos de componentes: un descargador que descarga una carga útil cifrada, un cargador que ejecuta la carga útil desde recursos internos y otro cargador que ejecuta la carga útil desde un archivo externo en el disco. Los datos telemétricos muestran un aumento significativo en las detecciones de Rugmi, pasando de cifras de un solo dígito diario a cientos por día en octubre y noviembre de 2023. Rugmi se distribuye de diversas maneras, desde publicidad maliciosa hasta actualizaciones de navegador falsas y versiones pirateadas de software popular.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/12/new-rugmi-malware-loader-surges-with.html

---

Carbanak, malware bancario, resurge en ataques de ransomware

La firma de ciberseguridad NCC Group informa que Carbanak ha vuelto con nuevas cadenas de distribución, utilizando sitios web comprometidos, haciéndose pasar por software empresarial popular como HubSpot y Veeam. Se observa un aumento en los ataques de ransomware, con 442 informados solo en noviembre. Las industrias más afectadas son las industriales (33%), cíclicas de consumo (18%) y de salud (11%). Las familias de ransomware prominentes incluyen LockBit, BlackCat y Play, que representan el 47% de los ataques.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/12/carbanak-banking-malware-resurfaces.html

---

Nuevo malware nim: entregado por documento de Word weaponizado

Hackers están utilizando documentos de Word maliciosos para propagar un nuevo malware basado en Nim. Al aprovechar la familiaridad con este formato de archivo, los atacantes engañan a los usuarios mediante ingeniería social. El malware, entregado como un archivo adjunto falso de un funcionario nepalí, utiliza macros para ejecutar su carga útil. El backdoor Nim resultante imita autoridades nepalíes y se comunica con servidores C&C que simulan dominios gubernamentales.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/nim-based-malware-word-document/

"Android/Xamalicious" infecta dispositivos para tomar control absoluto

Se ha descubierto un troyano de Android conocido como "Android/Xamalicious" que utiliza el framework Xamarin para infectar dispositivos, logrando tomar control total. Este malware, que utiliza estrategias de ingeniería social para obtener privilegios de accesibilidad, se comunica con un servidor de comando y control (C2). Su segundo payload se inyecta de manera dinámica como una DLL de ensamblado, permitiéndole llevar a cabo actividades ilícitas, como fraude publicitario, instalación de aplicaciones o acciones financieras no autorizadas. A pesar de las medidas preventivas de McAfee y Google Play Protect, el troyano ha infectado al menos 327.000 dispositivos, además, sigue siendo activo en países como Estados Unidos, Brasil, Argentina, el Reino Unido, España y Alemania.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/android-malware-actively-infecting-devices/

Hackers atacan servidores Linux SSH para desplegar malware

Los hackers están enfocando sus ataques en servidores Linux SSH debido a su uso generalizado en la prestación de servicios críticos. Detectando debilidades como contraseñas frágiles, vulnerabilidades sin parchear y configuraciones incorrectas, los atacantes buscan obtener acceso no autorizado y explotar estos servidores con fines maliciosos. Investigadores del AhnLab Security Emergency Response Center (ASEC) han identificado una actividad significativa, donde los atacantes aprovechan IPs y credenciales SSH para instalar malware DDoS y CoinMiner. Algunas de las amenazas utilizadas incluyen ShellBot, Tsunami, ChinaZ DDoS Bot, XMRig CoinMiner, Mirai, Gafgyt y XorDDoS. Se recomienda tomar medidas como el fortalecimiento de contraseñas, la aplicación regular de parches de seguridad, el uso de firewalls y la precaución con las versiones de seguridad actualizadas.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/hackers-attacking-linux-ssh-servers/

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

Violación de datos a Radware desencadena fuga de información de clientes

Un reciente ataque cibernético contra Radware, empresa israelí de ciberseguridad, resultó en la filtración de datos personales de millones de israelíes. Aunque Radware fue el objetivo, los clientes, especialmente del servicio Signature-IT, sufrieron pérdidas de información, como correos electrónicos y números de teléfono.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.segu-info.com.ar/2023/12/por-operaciones-contra-israel-roban.html

---

Servicio de estafa ayuda a ciberdelincuentes en ataques de despojo a billeteras de criptomonedas

Investigadores de ciberseguridad advierten sobre un aumento en ataques de phishing capaces de vaciar billeteras de criptomonedas. Destacan la amenaza de un grupo de phishing llamado "Angel Drainer", que ofrece un "servicio de estafa" cobrando un porcentaje de la cantidad robada, generalmente del 20% al 30%. Proporcionan scripts para vaciar billeteras y otros servicios. La

tendencia preocupante también involucra servicios similares, como "Inferno Drainer". Estos kits de robo de criptomonedas facilitan el robo de cripto al transferir ilegalmente fondos de las billeteras de las víctimas sin su consentimiento.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/12/beware-scam-as-service-aiding.html

---

Chrome ahora busca contraseñas comprometidas en segundo plano

Google ha actualizado Chrome para verificar contraseñas comprometidas en segundo plano. Safety Check se ejecutará automáticamente, alertando sobre extensiones peligrosas, versión de Chrome y estado de Navegación Segura. Safety Check también revocará automáticamente permisos para sitios no visitados. Próximamente, los usuarios podrán guardar grupos de pestañas y reanudar la navegación en otros dispositivos. Los controles de rendimiento, como el modo de ahorro de memoria, se están actualizando, y Google ha mejorado la seguridad al actualizar automáticamente solicitudes HTTP inseguras a HTTPS y proporcionar protección contra phishing en tiempo real.

Prioridad: 3 Importante.

Ampliar información:

- https://blog.segu-info.com.ar/2023/12/chrome-ahora-busca-contrasenas.html

---