GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4623

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín de ciberseguridad semanal 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, tecnología y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	2	2	
MALWARE	2	3	1
NOTICIAS DE CIBERSEGURIDAD	1	1	1

VULNERABILIDADES

OwnCloud Advierte sobre 3 Vulnerabilidades Críticas

Los desarrolladores de OwnCloud, una plataforma de intercambio de archivos de código abierto, han emitido advertencias sobre tres vulnerabilidades críticas de seguridad. Estos fallos podrían exponer información sensible, permitiendo además, la modificación de archivos. Los problemas incluyen la revelación de credenciales, configuración en implementaciones en contenedores, el bypass de autenticación WebDAV Api mediante URL prefirmadas y la evasión en la validación de subdominios. Se recomienda a los usuarios aplicar las soluciones y medidas recomendadas para mitigar los riesgos asociados con estas vulnerabilidades.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/warning-3-critical-vulnerabilities.html?&web_view=true

---

Hackers de Kinsing Explotan Vulnerabilidad en Apache ActiveMQ para Desplegar Rootkits en Linux

El grupo de amenazas Kinsing está aprovechando activamente una vulnerabilidad crítica en servidores Apache ActiveMQ para infectar sistemas Linux con mineros de criptomonedas y rootkits. Esta campaña utiliza la falla CVE-2023-46604, permitiendo la ejecución remota de código y la instalación del malware Kinsing. Se recomienda a las organizaciones actualizar a versiones parcheadas de Apache ActiveMQ para mitigar posibles amenazas. Este hallazgo coincide con advertencias de AhnLab Security Emergency Response Center sobre ataques de cryptojacking dirigidos a servidores web Apache vulnerables.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/kinsing-hackers-exploit-apache-activemq.html?&web_view=true

---

Descubiertas 117 Vulnerabilidades en Microsoft 365 Apps

El equipo de ThreatLabz reveló 117 vulnerabilidades en las aplicaciones de Microsoft 365, exponiendo fallas de seguridad tras la introducción del soporte para archivos SketchUp en junio de 2022. Microsoft deshabilitó temporalmente SketchUp en junio de 2023 debido a estas vulnerabilidades, que podrían ser explotadas por atacantes para comprometer sistemas y acceder a información sensible. Se recomienda realizar auditorías de seguridad, pruebas de fuzzing y mantener actualizadas las aplicaciones de Microsoft 365 para mitigar riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/117-vulnerabilities-microsoft-365-apps/

Nuevas Vulnerabilidades Permiten a Atacantes Sortear la Autenticación de Huellas Digitales en Windows Hello

Investigadores de Blackwing Intelligence descubren múltiples vulnerabilidades que podrían ser explotadas para eludir la autenticación de Windows Hello en laptops Dell Inspiron 15, Lenovo ThinkPad T14 y Microsoft Surface Pro X. Las fallas afectan a los sensores de huellas digitales de Goodix, Synaptics y ELAN integrados en los dispositivos. Aunque estos sensores utilizan la tecnología "match on chip" para integrar funciones biométricas, los investigadores encuentran formas de suplantar la autenticación legítima. Se señalan problemas en la implementación del Protocolo de Conexión Segura de Dispositivos (SDCP) de Microsoft, permitiendo ataques de adversario en el medio (AitM). Se recomienda que los fabricantes habiliten SDCP y realicen auditorías de implementación para mitigar estos riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/new-flaws-in-fingerprint-sensors-let.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

Nuevo Malware WailingCrab se Propaga a través de Correos Temáticos

Un malware sofisticado conocido como WailingCrab, también llamado WikiLoader, está siendo distribuido a través de correos electrónicos con temáticas de envíos y entregas. Este malware, atribuido al grupo de amenazas TA544 (también conocido como Bamboo Spider o Zeus Panda), se compone de múltiples elementos, incluyendo un cargador, inyector, descargador y puerta trasera. Los correos maliciosos contienen archivos PDF que, al ser abiertos, descargan un archivo JavaScript para lanzar el cargador WailingCrab desde Discord. Este malware ha evolucionado para priorizar la furtividad, resistiendo los esfuerzos de análisis, utilizando sitios web legítimos o plataformas conocidas como Discord para sus comunicaciones de comando y control.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/alert-new-wailingcrab-malware-loader.html?&web_view=true

---

ParaSiteSnatcher: Amenaza Latente en Extensiones de Chrome

Investigaciones recientes revelan la presencia de la extensión maliciosa "ParaSiteSnatcher", diseñada para apuntar a usuarios en América Latina, especialmente en Brasil. Esta extensión utiliza tácticas sofisticadas para interceptar y exfiltrar datos sensibles, centrándose en URLs relacionadas con instituciones financieras brasileñas o métodos de pago específicos. Los usuarios deben estar alerta al descargar extensiones y ser conscientes de la persistencia del sigilo de amenazas como ParaSiteSnatcher.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.trendmicro.com/en_us/research/23/k/parasitesnatcher-how-malicious-chrome-extensions-target-brazil-.html?&web_view=true

---

Amenaza a Usuarios de Mac: Atomic Stealer se Distribuye Mediante Falsas Actualizaciones de Navegadores

Atomic Stealer, conocido como AMOS, ha dado un paso audaz al llegar a usuarios de Mac a través de una cadena de actualizaciones de navegador falsas denominada 'ClearFake'. Esta táctica, anteriormente reservada para Windows, amplía su alcance geográfico y se dirige a sistemas operativos de Mac. ClearFake utiliza sitios comprometidos para distribuir actualizaciones de navegador falsas, siendo una de las campañas de ingeniería social más peligrosas. Los usuarios de Mac deben estar alerta, ya que la popularidad de amenazas como AMOS facilita la adaptación de cargas útiles a diferentes víctimas con ajustes mínimos.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.malwarebytes.com/blog/threat-intelligence/2023/11/atomic-stealer-distributed-to-mac-users-via-fake-browser-updates?&web_view=true

---

LummaC2 Despliega Nueva Técnica Anti-Sandbox Basada en Trigonometría

El malware LummaC2, también conocido como Lumma Stealer, ha introducido una nueva técnica anti-sandbox que utiliza la trigonometría para evadir la detección y robar información de dispositivos infectados. Esta táctica detecta la actividad humana al considerar las posiciones del cursor, retrasando su ejecución hasta que se detecte un comportamiento humano. LummaC2 se ha actualizado continuamente desde su aparición en diciembre de 2022, y la versión actual (v4.0) requiere que los usuarios utilicen un "crypter" para mayor ocultamiento y seguridad contra fugas de datos. La evolución de este tipo de amenazas destaca la importancia de mantenerse alerta ante nuevas tácticas utilizadas por actores malintencionados en el ciberespacio.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/lummac2-malware-deploys-new.html

---

Nuevo Variante de Agent Tesla Utiliza Compresión ZPAQ en Ataques de Correo Electrónico

Un nuevo tipo del malware Agent Tesla se ha identificado siendo entregado a través de un archivo señuelo con formato de compresión ZPAQ. Este malware, utilizado como parte de un modelo de malware como servicio (MaaS), busca recolectar datos de múltiples clientes de correo electrónico y casi 40 navegadores web. Este desarrollo resalta la tendencia de los actores de amenazas a experimentar con formatos de archivo no convencionales, subrayando la importancia de que los usuarios estén alerta ante correos electrónicos sospechosos y mantengan sus sistemas actualizados.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/new-agent-tesla-malware-variant-using.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

Tácticas de Phishing Multietapa: Explotando Códigos QR, CAPTCHAs y Esteganografía

En la evolución constante del phishing, los ciberdelincuentes ahora emplean tácticas avanzadas como "Quishing" con códigos QR maliciosos, el uso de CAPTCHAs para ocultar formularios de robo de credenciales y campañas de malware con esteganografía. Estas técnicas sofisticadas buscan eludir las defensas tradicionales.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/how-multi-stage-phishing-attacks.html?&web_view=true

---

Hackers Usan WhatsApp para Instalar Malware en Android

Microsoft revela campañas de troyanos bancarios en India, explotando a usuarios a través de WhatsApp. Los atacantes distribuyen archivos APK maliciosos directamente, evitando enlaces convencionales. Dos casos destacan ataques de phishing en WhatsApp y robo de datos de tarjetas de crédito. La exposición destaca la necesidad de vigilancia, generando defensas proactivas ante la evolución de amenazas. Microsoft insta a la atención a signos de infección y medidas preventivas en el cambiante panorama cibernético.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/hackers-abusing-whatsapp-messages/

Sextorsión: lo que todo padre necesita saber

La sextorsión, una forma de chantaje sexual que involucra la amenaza de compartir imágenes íntimas, afecta a adolescentes globalmente. En un caso típico, los jóvenes son engañados para enviar imágenes comprometedoras, y los chantajistas exigen dinero o más contenido sexual bajo la amenaza de hacer públicas las imágenes. Este fenómeno, impulsado en parte por organizaciones criminales, destaca la importancia de la prevención, incluyendo configurar la privacidad en redes sociales, fomentando una comunicación abierta con los hijos. En caso de que un adolescente sea víctima de sextorsión, se aconseja brindar apoyo, recopilar evidencia, informar a las autoridades y detener cualquier contacto con el chantajista sin ceder a sus demandas.

Prioridad: 3 Importante.

Ampliar información:

- https://www.mcafee.com/blogs/internet-security/sextortion-what-every-parent-needs-to-know/
