GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2123

En alianza con

TD SYNNEX FORTINET

BOLETIN 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
VULNERABILIDADES	2	1	
MALWARE	2		4
BRECHAS DE SEGURIDAD	1		
NOTICIAS DE CIBERSEGURIDAD	1		1
SECTOR GOBIERNO	1		

VULNERABILIDADES

Dispositivos de seguridad de correo electrónico Barracuda pirateados a través de una vulnerabilidad de día cero (CVE-2023-2868)

Una vulnerabilidad (CVE-2023-2868) en los dispositivos Email Security Gateway (ESG) de Barracuda Networks ha sido explotada por atacantes, advirtió la compañía.

Esta vulnerabilidad surge de una falla en la desinfección integral del procesamiento del archivo .tar. La vulnerabilidad se deriva de la validación de entrada incompleta de un archivo .tar proporcionado por el usuario en lo que respecta a los nombres de los archivos contenidos en el archivo. Como consecuencia, un atacante remoto puede formatear

específicamente estos nombres de archivo de una manera particular que resultará en la ejecución remota de un comando del sistema. Este problema se solucionó como parte del parche BNSF-36456, el cual se aplicó automáticamente a todos los dispositivos de los clientes.

Prioridad: 1 Crítico.

Ampliar información:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2868
- https://status.barracuda.com/incidents/34kx82j5n4q9
- https://www.helpnetsecurity.com/2023/05/25/cve-2023-2868/
- https://noticiasseguridad.com/seguridad-informatica/barracuda-una-grande-empresa-de-ciberseguridad-fue-hackeada/
- https://www.cisa.gov/news-events/alerts/2023/05/26/cisa-adds-one-known-exploited-vulnerability-catalog

---

Blacktail Threat Actor aprovecha la vulnerabilidad de PaperCut (CVE-2023-27350) para distribuir el ransomware Buhti

FortiGuard Labs está al tanto de un informe de que el actor de amenazas Blacktail explotó la vulnerabilidad PaperCut recientemente parcheada (CVE-2023-27350) para distribuir la versión de Windows del ransomware Buhti. La vulnerabilidad de ejecución de código de IBM Aspera Faspex (CVE-2022-47986) también está siendo explotada por el mismo actor de amenazas.

¿Qué es la vulnerabilidad PaperCut (CVE-2023-27350)?

CVE-2023-27350 es una vulnerabilidad de omisión de autenticación en PaperCut NG debido a un control de acceso inadecuado en la aplicación vulnerable. Un atacante remoto

no autenticado puede aprovechar esto a través de una solicitud manipulada. La explotación exitosa podría conducir a la ejecución de código arbitrario dentro del contexto de seguridad del sistema afectado.

Prioridad: 1 Crítico.

Ampliar información:

- https://fortiguard.fortinet.com/threat-signal-report/5170

Hackear gitlab con vulnerabilidad permite filtrar código, contraseñas de usuario, tokens

GitLab Inc. es una corporación que ejecuta GitLab, un paquete de software que se puede usar para crear, proteger y administrar software. Los proyectos grandes de DevOps y DevSecOps pueden beneficiarse del uso de GitLab, ya que proporciona un lugar para el código fuente abierto y una plataforma para el desarrollo de software colaborativo. Además, esta es una plataforma que proporciona un espacio para el almacenamiento en línea de código, así como herramientas para el seguimiento de errores y CI/CD. Se ha encontrado que GitLab Community Edition y Enterprise Edition tienen un problema, aunque la versión 16.0.0 es la única que afecta.

Prioridad: 2 Urgente.

Ampliar información:

- https://noticiasseguridad.com/importantes/hackear-gitlab-con-esta-vulnerabilidad-permite-filtrar-codigo-contrasenas-de-usuario-tokens/

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

Millones de televisores Android TV y teléfonos vendrían con malware preinstalado de fábrica

Existe un enorme número de fabricantes desconocidos cuyos productos no son sometidos al mismo escrutinio que los de las grandes firmas, y un artículo de ArsTechnica ayuda a comprender mejor sus riesgos: millones de televisores, reproductores multimedia y teléfonos basados en Android con *malware* instalado de serie.

Prioridad: 3 Importante.

Ampliar información:

- https://arstechnica.com/information-technology/2023/05/potentially-millions-of-android-tvs-and-phones-come-with-malware-preinstalled/
- https://blog.elhacker.net/2023/05/malware-preinstalado-millones-telefonos-tv-android.html
- https://www.elotrolado.net/noticias/tecnologia/malware-preinstalado-televisores-android-tv-telefonos-baratos

---

Mirai botnet está de vuelta con una nueva versión iz1h9 ¿cómo detectarlo?

Los investigadores de Unit42 descubrieron una versión de Mirai conocida como IZ1H9 que explotaba muchas vulnerabilidades para propagarse. Los actores de amenazas explotan las siguientes vulnerabilidades para atacar servidores Linux desprotegidos y dispositivos de red que ejecutan el sistema operativo:

Vulnerabilidad de inyección de comando Tenda G103, denominada CVE-2023-27076. Vulnerabilidad de inyección de comando LB-Link, también conocida como CVE-2023-26801.
CVE-2023-26802: vulnerabilidad de ejecución remota de código DCN DCBI-Netlog-LAB Vulnerabilidad de ejecución remota de código Zyxel.

Prioridad: 2 Crítico.

Ampliar información:

- https://noticiasseguridad.com/malware-virus/mirai-botnet-esta-de-vuelta-con-una-nueva-version-iz1h9-como-detectarlo/

Predator, otro spyware mercenario

Con el nombre de PREDATOR y en honor a la famosa figura del mundo del cine, se le conoce a un spyware cuyo funcionamiento y existencia ha sido revelado desde no hace mucho tiempo y que ha afectado a personalidades de varias partes del mundo. El software espía puede grabar llamadas telefónicas, recopilar información de aplicaciones de mensajería o incluso ocultar aplicaciones e impedir su ejecución en dispositivos Android infectados.

Prioridad: 3 Importante.

Ampliar información:

- https://blog.talosintelligence.com/mercenary-intellexa-predator/
- https://elchapuzasinformatico.com/2023/05/predator-spyware/
- https://www.bleepingcomputer.com/news/security/predator-looking-under-the-hood-of-intellexas-android-spyware/

El nuevo ransomware Buhti usa payloads filtrados y exploits públicos

Una operación de ransomware recientemente identificada ha remodelado las cargas útiles filtradas de LockBit y Babuk en el ransomware Buhti, para lanzar ataques en sistemas Windows y Linux.

Prioridad: 3 Importante.

Ampliar información:

- https://www.helpnetsecurity.com/2023/05/26/buhti-ransomware/

El malware QBot utiliza del EXE de WordPad en Windows para cargar una DLL maliciosa y evitar ser detectado

El malware QBot ha comenzado a abusar de secuestro de DLL en el programa WordPad de Windows 10 para infectar ordenadores, utilizando el programa legítimo para evadir la detección del software de seguridad.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/qbot-malware-abuses-windows-wordpad-exe-to-infect-devices/
- https://blog.elhacker.net/2023/05/el-malware-qbot-utiliza-del-exe-de-Wordpad-secuestro-DLL.html

---

Royal Ransomware activo en América Latina

Si bien es de esperar la evolución de las técnicas de ransomware, la velocidad a la que Royal Ransomware Group ha podido adaptarse es impresionante. Desde que se informó por primera vez, los responsables del ransomware Royal han avanzado rápidamente durante un corto período de tiempo, aprovechando técnicas antiguas y nuevas, así como explotando nuevas vulnerabilidades a medida que se descubren. Solo en los últimos seis

meses, han escalado rápidamente los ataques dirigidos a víctimas en numerosas industrias y países, incluidos América Latina.

Prioridad: 2 Crítico.

Ampliar información:

- https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware
- https://unit42.paloaltonetworks.com/royal-ransomware/
- https://blogs.vmware.com/security/2023/03/unveiling-the-evolution-of-royal-ransomware.html
- https://blog.segu-info.com.ar/2023/05/royal-ransomware-activo-en-america.html

---

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

Posible fuga masiva de Tesla prueba la invasión a la privacidad de sus usuarios

Tesla no ha podido proteger adecuadamente los datos de los clientes, empleados y socios comerciales y ha recibido miles de quejas de sus clientes con respecto al sistema de asistencia al conductor del fabricante de automóviles, informó el medio Handelsblatt de Alemania, citando 100 gigabytes de datos confidenciales filtrados por un denunciante.

Prioridad: 1 Crítica

Ampliar información:

- https://blog.segu-info.com.ar/2023/05/posible-fuga-masiva-de-tesla-prueba-la.html
- https://www.theguardian.com/technology/2023/may/26/tesla-data-leak-customers-employees-safety-complaints

NOTICIAS DE CIBERSEGURIDAD

Colombia: Senadores proponen la creación de una Agencia Nacional de Seguridad Digital

Los senadores David Luna y Ana Maria Castañeda presentaron un proyecto de ley para crear una Agencia Nacional de Seguridad Digital con el objetivo de combatir el cibercrimen y los ciberataques en Colombia.

David Luna, senador de Colombia, recientemente compartió en sus redes un comunicado sobre un nuevo proyecto de ley que él y la senadora Ana María Castañeda han presentado. El proyecto tiene como objetivo crear una **Agencia Nacional de Seguridad Digital** para combatir el cibercrimen y los ciberataques a los que Colombia se enfrenta actualmente.

Prioridad: 2 Crítico.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/05/23/colombia-senadores-proponen-la-creacion-de-una-agencia-nacional-de-seguridad-digital/
- https://twitter.com/i/web/status/1661007249660329985

Videollamadas con el rostro y la voz clonada para pedir dinero: las estafas con inteligencia artificial se disparan en China

Un estafador chino utilizó la inteligencia artificial para hacerse pasar por un amigo de confianza de un empresario y convencerle de que le entregara 4,3 millones de yuanes (609.000 dólares), según han declarado las autoridades.

Prioridad: 3 Importante.

Ampliar información:

- https://www.infobae.com/america/mundo/2023/05/25/fraude-con-inteligencia-artificial-en-china-se-hizo-pasar-por-el-amigo-de-un-empresario-y-le-robo-usd-600-mil/
- https://blog.elhacker.net/2023/05/videollamadas-con-la-cara-y-la-voz-clonada-inteligencia-artificial-estafas-china.html