GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición º1024

En alianza con

TD SYNNEX FORTINET

# BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

Bienvenidos a su boletín semanal de inteligencia de amenazas de Gamma Ingenieros, en este boletín se compartirán noticias y vulnerabilidades más importantes y críticas relevantes para nuestras operaciones y aliados de negocio.

Aquí encontraras información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados.

## VISTA RÁPIDA

| | CRITICO | URGENTE | IMPORTANTE |
|---|---|---|---|
| VULNERABIILIDADES | 1 | 1 | 3 |
| MALWARE | 0 | 1 | 5 |
| NOTICIAS DE CIBERSEGURIDAD | 0 | 0 | 6 |

## VULNERABILIDADES

### Recompensa de 2.063 por Vulnerabilidad de Inyección SQL no Autenticada Parcheado en el Complemento de WordPress Ultimate Member

El 30 de enero de 2024, en el contexto de nuestro segundo Bug Bounty Extravaganza, se nos notificó la existencia de una vulnerabilidad crítica. Esta vulnerabilidad, una inyección SQL no autenticada, fue identificada en Ultimate Member, un renombrado complemento de WordPress con una base de usuarios que supera las 200.000 instalaciones activas. Esta vulnerbailidad representa una amenaza significativa, ya que permite el acceso no autorizado a la base de datos, potencialmente exponiendo datos sensibles, incluidos los hashes de contraseñas.

**Prioridad:** 1 Critico.

**Ampliar información:**

https://www.wordfence.com/blog/2024/02/2063-bounty-awarded-for-unauthenticated-sql-injection-vulnerability-patched-in-ultimate-member-wordpress-plugin/

---

## Vulnerabilidad XSS en el Complemento LiteSpeed Cache que Afecta a 4+ millones de Sitios

Esta publicación de blog aborda la crítica vulnerabilidad encontrada en el complemento LiteSpeed. En caso de ser un usuario de LiteSpeed, es de suma importancia que proceda con la actualización del plugin a la versión mínima 5.7.0.1 para garantizar la seguridad de sus sistemas.

**Prioridad:** 2 Urgente.

**Ampliar información:**

https://thehackernews.com/2024/02/wordpress-litespeed-plugin.htm/

---

## Múltiples Vulnerabilidades en Adobe Acrobat Reader Podrían Conducir a Ejecución de Código

En febrero, Cisco Talos ha identificado más de 30 vulnerabilidades, destacando entre ellas siete que afectan a Adobe Acrobat Reader, una herramienta de edición y visualización de PDF ampliamente utilizada. Estas vulnerabilidades representan una seria amenaza, ya que podrían ser aprovechadas por adversarios para provocar la liberación de objetos previamente utilizados, dando lugar a la corrupción de memoria y potencialmente permitiendo la ejecución de código arbitrario en la máquina objetivo.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://blog.talosintelligence.com/vulnerability-roundup-feb-27-2024

---

## Las Vulnerabilidades de las VPN Empresariales en el Punto de Mira

Con el aumento del interés de los adversarios en vulnerabilidades presentes en el software VPN empresarial como medio para infiltrarse en redes corporativas, se intensifica la preocupación sobre si las propias VPN representan una amenaza cibernética significativa.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.welivesecurity.com/en/business-security/vulnerabilities-business-vpns-spotlight

---

## Vulnerabilidad de Ejecución Remota de Código de Microsoft Outlook

El equipo de investigación de amenazas de SonicWall Capture Labs ha descubierto la vulnerabilidad de ejecución remota de código MonikerLink (CVE-2024-21413) en Microsoft Outlook. Tras evaluar su impacto, se han implementado medidas de mitigación para abordar esta vulnerabilidad.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://blog.sonicwall.com/en-us/2024/02/microsoft-outlook-remote-code-execution-vulnerability/

---

**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

### LockBit de Regreso

Tan solo cinco días después de una operación internacional liderada por las fuerzas del orden que clausuró los sitios de filtraciones de LockBit, se ha observado el resurgimiento del grupo. LockBit3.0 ha reaparecido con un nuevo sitio en Tor, el cual guarda similitud con su predecesor. Actualmente, se han identificado al menos media docena de entradas en este nuevo sitio. Entre ellas, destaca un nuevo registro relacionado con el condado de Fulton,

Georgia, un objetivo previamente atacado a fines de enero y nuevamente comprometido a mediados de febrero.

**Prioridad:** 2 Urgente.

**Ampliar información:**

https://securityaffairs.com/159584/cyber-crime/lockbit-gang-resumed-raas.html

---

## Nood RAT utilizado en Ataques Contra Linux (variante de Gh0st RAT)

Recientemente, el Centro de Inteligencia de Seguridad de AhnLab (ASEC) ha identificado el uso del malware Nood RAT en ataques cibernéticos. Nood RAT, una variante de Gh0st RAT diseñada para operar en sistemas Linux, ha llamado la atención de los investigadores. Aunque el número de instancias de Gh0st RAT para Linux es menor en comparación con su contraparte para Windows, la recopilación de casos de Gh0st RAT para Linux es un fenómeno en constante crecimiento.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://asec.ahnlab.com/en/62144/

---

## CISA, NCSC-UK y sus Socios Publican un Aviso Sobre los Actores Rusos de SVR Orientación a la Infraestructura en la Nube

La Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA), en colaboración con el Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC) y otros organismos asociados, ha lanzado un aviso conjunto titulado "SVR Cyber Actors Adapt Tactics for Initial Cloud Access". Este aviso detalla las tácticas, técnicas y procedimientos (TTP) más

recientes empleados por los actores cibernéticos del Servicio de Inteligencia ruso (SVR), también conocidos como APT29, Dukes, CozyBear y NOBELIUM/Midnight Blizzard, para obtener acceso inicial a entornos en la nube.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.cisa.gov/news-events/alerts/2024/02/26/cisa-ncsc-uk-and-partners-release-advisory-russian-svr-actors-targeting-cloud-infrastructure

---

## Ransomware - Abyss Locker

Cada quince días, FortiGuard Labs recopila datos sobre las variantes de ransomware más relevantes, que han ido ganando notoriedad tanto dentro de nuestros propios conjuntos de datos como en la comunidad OSINT. El informe Ransomware Roundup tiene como objetivo brindar a los lectores una visión concisa del panorama en constante evolución del ransomware, así como destacar las soluciones de Fortinet diseñadas para proteger contra estas variantes.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.fortinet.com/blog/threat-research/ransomware-roundup-abyss-locker

---

## Phishing que envía información robada mediante la API de Telegram

El año pasado, el Centro de Inteligencia de Seguridad de AhnLab (ASEC) identificó archivos de script de phishing que empleaban Telegram para filtrar información de usuarios.

Recientemente, se han detectado múltiples scripts de phishing que utilizan Telegram y se distribuyen indiscriminadamente mediante palabras clave como "remesas" y "recibos".

**Prioridad:** 3 Importante.

**Ampliar información:**

https://asec.ahnlab.com/en/62177/

---

## Black Basta, está Explotando las Recientes Vulnerabilidades de ScreenConnect

En esta entrada de blog, presentamos un análisis exhaustivo de las vulnerabilidades más recientes descubiertas en ScreenConnect. Además, abordamos nuestro hallazgo sobre grupos de actores de amenazas, entre ellos las bandas Black Basta y Bl00dy Ransomware, que están explotando activamente las vulnerabilidades CVE-2024-1708 y CVE-2024-1709, según nuestra telemetría.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.securityweek.com/black-basta-bl00dy-ransomware-exploiting-recent-screenconnect-flaws

---

## 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

### La banda de Ransomware LockBit tiene más de USD 110 millones en Bitcoin sin gastar

En ScreenConnect. Además, abordamos nuestro hallazgo sobre grupos de actores de amenazas, entre ellos las bandas Black Basta y Bl00dy Ransomware, que están explotando activamente las vulnerabilidades.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-has-over-110-million-in-unspent-bitcoin/

---

### El Panorama de las Amenazas de Malware Móvil en 2023

Las cifras mencionadas anteriormente se fundamentan en las estadísticas de detección recopiladas de los usuarios de Kaspersky que han otorgado su consentimiento para compartir datos de uso con Kaspersky Security Network. Es importante señalar que los

datos anteriores a 2023 podrían variar con respecto a los informes previamente publicados, ya que la metodología de cálculo ha sido refinada y revisada retrospectivamente en 2023.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.infosecurity-magazine.com/news/expert-warns-growing-android/

---

## Informe Anual de Alertas de Brotes de FortiGuard Labs 2023: un Vistazo a la Panorama de Amenazas en Evolución

En el dinámico entorno de amenazas actual, mantenerse informado y ser proactivo es crucial para cualquier organización que busque proteger sus redes. El Informe Anual de Alertas de Brotes de FortiGuard Labs 2023 es un recurso integral que examina ejemplos reales de ataques en diversas verticales, proporcionando información valiosa sobre los ciberataques más relevantes del año pasado y ofreciendo datos críticos que las organizaciones pueden utilizar para evaluar su postura en ciberseguridad.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.fortinet.com/blog/threat-research/fortiguard-labs-outbreak-alerts-report-2023

---

## Desenmascarando el Panorama de la Seguridad del Correo Electrónico en 2024

En el siempre cambiante ámbito digital, mantenerse al tanto de las tendencias de amenazas en evolución es esencial para las organizaciones que buscan proteger sus activos. En este panorama dinámico, el correo electrónico emerge como un campo de batalla principal para la defensa cibernética. El último informe del Grupo de Seguridad

VIPRE, "Seguridad del correo electrónico en 2024: Una visión experta de las amenazas del correo electrónico", explora en detalle las tácticas y tecnologías de vanguardia adoptadas por los ciberdelincuentes este año.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://securityaffairs.com/159710/hacking/unmasking-2024s-email-security-landscape.html

---

## Los Staques de Vishing, Smishing y Phishing se Disparan un 1.265% tras ChatGPT

El 76% de las empresas se enfrentan a una falta de protección adecuada contra el fraude de voz y mensajería, especialmente ante el aumento del vishing impulsado por IA y el smishing, que ha experimentado un notable aumento tras el lanzamiento de ChatGPT.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://www.helpnetsecurity.com/2024/02/29/mobile-fraud-losses

---

## Cómo Priorizar el Gasto en Ciberseguridad: una Estrategia Basada en el Riesgo para el ROI más Alto

Como líder de TI, es fundamental mantenerse al día con los últimos avances en ciberseguridad para garantizar la seguridad de su organización. Con amenazas que surgen constantemente y hackers que están constantemente desarrollando nuevos exploits, la pregunta es: ¿cómo podemos crear estrategias proactivas y ágiles de ciberseguridad? Además, ¿cómo podemos asegurarnos de obtener el máximo rendimiento

de nuestra inversión en ciberseguridad, mitigando los riesgos y maximizando el valor de nuestras inversiones?.

**Prioridad:** 3 Importante.

**Ampliar información:**

https://thehackernews.com/2024/02/why-risk-based-approach-to.html

---