GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1225

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	0	4	0
MALWARE	0	3	0
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Explotan día cero de Chrome en la Operación ForumTroll

Investigadores de Kaspersky descubrieron a mediados de marzo de 2025 una sofisticada campaña de ataque denominada "Operación ForumTroll", en la que un grupo de amenazas persistentes avanzadas (APT) explotó una vulnerabilidad de día cero en Google Chrome, identificada como CVE-2025-2783. Esta vulnerabilidad permitía a los atacantes eludir las protecciones de sandbox de Chrome, esenciales para aislar y contener código malicioso. El ataque se iniciaba mediante correos electrónicos de phishing personalizados que dirigían a las víctimas a enlaces maliciosos; al abrirlos en Chrome, el sistema se infectaba sin necesidad de interacción adicional del usuario.

Los objetivos principales de esta operación fueron medios de comunicación e instituciones educativas en Rusia, sugiriendo que el propósito principal era el espionaje. La sofisticación del malware y las tácticas empleadas indican la participación de un grupo APT patrocinado

por un estado. Tras el informe de Kaspersky, Google lanzó una actualización el 25 de marzo de 2025 para corregir la vulnerabilidad, bloqueando efectivamente la cadena de ataque. Se recomienda a los usuarios actualizar Chrome a la versión más reciente para protegerse contra esta amenaza.

Prioridad: Urgente.

Ampliar Información:

https://gbhackers.com/apt-hackers-exploit-google-chrome-zero-day/

Vulnerabilidad en Security Fabric expone productos Fortinet a ataques remotos

Fortinet ha identificado una vulnerabilidad de "traversal de directorios" (CWE-22) en el demonio csfd que afecta a varios de sus productos, incluyendo FortiManager, FortiOS, FortiProxy, FortiRecorder, FortiVoice y FortiWeb. Esta vulnerabilidad podría permitir que un atacante remoto autenticado, con acceso a la interfaz y al puerto del Security Fabric, escriba archivos arbitrarios. Además, un atacante remoto no autenticado con el mismo acceso podría eliminar carpetas arbitrarias.

Fortinet ha lanzado actualizaciones para mitigar esta vulnerabilidad en las versiones afectadas de sus productos. Se recomienda encarecidamente a los usuarios que actualicen a las versiones corregidas según las indicaciones proporcionadas. Como medida alternativa, se puede deshabilitar el Security Fabric para mitigar el riesgo. Para más detalles sobre las versiones afectadas y las soluciones específicas, consulte el aviso oficial de Fortinet.

Prioridad: Urgente.

Ampliar Información:

https://www.fortiguard.com/psirt/FG-IR-24-259

Hackers explotan falla de PHP para implementar Quasar RAT y mineros XMRig

Investigadores de Bitdefender han detectado una explotación activa de la vulnerabilidad CVE-2024-4577 en PHP, que afecta a sistemas Windows operando en modo CGI. Esta falla permite a atacantes remotos ejecutar código arbitrario, facilitando la instalación de malware como el minero de criptomonedas XMRig y el troyano de acceso remoto Quasar RAT.

Se ha observado que aproximadamente el 5% de los ataques culminan en la instalación de XMRig, mientras que otros despliegan Quasar RAT o ejecutan archivos MSI maliciosos desde servidores remotos. Curiosamente, algunos atacantes modifican configuraciones de firewall en los servidores comprometidos para bloquear accesos desde IPs maliciosas conocidas, posiblemente para evitar competencia de otros grupos. Se recomienda actualizar las instalaciones de PHP a la versión más reciente y restringir el uso de herramientas como PowerShell a usuarios privilegiados para mitigar estos riesgos.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/03/hackers-exploit-severe-php-flaw-to.html

---

El plugin de WordPress WP Ghost es vulnerable a un error de ejecución remota de código

El plugin de seguridad para WordPress, WP Ghost, ha sido identificado con una vulnerabilidad crítica que podría permitir a atacantes no autenticados ejecutar código de forma remota y tomar el control de servidores afectados. Este fallo, catalogado como CVE-2025-26909 con una puntuación CVSS de 9.6, afecta a todas las versiones hasta la 5.4.01 y se origina por una validación insuficiente de entradas en la función 'showFile()'. La

explotación de esta vulnerabilidad es posible cuando la función "Change Paths" del plugin está configurada en los modos Lite o Ghost, aunque estos no están habilitados por defecto.

Tras el descubrimiento de este fallo por el investigador Dimas Maulana el 25 de febrero de 2025, Patchstack notificó al proveedor el 3 de marzo. Al día siguiente, los desarrolladores de WP Ghost lanzaron la versión 5.4.02, incorporando una validación adicional en las URL o rutas proporcionadas por los usuarios para corregir la vulnerabilidad. Se recomienda a los usuarios actualizar a la última versión disponible para mitigar el riesgo asociado a CVE-2025-26909.

Prioridad: Urgente.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/wordpress-security-plugin-wp-ghost-vulnerable-to-remote-code-execution-bug/

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
2. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
3. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
4. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

El ransomware Medusa utiliza un controlador malicioso para desactivar el antimalware

Investigadores de Elastic Security Labs han identificado que el grupo detrás del ransomware Medusa está utilizando un controlador malicioso denominado ABYSSWORKER para desactivar herramientas de seguridad en sistemas comprometidos. Este controlador, "smuol.sys", imita al legítimo "CSAgent.sys" de CrowdStrike Falcon y está firmado con certificados revocados, probablemente robados de empresas chinas, lo que le permite evadir las defensas de seguridad.

El ataque se lleva a cabo mediante la técnica "Bring Your Own Vulnerable Driver" (BYOVD), donde los atacantes instalan un controlador vulnerable en el sistema objetivo para obtener privilegios elevados y desactivar soluciones de detección y respuesta de endpoints (EDR). Una vez que ABYSSWORKER está activo, puede realizar diversas operaciones, como manipulación de archivos y terminación de procesos, facilitando la desactivación de sistemas EDR y permitiendo el despliegue del ransomware Medusa sin ser detectado.

Prioridad: Importante.

https://thehackernews.com/2025/03/medusa-ransomware-uses-malicious-driver.html

---

Extensiones de VSCode que descargaban ransomware en etapa inicial

Dos extensiones maliciosas fueron detectadas en el Marketplace de Visual Studio Code (VSCode), bajo los nombres "ahban.shiba" y "ahban.cychelloworld", las cuales contenían comandos de PowerShell diseñados para descargar y ejecutar scripts desde un servidor remoto alojado en Amazon AWS. Aunque el ransomware involucrado se encontraba en una etapa temprana de desarrollo y solo cifraba archivos dentro de una carpeta de prueba,

este incidente expone fallos importantes en los controles de seguridad del ecosistema de extensiones de VSCode.

Estas extensiones estuvieron disponibles durante un periodo prolongado antes de ser finalmente retiradas tras ser reportadas. Este incidente subraya la necesidad urgente de reforzar los mecanismos de verificación y control en los marketplaces de software, en especial aquellos dirigidos a entornos de desarrollo, donde una extensión maliciosa puede comprometer gravemente la seguridad de sistemas críticos.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/vscode-extensions-found-downloading-early-stage-ransomware/

Descubren cerca de 200 dominios C2 vinculados al malware Raspberry Robin

Una investigación reciente ha identificado cerca de 200 dominios únicos de comando y control (C2) asociados con el malware conocido como Raspberry Robin. Este malware, también denominado Roshtyak o Storm-0856, actúa como un corredor de acceso inicial para diversos grupos criminales, muchos de ellos vinculados a Rusia. Desde su aparición en 2019, Raspberry Robin ha facilitado la distribución de otras amenazas como SocGholish, Dridex, LockBit, IcedID, BumbleBee y TrueBot. Es conocido también como el "gusano QNAP" debido al uso de dispositivos QNAP comprometidos para obtener sus cargas útiles.

El análisis reveló que Raspberry Robin utiliza dominios C2 cortos, como q2[.]rs, m0[.]wf y h0[.]wf, que rotan rápidamente entre dispositivos comprometidos mediante una técnica llamada "fast flux", dificultando su eliminación. Los dominios están registrados en TLDs como .wf, .pm, .re, .nz y .eu, utilizando registradores específicos. Además, se ha observado que el actor de amenazas ruso Cadet Blizzard podría haber empleado Raspberry Robin para

facilitar accesos iniciales, alineándose con su historial de colaboración con otros actores maliciosos con conexiones rusas.

Prioridad: Importante

Ampliar Información:

https://thehackernews.com/2025/03/researchers-uncover-200-unique-c2.html

---

Recomendaciones generales sobre malware:

Para protegerse contra malware, es esencial:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Ciberataque afecta al operador ferroviario nacional de Ucrania

La empresa ferroviaria estatal de Ucrania, Ukrzaliznytsia, sufrió un ciberataque a gran escala que afectó sus servicios en línea, incluyendo la venta de boletos y operaciones de

carga. Aunque el tráfico ferroviario continuó sin interrupciones, los pasajeros se vieron obligados a comprar boletos en las estaciones debido a la caída del sistema en línea. La compañía implementó temporalmente la gestión de documentos en papel y está trabajando con especialistas en TI para restaurar completamente los servicios afectados.

Funcionarios de seguridad ucranianos, bajo condición de anonimato, indicaron que el ataque parece haber sido llevado a cabo por Rusia. Este incidente subraya la creciente amenaza de ciberataques dirigidos a infraestructuras críticas en Ucrania, especialmente en el contexto del conflicto en curso con Rusia.

Prioridad: Importante.

Ampliar Información:

https://securityaffairs.com/175810/hacking/cyberattack-hit-ukraines-national-railway-operator.html

---

Campaña mundial de HellCat apunta a servidores Jira expuestos

Un grupo de hackers conocido como HellCat ha llevado a cabo una serie de ataques dirigidos a servidores Jira en todo el mundo, utilizando credenciales comprometidas para acceder a sistemas internos de diversas organizaciones. Uno de los casos más destacados es el de Ascom, una empresa suiza de soluciones globales, que confirmó una brecha en su infraestructura de TI el 20 de marzo de 2025. Los atacantes lograron acceder a su sistema de gestión de incidencias técnicas y sustrajeron aproximadamente 44 GB de datos, incluyendo código fuente de múltiples productos, detalles de proyectos, facturas y documentos confidenciales.

Este patrón de ataque no es aislado. HellCat también ha sido vinculado a brechas en otras empresas, como Schneider Electric y Telefónica, donde se infiltraron en servidores Jira y extrajeron grandes volúmenes de datos sensibles. Estos incidentes resaltan la importancia de proteger adecuadamente las plataformas de gestión de proyectos y seguimiento de

incidencias, ya que suelen contener información crítica. Se recomienda a las organizaciones revisar y fortalecer sus políticas de seguridad, especialmente en lo que respecta a la gestión de credenciales y la protección de sistemas accesibles desde Internet.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/hellcat-hackers-go-on-a-worldwide-jira-hacking-spree/
