GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °1325

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	2	1
MALWARE	0	2	1
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Omisión de autenticación en el módulo websocket de Node.js y solicitudes CSF

La vulnerabilidad FG-IR-24-535 afecta a FortiOS y permite a un atacante ejecutar comandos arbitrarios en el sistema a través de peticiones HTTP especialmente diseñadas, debido a una vulnerabilidad de inyección de comandos en la interfaz de administración web. Esta vulnerabilidad ha sido clasificada como crítica, con una puntuación CVSS de 9.3, ya que permite la ejecución remota de código sin autenticación previa. Los productos afectados incluyen versiones específicas de FortiOS y FortiProxy.

Fortinet ha publicado actualizaciones de seguridad para corregir esta vulnerabilidad y recomienda encarecidamente a los usuarios que actualicen a las versiones parcheadas lo antes posible para evitar posibles ataques. Además, se recomienda limitar el acceso a la interfaz de administración a direcciones IP de confianza como medida de mitigación.

Las organizaciones deben priorizar esta actualización debido al impacto significativo que puede tener un exploit exitoso.

Prioridad: Urgente.

Ampliar Información:

https://www.fortiguard.com/psirt/FG-IR-24-535

Hackers rusos explotan CVE-2025-26633 a través de MSC EvilTwin

Un grupo de hackers rusos conocido como Water Gamayun (también llamado EncryptHub y LARVA-208) está explotando la vulnerabilidad CVE-2025-26633, apodada MSC EvilTwin, que afecta al marco de la Consola de Administración de Microsoft (MMC). Esta vulnerabilidad permite ejecutar archivos maliciosos .msc que terminan desplegando dos backdoors avanzados: SilentPrism y DarkWisp. Estos implantes, entregados mediante paquetes de aprovisionamiento y archivos MSI firmados, pueden mantener persistencia, ejecutar comandos de forma remota y exfiltrar información sensible. El malware se comunica con el servidor de C&C a través de conexiones TCP codificadas en Base64, lo que permite una interacción continua con los sistemas comprometidos.

El grupo utiliza múltiples técnicas de evasión y persiste mediante artefactos MSI disfrazados como software legítimo (DingTalk, QQTalk, VooV Meeting) para ejecutar PowerShell y descargar la siguiente fase del ataque. Además, se han identificado variantes personalizadas del EncryptHub Stealer que recopilan credenciales, contraseñas de Wi-Fi y claves de productos Windows, enfocándose también en frases de recuperación de criptomonedas. Water Gamayun demuestra alta sofisticación al emplear técnicas Living-off-the-Land (LOLBin), destacando su capacidad para comprometer sistemas y ocultar rastros forenses.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/03/russian-hackers-exploit-cve-2025-26633.html

---

Hackers explotan los mu-plugins de WordPress

Hackers están explotando el directorio "mu-plugins" de sitios WordPress para ocultar código malicioso, logrando acceso remoto persistente y redireccionando a los visitantes hacia sitios maliciosos. Los mu-plugins (Must-Use plugins) son ejecutados automáticamente por WordPress desde el directorio wp-content/mu-plugins sin necesidad de activación manual, lo que facilita que estos ataques pasen desapercibidos para los administradores. Los atacantes han desplegado varios scripts maliciosos, incluyendo redirect.php para redireccionar tráfico, index.php que funciona como web shell para ejecutar comandos remotos, y custom-js-loader.php para inyectar spam y reemplazar imágenes con contenido explícito.

El malware también puede disfrazarse como actualizaciones de navegador para engañar a los usuarios e instalar software malicioso. Además, los sitios WordPress comprometidos son utilizados para ejecutar comandos maliciosos de PowerShell en equipos Windows bajo la apariencia de verificaciones CAPTCHA de Google o Cloudflare. Los investigadores de Patchstack han identificado múltiples vulnerabilidades críticas en plugins de WordPress, como ejecuciones remotas de código y cargas arbitrarias de archivos, destacando la necesidad de mantener actualizados plugins, auditar el código regularmente y utilizar firewalls de aplicaciones web para prevenir inyecciones de código.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/03/hackers-exploit-wordpress-mu-plugins-to.html

---

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.

1. 5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

DarkCloud: malware avanzado tipo stealer vendido en Telegram para robar datos en Windows

DarkCloud es un malware avanzado de tipo 'stealer' que ha emergido como una amenaza significativa para sistemas Windows desde su aparición en 2022. Originalmente distribuido en foros clandestinos, ahora se comercializa ampliamente en Telegram, facilitando su acceso a ciberdelincuentes a nivel mundial. Este malware se propaga principalmente a través de campañas de phishing, donde los atacantes disfrazan cargas maliciosas como facturas o multas dirigidas a departamentos de recursos humanos y usuarios desprevenidos. Otras técnicas de distribución incluyen malvertising, ataques de watering hole y la agrupación con otros malware como DbatLoader o ClipBanker.

Una vez ejecutado, DarkCloud inicia un proceso de infección en múltiples etapas. Las víctimas suelen ser engañadas para descargar archivos comprimidos que contienen loaders o scripts escritos en lenguajes como PowerShell o JAR, los cuales ofuscan la

siguiente fase del malware. La carga final se inyecta directamente en la memoria, permitiendo al malware evadir la detección mientras roba información sensible como datos de navegadores, credenciales FTP y detalles de tarjetas de crédito. Además, DarkCloud actúa como keylogger, captura capturas de pantalla y monitorea procesos en ejecución. Una característica notable es su integración con Telegram para operaciones de comando y control, utilizando bots para exfiltrar datos robados y recibir instrucciones, lo que complica su detección debido al uso de canales de comunicación legítimos.

Prioridad: Importante.

https://gbhackers.com/an-advanced-stealer-malware-sold-on-telegram/

Nuevo malware para Android que apunta a 750 apps de banca, finanzas y criptomonedas

TsarBot es un nuevo malware bancario para Android que ha sido diseñado para atacar más de 750 aplicaciones en sectores como banca, fintech, criptomonedas y comercio electrónico. Se propaga a través de sitios de phishing que simulan ser plataformas legítimas. Una vez instalado en el dispositivo, TsarBot despliega pantallas de superposición (overlay) que imitan interfaces reales de apps bancarias para engañar a los usuarios y robar credenciales, información de tarjetas y otros datos sensibles.

Además, este malware cuenta con funciones avanzadas como grabación de pantalla, control remoto del dispositivo y la capacidad de simular acciones del usuario (clics, toques, desplazamientos). Incluso puede mostrar una pantalla negra para ocultar su actividad mientras ejecuta acciones maliciosas en segundo plano. También captura códigos de desbloqueo mediante pantallas falsas de PIN o patrón. Para comunicarse con su servidor de comando y control, utiliza conexiones persistentes a través de WebSocket, lo que le permite recibir instrucciones y exfiltrar datos en tiempo real.

Prioridad: Urgente.

Ampliar Información:

https://gbhackers.com/new-android-malware-tsarbot-targeting-750-banking/

El malware SHELBY explota GitHub como servidor C2

HELBY es una familia de malware recientemente descubierta que ha sido utilizada en la campaña REF8685, dirigida al sector de telecomunicaciones en Irak. Este malware se compone de dos componentes principales: SHELBYLOADER y SHELBYC2. La infección comienza con un correo electrónico de phishing que contiene un archivo adjunto malicioso. Al ejecutarse, este instala varios archivos en el directorio %AppData%\Local\Microsoft\HTTPApi, incluyendo HTTPApi.dll (SHELBYC2) y HTTPService.dll (SHELBYLOADER). SHELBYLOADER emplea técnicas avanzadas de detección de entornos de análisis para evadir la detección y establece persistencia mediante la modificación del registro de Windows.

Una característica distintiva de SHELBY es su uso innovador de la API de GitHub como infraestructura de comando y control (C2). Utiliza un repositorio privado y un Token de Acceso Personal (PAT) incrustado en el binario para autenticar y realizar acciones en el repositorio sin emplear herramientas Git estándar. SHELBYC2, el componente de puerta trasera se carga en memoria utilizando técnicas de reflexión después de ser descifrado con una clave AES derivada de un archivo descargado del servidor C2. Este componente admite varios comandos, incluyendo la descarga y carga de archivos, así como la capacidad de cargar de manera reflexiva binarios .NET adicionales. Sin embargo, este diseño presenta una vulnerabilidad crítica: cualquier persona con acceso al PAT podría potencialmente controlar las máquinas infectadas o acceder a datos sensibles, exponiendo a las víctimas a riesgos adicionales.

Prioridad: Urgente.

Ampliar Información:

https://gbhackers.com/shelby-malware-steals-data-by-abusing-github/

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

Microsoft refuerza el uso obligatorio de cuentas en línea en Windows 11

Microsoft ha bloqueado el uso del conocido script bypassnro.cmd en la versión más reciente de Windows 11, lo que impide a los usuarios saltarse la obligatoriedad de configurar una cuenta Microsoft durante la instalación inicial del sistema. Esta decisión forma parte de los esfuerzos de la compañía por reforzar la seguridad y centralizar la experiencia del usuario en servicios conectados a la nube.

Sin embargo, aún existen métodos alternativos para crear una cuenta local. Uno de los más efectivos consiste en presionar Shift + F10 para abrir la consola durante la instalación y ejecutar el comando start ms-cxh:localonly, lo que permite continuar sin conexión y crear una cuenta local. Aunque este tipo de soluciones siguen funcionando por ahora, es probable que Microsoft las cierre en futuras actualizaciones del sistema operativo.

Prioridad: Importante.

Ampliar Información:

https://www.zdnet.com/article/microsoft-just-blocked-this-popular-windows-11-local-account-trick-but-workarounds-remain/

Cuatro vulnerabilidades de WordPress bajo ataque activo en los primeros meses de 2025

Durante el primer trimestre de 2025, los ciberatacantes se enfocaron principalmente en explotar cuatro vulnerabilidades críticas en plugins y temas de WordPress, todos ellos con parches disponibles desde 2024. A pesar de que las fallas fueron corregidas, miles de sitios web continúan operando con versiones desactualizadas, lo que los deja expuestos a ataques que incluyen inyecciones SQL, cargas de archivos maliciosos y ejecución remota de código.

Entre las vulnerabilidades más explotadas se encuentran una falla crítica de inyección SQL en el plugin WordPress Automatic Plugin, un fallo en Startklar Elementor Addons que permite la carga de archivos sin restricciones, una ejecución remota de código en el tema Bricks, y otra vulnerabilidad en Example Plugin que permite la exfiltración de datos sensibles sin necesidad de autenticación. Estas debilidades reflejan la importancia de mantener actualizados los componentes de WordPress, ya que los atacantes continúan escaneando activamente la web en busca de instalaciones vulnerables. Mantener buenas

prácticas de seguridad y aplicar parches de forma regular sigue siendo esencial para mitigar estos riesgos.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/the-four-wordpress-flaws-hackers-targeted-the-most-in-q1-2025/
