GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición °2726

## 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 |
|---|---|---|---|
| **VULNERABILIDADES** | 1 | 2 | 0 |
| **MALWARE** | 0 | 1 | 0 |
| **NOTICIAS DE CIBERSEGURIDAD** | 0 | 1 | 0 |

## VULNERABILIDADES

### CVE-2026-46242 – BAD EPOLL (EJECUCIÓN DE CÓDIGO LOCAL Y ESCALACIÓN DE PRIVILEGIOS A ROOT)

Se ha divulgado una vulnerabilidad crítica de escalación local de privilegios (LPE) denominada "Bad Epoll", la cual reside en el subsistema de notificación de eventos de E/S del kernel de Linux (epoll). El fallo permite a un usuario local ordinario, sin ningún tipo de privilegios especiales en el sistema, corromper la memoria interna y obtener acceso total como el usuario root.

Esta vulnerabilidad representa un riesgo operativo severo debido a la ubicuidad del componente afectado, el cual es utilizado de forma nativa por servidores de alto rendimiento, servicios de red y navegadores web para la gestión simultánea de descriptores de archivos. A diferencia de otros fallos recientes del kernel, "Bad Epoll" destaca por su capacidad de romper el aislamiento y afectar directamente a entornos de escritorio, servidores e infraestructuras basadas en el sistema operativo Android.

**Resumen técnico:**

- Identificador principal: CVE-2026-46242.
- Severidad: Alta / Crítica (Puntaje base de 7.8 en CVSS v3.1).
- Causa raíz: Una vulnerabilidad de uso de memoria después de ser liberada (Use-After-Free - UAF) gatillada por una condición de carrera (Race Condition) en la ruta de liberación de archivos (file-release path) del mecanismo epoll.
- Mecanismo de falla: El fallo se produce cuando dos rutas de cierre coordinadas (close paths) de la infraestructura eventpoll se ejecutan simultáneamente y colisionan: un hilo libera la estructura de memoria de un objeto mientras el otro continúa realizando operaciones de escritura sobre ella. El exploit desarrollado amplía artificialmente esta ventana temporal (la cual dura originalmente solo seis instrucciones de máquina) y ejecuta un bucle repetitivo que logra una tasa de éxito del 99% sin provocar pánicos en el kernel. Posteriormente, convierte la escritura UAF inicial de 8 bytes en un compromiso sobre un objeto de archivo mediante un ataque de caché cruzada (cross-cache attack), logrando capacidades de lectura arbitraria del kernel a través de /proc/self/fdinfo, el secuestro del puntero de instrucciones de la CPU y la ejecución de una cadena ROP para invocar un shell como root.
- Estado de explotación: No se han reportado campañas de explotación activa en el entorno real (actualmente ausente en el catálogo KEV de CISA). No obstante, el código de prueba de concepto (PoC) funcional fue validado y publicado a través del programa kernelCTF de Google, y variantes orientadas a la explotación en dispositivos móviles se encuentran en fases avanzadas de desarrollo.
- Versiones afectadas: Distribuciones de Linux y dispositivos móviles que implementen ramas del Kernel de Linux basadas en la versión 6.4 o superior (origen del cambio de código introducido en 2023). Se confirma la vulnerabilidad en plataformas empresariales como AlmaLinux 9 y 10, así como en terminales móviles como la serie Pixel 10 (Kernel 6.6). Las ramas LTS basadas en el Kernel 6.1 o inferiores se evalúan como no vulnerables.

**Impacto potencial:**

- Escalación de privilegios locales (LPE) a nivel de Root: Concede de forma inmediata a actores de amenazas internos u operadores de malware de bajo nivel el control total del sistema operativo subyacente, permitiéndoles anular cualquier política de restricción local, alterar configuraciones del sistema e implantar persistencia a nivel de kernel.
- Evasión de entornos aislados de aplicaciones (Sandbox Escape): Los análisis de laboratorio demuestran que la falla puede ser invocada de manera exitosa desde procesos fuertemente restringidos, como el renderizador aislado de Google Chrome, sirviendo como el eslabón definitivo (Chain Exploit) para escapar de las restricciones del navegador tras un compromiso web inicial.
- Compromiso total de la integridad en dispositivos Android: Al romper las barreras defensivas tradicionales del kernel que suelen mitigar exploits en entornos móviles, "Bad Epoll" califica dentro del selecto grupo de fallas capaces de realizar procesos de rooting no autorizados, exponiendo datos de aplicaciones financieras, tokens de autenticación y particiones críticas del dispositivo.
- Ruptura de aislamiento en arquitecturas multi-inquilino y contenedores: En entornos de infraestructura compartida donde los usuarios interactúan directamente con el kernel del host a través de espacios de nombres o contenedores permisivos, un atacante local puede abastardear el fallo para comprometer la estabilidad del nodo o recolectar información técnica residual de otros inquilinos.

**Recomendaciones de mitigación:**

1. Aplicación prioritaria del parche de seguridad del fabricante: Se urge a los administradores de infraestructura y equipos de ingeniería de plataformas a aplicar el commit de blindaje upstream a6dc643c6931 en sus árboles de compilación del kernel de Linux, o en su defecto, forzar la actualización inmediata de los paquetes del sistema a las versiones oficiales provistas por su distribución (ej. Debian 13 bajo la actualización 6.12.95-1).
2. Validación técnica previa en entornos empresariales afectados: Para sistemas basados en clones de Red Hat Enterprise Linux como AlmaLinux (versiones 9 y 10), se recomienda habilitar temporalmente el repositorio de pruebas (almalinux-release-testing) para descargar e inspeccionar los kernels corregidos (kernel-5.14.0-687.20.3 y kernel-6.12.0-211.30.3 respectivamente) antes de su promoción definitiva a producción.
3. Inviabilidad absoluta de desactivación del componente: Se advierte explícitamente a los equipos de TI no intentar inhabilitar o bloquear el subsistema epoll como medida provisional. Al ser un pilar básico en la arquitectura de comunicaciones de Linux, cualquier intento de restricción perimetral sobre este mecanismo resultará en la inoperabilidad inmediata de los servicios de red, navegadores y demonios críticos del sistema.
4. Despliegue de reglas de detección de comportamiento anómalo (EDR/SIEM): Implementar firmas de monitoreo heurístico sobre las soluciones de seguridad de endpoint para identificar ejecuciones cíclicas inusuales que consulten de forma repetitiva descriptores de archivos a través de /proc/self/fdinfo, un patrón característico utilizado por el exploit para evadir los controles de KASAN y estabilizar la condición de carrera.

**Prioridad: Urgente.**

**Ampliar información:**

- https://www.securityweek.com/proof-of-concept-exploit-released-for-linux-bad-epoll-root-access-vulnerability/
- https://thehackernews.com/2026/07/new-bad-epoll-linux-kernel-flaw-lets.html
- https://securityaffairs.com/194795/hacking/bad-epoll-flaw-gives-attackers-root-access-on-linux-and-android.html
- https://www.it-connect.tech/bad-epoll-the-linux-kernel-flaw-that-can-root-android-and-mythos-missed-it/
- https://almalinux.org/blog/2026-07-06-januscape-bad-epoll/

## CVE-2026-43499 – GHOSTLOCK (ESCALACIÓN DE PRIVILEGIOS LOCALES Y ESCAPE DE CONTENEDORES EN ENTORNOS LINUX)

Se ha revelado una vulnerabilidad histórica de escalación de privilegios y ruptura de aislamiento de seguridad en el kernel de Linux denominada "GhostLock". El fallo, que permaneció latente y sin detectar por aproximadamente 15 años (desde 2011), reside en el mecanismo de sincronización interna del sistema operativo y permite a un usuario local autenticado sin privilegios previos obtener control absoluto como el usuario root.

La criticidad de esta amenaza se amplifica exponencialmente debido a que es capaz de propiciar el escape completo desde entornos contenerizados (como Docker y Kubernetes) hacia el sistema operativo del host. Dado que el subsistema afectado se distribuye por defecto en la totalidad del ecosistema Linux corporativo, el fallo compromete de forma transversal a servidores de centros de datos, instancias cloud multi-inquilino, corredores de integración continua (CI Runners) e infraestructura crítica que ejecute arquitecturas compartidas.

**Resumen técnico:**

- Identificador principal: CVE-2026-43499 (Fallo asociado en la primera revisión: CVE-2026-53166).
- Severidad: Alta (Puntaje base de 7.8 en CVSS v3.1; Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Un defecto de liberación de memoria después de su uso (Use-After-Free - UAF) catalogado como CWE-416, ubicado específicamente en la función remove_waiter() del código de exclusión mutua en tiempo real (rt_mutex) y gestionado a través del subsistema futex.
- Mecanismo de falla: El error ocurre durante el rollback de un bloqueo proxy (proxy lock) ejecutado por la función futex_requeue(). Bajo un escenario de colisión por condición de carrera, el paso de limpieza del kernel se ejecuta a destiempo, provocando que se elimine el registro de una tarea equivocada y dejando un puntero colgante (stale pointer) hacia una sección de memoria que ya fue liberada y reutilizada para otros fines por el sistema. El exploit desarrollado por la firma Nebula Security manipula de forma controlada llamadas rutinarias de hilos (threading) para tomar control de dicho puntero correlacionado, logrando inyectar y ejecutar código en el espacio de memoria del kernel para otorgar un shell de root con una fiabilidad del 97% en un lapso aproximado de 5 segundos.
- Estado de explotación: No se registra evidencia de explotación activa en el entorno real por parte de actores de amenazas al momento del reporte. Sin embargo, los investigadores publicaron el código de explotación funcional (PoC) tras recibir una recompensa a través del programa kernelCTF de Google, incrementando de forma drástica la probabilidad de su pronta adopción y weaponización en campañas cibercriminales.
- Versiones afectadas: El fallo afecta de manera generalizada a prácticamente todas las distribuciones de Linux (incluyendo Ubuntu, Debian, Red Hat Enterprise Linux y CentOS) desde la versión de kernel 2.6.39 hasta la versión 7.1.

**Impacto potencial:**

- Compromiso total del sistema operativo central (LPE): Permite a atacantes internos, usuarios legítimos de baja confianza o procesos comprometidos anular de inmediato la matriz de permisos local y asumir la identidad del usuario root, comprometiendo de forma irreversible la confidencialidad, integridad y disponibilidad del host.
- Ruptura de aislamiento de cargas (Container Escape): Habilita a un contenedor Docker o un pod de Kubernetes previamente comprometido a romper el aislamiento lógico provisto por los espacios de nombres (namespaces) y cgroups, obteniendo acceso directo al kernel del nodo anfitrión y poniendo en riesgo la infraestructura cloud subyacente.
- Encadenamiento para ejecución remota de código (Chain Exploitation / IonStack): Al formar parte de la cadena de explotación denominada "IonStack", el fallo puede ser enlazado de forma remota con exploits de navegador (como el fallo de Firefox CVE-2026-10702), permitiendo que una simple navegación hacia un enlace malicioso desencadene una escalación automática hasta root, incluso en terminales móviles basados en Android.
- Vulnerabilidad extendida en plataformas legadas y sistemas embebidos: Debido a la antigüedad del código afectado (15 años), la falla expone masivamente a appliances de red, dispositivos IoT corporativos y servidores empresariales antiguos que carecen de canales automatizados o ágiles de actualización de firmware y software.

**Recomendaciones de mitigación:**

1. Actualización del kernel y validación técnica del fix definitivo: Priorizar la instalación inmediata de los parches oficiales distribuidos por el fabricante del sistema operativo (actualizando al kernel 7.2.0 o superior, o aplicando los backports de seguridad específicos como Ubuntu 22.04.3+ y RHEL 9.4+). Es crítico verificar que la compilación aplicada incluya el parche final (commit 3bfdc63936dd) y no la versión inicial intermedia, ya que esta última introducía un fallo secundario de denegación de servicio (CVE-2026-53166).
2. Endurecimiento de perfiles de contenedor mediante Seccomp: En entornos de orquestación donde la actualización inmediata del kernel del host no sea viable debido a ventanas de mantenimiento estrictas, se deben modificar o asegurar las políticas de seccomp en Kubernetes y Docker para restringir y bloquear las llamadas de sistema de futex y operaciones concurrentes de sincronización que gatillan la condición de carrera.
3. Implementación de mitigaciones de compilación de bajo nivel: Asegurar que los sistemas en producción cuenten con características operativas de mitigación activas tales como RANDOMIZE_KSTACK_OFFSET (aleatorización del desplazamiento de la pila del kernel) y STATIC_USERMODE_HELPER, las cuales dificultan la predictibilidad de la memoria y degradan la efectividad del exploit público.
4. Restricción de interfaces locales y monitoreo forense de logs: Limitar estrictamente el acceso interactivo por shell en servidores multiusuario o nodos de desarrollo a personal estrictamente verificado. De manera complementaria, configurar las herramientas de monitoreo (SIEM/EDR) para auditar de forma heurística los registros del kernel en busca de pánicos, anomalías de estabilidad o llamadas inusuales en las funciones de rt_mutex.

**Prioridad: Urgente.**

**Ampliar información:**

- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-ghostlock-en-el-kernel-de-linux-cve-2026-43499/
- https://secarma.com/08-07-2026-ghostlock-linux-kernel-vulnerability
- https://thehackernews.com/2026/07/15-year-old-ghostlock-flaw-enables-root.html
- https://threat-modeling.com/cve-2026-43499-ghostlock-linux-kernel-root-container-escape/
- https://unaaldia.hispasec.com/un-fallo-de-15-anos-en-el-kernel-de-linux-permite-hacerse-root-y-escapar-de-contenedores/

## CVE-2026-40138 / CVE-2026-40139 – BEYONDTRUST REMOTE SUPPORT & PRA (ELUSIÓN DE CONTROLES DE AUTENTICACIÓN PRE-AUTENTICACIÓN)

BeyondTrust ha emitido una alerta de seguridad (advisory BT26-03) detallando múltiples vulnerabilidades críticas en sus plataformas de gestión de acceso privilegiado Remote Support (RS) y Privileged Remote Access (PRA). Los fallos más severos permiten a un actor de amenazas remoto y no autenticado eludir por completo las barreras de control de acceso y obtener facultades administrativas sobre la appliance comprometida sin necesidad de poseer credenciales válidas.

Debido a que estas herramientas actúan de manera centralizada como pasarelas (gateways) de administración y control de activos críticos (servidores, endpoints e infraestructura de red), el compromiso de la plataforma representa uno de los peores escenarios de riesgo operativo para una organización. Históricamente, las soluciones de acceso remoto de este fabricante han sido objetivos de alto valor para operadores de ransomware y grupos APT estatales debido a los canales de confianza que manejan de forma perimetral.

**Resumen técnico:**

- Identificador principal: CVE-2026-40138 y CVE-2026-40139 (Adicionalmente vinculados en el boletín: CVE-2026-40140 y CVE-2026-40141).
- Severidad: Crítica (Puntaje base de 9.2 bajo el estándar CVSS v4 / v3.1).
- Causa raíz: Defectos lógicos de validación y procesamiento de solicitudes en el subsistema de autenticación pre-autenticación, catalogados formalmente bajo la debilidad CWE-287 (Autenticación Impropia).
- Mecanismo de falla: El fallo se subdivide en dos vectores: CVE-2026-40138 (afecta a RS y PRA) surge de la validación deficiente de los datos de autenticación de red por parte de un atacante posicionado, requiriendo una configuración específica de autenticación activa; CVE-2026-40139 (específico de RS) es más directo, ya que un atacante remoto aprovecha el procesamiento inadecuado de las solicitudes de ingreso para forzar un bypass total de la interfaz web de login. Al combinarse con las fallas adyacentes de denegación de servicio (CVE-2026-40140) y de validación de entradas de usuarios limitados (CVE-2026-40141), un atacante puede desestabilizar la disponibilidad o escalar verticalmente su alcance operativo dentro de la solución de acceso unificado. Cabe destacar que el descubrimiento interno de estas fallas contó con el apoyo de modelos avanzados de inteligencia artificial (Claude Opus 4.8) combinados con herramientas propietarias de BeyondTrust.
- Estado de explotación: No se ha confirmado explotación activa en el entorno real al momento de su divulgación pública. No obstante, dado el historial de ataques dirigidos contra estas tecnologías, se anticipa la creación y estabilización de exploits públicos de forma inminente tan pronto se distribuyan los detalles de ingeniería inversa de los parches.
- Versiones afectadas: Todas las implementaciones locales (self-hosted) de BeyondTrust Remote Support y Privileged Remote Access en versiones 25.3.2 y anteriores. Las instancias basadas en la nube (SaaS) administradas por el fabricante fueron mitigadas de manera automatizada a partir del 21 de abril de 2026.

**Impacto potencial:**

- Secuestro completo de la identidad corporativa privilegiada: Permite el aprovisionamiento ilícito de accesos con privilegios máximos del sistema, lo que otorga al atacante control total sobre las políticas de soporte remoto y la capacidad de pivotar libremente hacia cualquier servidor o endpoint interno enlazado.
- Despliegue masivo de persistencia (Web Shells y Backdoors): Tomando como referencia incidentes históricos previos en la plataforma (como CVE-2024-12356), los atacantes suelen capitalizar el acceso administrativo de estas interfaces para implantar código malicioso persistente, facilitando la exfiltración silenciosa de datos a largo plazo.
- Efecto dominó en cadenas de suministro tecnológicas (Third-Party Risk): Al ser herramientas frecuentemente delegadas a proveedores externos de TI, un compromiso en el portal de soporte expone de manera directa las redes de múltiples organizaciones aliadas, subvirtiendo los perímetros defensivos tradicionales a través de canales de confianza preestablecidos.
- Pérdida total del control de auditoría de accesos: El compromiso de la infraestructura PAM (Privileged Access Management) faculta al atacante para manipular, borrar o alterar los registros de auditoría y logs de sesión internos de la appliance, imposibilitando las tareas de atribución e investigación forense ante un incidente.

**Recomendaciones de mitigación:**

1. Actualización inmediata a versiones seguras (Self-Hosted): Se urge a las organizaciones que operen despliegues autogestionados a aplicar de forma prioritaria el Rollup de seguridad de abril de 2026 o actualizar directamente a las versiones BeyondTrust RS 25.3.3 y PRA 25.3.3 (o superiores), confirmando manualmente la compilación instalada frente al advisory oficial.
2. Restricción perimetral estricta de las interfaces de Login: Implementar políticas de control de acceso a nivel de red (ACLs/Firewall) para asegurar que los portales web de Remote Support y PRA no estén expuestos directamente a la totalidad de Internet; el acceso debe restringirse exclusivamente a rangos de direcciones IP públicas conocidas o segmentos VPN corporativos protegidos.
3. Auditoría y rotación preventiva de credenciales gestionadas: Tras la ejecución del proceso de parcheo, se recomienda realizar una rotación masiva de todas las credenciales administrativas locales y aquellas almacenadas o gestionadas dentro de las bóvedas de las soluciones afectadas, mitigando el riesgo de compromisos latentes previos.
4. Monitoreo forense de configuraciones y sesiones activas: Monitorear de forma exhaustiva los logs de autenticación de las appliances en busca de patrones de inicio de sesión inesperados, creación anómala de cuentas con privilegios elevados o modificaciones no autorizadas en las configuraciones de autenticación externas (como LDAP o SAML).

**Prioridad: Crítica.**

**Ampliar información:**

- https://thehackernews.com/2026/07/beyondtrust-patches-critical-auth.html
- https://threat-modeling.com/cve-2026-40138-cve-2026-40139-beyondtrust-remote-support-pra-auth-bypass/
- https://www.cycognito.com/blog/emerging-threat-cve-2026-40138-cve-2026-40139-beyondtrust-remote-support-authentication-bypass/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidades-criticas-en-beyondtrust-remote-support-y-privileged-remote-access-con-cvss-9-2/
- https://fieldeffect.com/blog/beyondtrust-patches-critical-authentication-bypass-vulnerabilities

## MALWARE

### MALWARE: UMBRIJ – SECUESTRO DE SESIONES DE GMAIL Y ABUSO DE TOKENS OAUTH (TODDYCAT APT)

Se ha identificado una campaña de ciberespionaje avanzada vinculada al grupo de amenazas persistentes (APT) ToddyCat, en la cual se despliega una nueva pieza de malware de post-explotación denominada "Umbrij". Este sofisticado software malicioso ha sido desarrollado con el objetivo específico de obtener acceso encubierto y persistente a las comunicaciones de correo electrónico corporativas alojadas en Gmail, abusando de la API oficial de Google y del protocolo de autorización OAuth 2.0.

A diferencia de los ladrones de credenciales tradicionales, Umbrij no recolecta contraseñas de manera directa, sino que manipula de forma automatizada las sesiones web legítimas que el usuario ya mantiene abiertas en su navegador. Al suplantar la identidad de herramientas oficiales de migración e interactuar de manera silenciosa con los servicios en la nube, el malware logra integrarse de forma invisible dentro del tráfico legítimo de la organización, comprometiendo drásticamente la confidencialidad de la información empresarial.

**Resumen técnico:**

- Identificador principal: Malware Umbrij (Atribuido al grupo APT ToddyCat).
- Tipo de amenaza: Malware de post-explotación / Herramienta de ciberespionaje orientada a APIs en la nube.
- Causa raíz / Técnica clave: Implementación de la técnica "Shadow Token via Remote Debug" (STRD), la cual combina la automatización de navegadores con el secuestro de sesiones locales autenticadas para la extracción fraudulenta de tokens de acceso OAuth corporativos.
- **Mecanismo de falla y operación:** Tras comprometer un equipo Windows, el malware suplanta los privilegios del usuario mediante el token de **explorer.exe**. Luego extrae datos de perfiles autenticados de **Google Chrome** o **Microsoft Edge** (cookies, *IndexedDB*, *Local Storage* y credenciales) y los copia a un directorio temporal. Con **Puppeteer**, inicia un navegador en modo *headless*, reutiliza las cookies para omitir el inicio de sesión y, mediante el puerto de depuración remota, suplanta el **client_id** de *Google Workspace Migration for Microsoft Outlook*. Finalmente, automatiza la aprobación de permisos, obtiene el código de autorización **OAuth** y lo exfiltra para conseguir un token de acceso válido a la API de Google.
- Vector de infección y evasión: El malware se introduce en el sistema mediante una tarea programada maliciosa que suplanta soluciones de seguridad locales (nombrada fraudulentamente como KasperskyEndpointSecurityEDRAvp). Dicha tarea invoca un binario legítimo y firmado digitalmente que es vulnerable a la carga lateral de DLL (DLL side-loading), tales como BDSubWiz.exe (Bitdefender), VSTestVideoRecorder.exe (Microsoft Visual Studio) o GoogleDesktop.exe. El ejecutable carga en memoria la DLL maliciosa de Umbrij, la cual está desarrollada sobre el framework .NET y se encuentra fuertemente protegida mediante el ofuscador de código abierto ConfuserEx.
- Versiones y entornos afectados: Estaciones de trabajo y servidores Windows que utilicen navegadores web basados en Chromium (Google Chrome y Microsoft Edge) con sesiones de cuentas corporativas de Google Workspace activas.

**Impacto potencial:**

- Acceso encubierto y persistente a comunicaciones de correo: Permite a los operadores del grupo APT ToddyCat interceptar, monitorizar y exfiltrar de manera silenciosa la correspondencia completa de Gmail de la organización, comprometiendo secretos comerciales, estrategias de negocio y datos de clientes sin levantar alertas de inicio de sesión inusuales.
- Compromiso extendido de la infraestructura en la nube (Google Workspace): Debido a que la aplicación suplantada solicita permisos amplios, el token OAuth generado concede acceso no solo a Gmail, sino también a recursos críticos almacenados en Google Drive, listas de Contactos, Calendarios empresariales y Google Tasks, expandiendo horizontalmente el alcance del espionaje.
- Evasión total de mecanismos tradicionales de autenticación y MFA: Al reutilizar las cookies de sesión vivas y clonar localmente el estado del navegador, el malware evade por completo los controles de contraseñas y las políticas de Autenticación Multifactor (MFA), ya que aprovecha un estado de confianza previamente validado y establecido por el usuario legítimo.
- Automatización del ciberespionaje a escala corporativa: El uso de herramientas de automatización como Puppeteer y la capacidad de Umbrij para mapear y procesar múltiples perfiles de usuario en el endpoint permiten a la amenaza ejecutar ataques de manera masiva, repetitiva y altamente escalable en redes empresariales complejas.

**Recomendaciones de mitigación:**

1. Auditoría periódica y revocación de permisos OAuth conectados: Los administradores de TI y equipos de seguridad deben inspeccionar de forma continua las conexiones de aplicaciones externas en los entornos de Google Workspace (mediante la consola de administración o de forma individual en myaccount.google.com/connections). Es prioritario buscar y revocar de inmediato el acceso de aplicaciones como "Google Workspace Migration for Microsoft Outlook" o "Google Workspace Sync for Microsoft Outlook" si estas no corresponden a una actividad de migración activa y legítimamente validada por la organización.
2. Restricción y control del puerto de depuración remota en navegadores: Implementar políticas de grupo (GPO) o configuraciones de administración de endpoints para bloquear o restringir estrictamente la inicialización de navegadores Chromium con flags que habiliten el puerto de depuración remota (remote debugging port), limitando su uso únicamente a entornos de desarrollo aislados y autorizados.
3. Despliegue de reglas de detección de comportamiento anómalo en Endpoint (EDR): Configurar y entrenar a las soluciones EDR corporativas para monitorizar y alertar sobre la ejecución sospechosa de procesos de Google Chrome o Microsoft Edge en modo desatendido (--headless), especialmente cuando estos sean invocados por procesos secundarios inusuales o frameworks de automatización web (como Puppeteer) en contextos de usuario final.
4. Monitoreo y mitigación de técnicas de DLL Side-Loading: Monitorear la creación de tareas programadas sospechosas que intenten suplantar software de seguridad conocido y restringir la ejecución de binarios legítimos fuera de sus rutas de instalación estándar, prestando especial atención a actividades inusuales de lectura y clonación de datos dentro de los directorios %LOCALAPPDATA%\Google\Chrome\ y %LOCALAPPDATA%\Microsoft\Edge\.

**Prioridad: Urgente.**

**Ampliar información:**

- https://blog.actipace.com/news/2026/07/toddycat-deploys-umbrij-malware-to-hijack-gmail-accounts-via-google-oauth-api/
- https://underc0de.org/foro/noticias-informaticas-120/umbrij-el-nuevo-malware-de-toddycat-roba-cuentas-de-gmail-mediante-oauth/
- https://blog.segu-info.com.ar/2026/07/el-malware-umbrij-abusa-de-oauth-para.html
- https://thehackernews.com/2026/07/toddycat-linked-umbrij-malware-abuses.html
- https://www.ingenieriatelematica.com.co/malware-umbrij-de-toddycat-abusa-de-oauth-para-acceder-a-gmail-via-google-api/

**Recomendaciones generales sobre malware:**

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

### CAMPAÑA FORTIBLEED VINCULADA DE FORMA DIRECTA A OPERACIONES DE RANSOMWARE INC Y LYNX

Se ha confirmado el nexo operativo directo entre la masiva campaña global de recolección de credenciales denominada "FortiBleed" y dos de las franquicias de Ransomware-as-a-Service (RaaS) más activas del panorama delictivo: INC Ransom y Lynx. El hallazgo, documentado por la Unidad de Investigación de Amenazas de SOCRadar (STRU), fue posible debido a una grave falla en la seguridad operativa (OpSec) de los atacantes, lo que expuso un servidor de coordinación interno en el que se constató que un mismo operador gestionaba simultáneamente los paneles de negociación de rescates de ambas bandas de ransomware.

Esta investigación eleva de manera crítica el nivel de riesgo para las organizaciones que ejecutan perímetros basados en Fortinet, demostrando que FortiBleed no funciona como un intermediario de acceso independiente (Initial Access Broker - IAB) que comercializa credenciales a largo plazo, sino que actúa como el componente directo de intrusión y suministro para despliegues inmediatos de ransomware altamente destructivos.

**Resumen técnico:**

- Identificador principal: Campaña FortiBleed / Herramienta maliciosa FortigateSniffer.
- Severidad: Crítica (Riesgo inminente de compromiso de dominio y despliegue de ransomware).
- Causa raíz: Interceptación pasiva y automatizada de tráfico de autenticación en dispositivos de seguridad perimetral expuestos a Internet.
- **Mecanismo de operación:** La campaña utiliza una herramienta en **Go** (*FortigateSniffer*) que abusa de los comandos de diagnóstico de **FortiOS** mediante más de dos docenas de protocolos. Su principal técnica de evasión consiste en escuchar pasivamente el tráfico de autenticación del dispositivo, sin inyectar código malicioso, para capturar contraseñas en texto plano y *hashes*. La infraestructura del grupo (aprox. 20 integrantes), liderado por el actor **"Toxman"**, emplea herramientas de IA como **CyberStrike** y **OpenRouter** para automatizar ataques y perfilar objetivos. Además, establece persistencia mediante la creación de una cuenta oculta llamada **adminin**.
- Estado de explotación: Campaña global masiva activa desde febrero de 2026. Se estima que ha apuntado a más de 430,000 dispositivos FortiGate en 150 países, recolectando más de 110 millones de credenciales. El sniffer estuvo activo en aproximadamente 19,000 entornos corporativos (reducido a unos 12,000 tras alertas). Se ha verificado el compromiso de nivel administrativo en 409 objetivos, logrando completar la cadena completa de intrusión (VPN -> Controlador de Dominio -> Domain Admin) en 354 de ellos, derivando directamente en al menos 12 despliegues confirmados de ransomware.
- **Plataformas afectadas:** Dispositivos perimetrales **Fortinet FortiGate (FortiOS)**. Los análisis forenses identificaron reconocimiento avanzado contra entornos **Citrix** (29.000 IPs y 37 dominios) y la explotación activa de una vulnerabilidad **Zero-Day** en **Nextcloud**, utilizada para facilitar el movimiento lateral tras el compromiso.

**Impacto potencial:**

- Compromiso total del Directorio Activo (Domain Admin): Al comprometer las credenciales de la VPN con privilegios administrativos, los atacantes logran pivotar hacia la red interna y comprometer los controladores de dominio principales, asumiendo facultades de Administrador de Dominio en el 86% de sus intrusiones exitosas.
- Cifrado destructivo masivo de la infraestructura: El control de la red es transferido de inmediato a las células operativas de INC Ransom o Lynx, culminando en la ejecución de ransomware a gran escala y el cifrado de cientos de endpoints y servidores empresariales en un lapso mínimo de tiempo.
- Exfiltración de datos bajo esquemas de doble extorsión: La infraestructura compartida y los directorios abiertos vinculados a INC Ransom demuestran que los datos críticos extraídos de las redes son utilizados en campañas coordinadas de extorsión pública a través de sus sitios de fuga de información (leak sites), impactando la reputación institucional y la conformidad regulatoria.
- Expansión horizontal de la superficie de ataque corporativa: El descubrimiento de listas de objetivos orientadas a Citrix y el uso de un Zero-Day en entornos Nextcloud confirman que el grupo criminal tiene la capacidad técnica de reutilizar sus flujos automatizados para vulnerar otras plataformas de acceso remoto y colaboración de la empresa.

**Recomendaciones para mitigar el riesgo:**

1. Auditoría forense inmediata de cuentas y comandos en FortiOS: Inspeccionar detalladamente la base de datos de usuarios locales y administradores del sistema en los dispositivos FortiGate para detectar y remover la presencia de cuentas anómalas (específicamente el usuario adminin). Revisar los logs de comandos internos para identificar ejecuciones no autorizadas de herramientas nativas de diagnóstico de paquetes o sniffing.
2. Rotación global de credenciales y robustecimiento de accesos VPN: Forzar un cambio masivo de contraseñas para todas las cuentas de administración local y usuarios de la VPN SSL/IPsec. Es mandatorio implementar o robustecer las políticas de Autenticación Multifactor (MFA) obligatoria, asegurando que utilicen esquemas resistentes al phishing o bypass de sesión.
3. Aislamiento y blindaje de plataformas de colaboración Nextcloud: Ante la evidencia de la explotación activa de un fallo de día cero (Zero-Day) en Nextcloud por parte de este grupo para su movimiento lateral, se recomienda auditar exhaustivamente los logs de acceso de estas instancias, restringir su exposición directa a Internet mediante proxies inversos y coordinar estrechamente con el proveedor para la aplicación de parches de emergencia.
4. Revisión preventiva de bitácoras en infraestructura Citrix: Dado que los atacantes poseen registros avanzados de reconocimiento sobre 29,000 activos Citrix, las organizaciones que implementen esta tecnología deben tratar la alerta como un vector de advertencia temprana, procediendo a auditar los logs de autenticación, validar la integridad de las sesiones de NetScaler y monitorizar cualquier comportamiento de login geográficamente anómalo.

**Prioridad: Urgente.**

**Ampliar Información:**

- https://securityaffairs.com/194645/security/430000-fortigate-devices-exposed-in-fortibleed-ransomware-link.html
- https://www.news4hackers.com/fortibleed-vulnerability-linked-to-inc-threat-group-and-lynx-ransomware-attacks/
- https://thehackernews.com/2026/07/fortibleed-credential-theft-linked-to.html
- https://www.darkreading.com/threat-intelligence/fortibleed-actors-inc-lynx-ransomware-gangs
- https://www.yahoo.com/news/science/articles/fortibleed-campaign-traced-inc-lynx-110516176.html
- https://www.cybersecuritydive.com/news/fortibleed-campaign-traced-to-inc-and-lynx-ransomware-operations/824348/
- https://www.techzine.eu/news/security/142639/fortibleed-linked-to-ransomware-groups-inc-and-lynx/