GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2226

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	0	1

VULNERABILIDADES

CVE-2026-46243 – CIFSWITCH (ESCALAMIENTO LOCAL DE PRIVILEGIOS EN EL KERNEL DE LINUX - LPE)

Se ha divulgado una vulnerabilidad crítica de escalamiento de privilegios locales en el Kernel de Linux denominada "CIFSwitch", la cual ha estado presente de manera latente en el código fuente durante 19 años (desde 2007). El fallo radica en la interacción entre el subsistema CIFS del kernel y las herramientas de espacio de usuario corporativas (cifs-utils), permitiendo a un atacante local con privilegios mínimos evadir los límites de seguridad y obtener acceso completo como el usuario root.

Resumen técnico:

- Identificador principal: CVE-2026-46243.
- Severidad: Alta (Puntaje base de 7.8 en CVSS v3.1 y hasta 8.5 en CVSS v4.0).
- Causa raíz: Una falla de validación de confianza en el límite entre el espacio de kernel y el espacio de usuario. El tipo de clave cifs.spnego del kernel carecía de la función de enganche .vet_description, lo que provocaba que el sistema aceptara solicitudes de descripción de claves arbitrarias generadas desde el espacio de usuario no confiable, asumiendo erróneamente que provenían del propio cliente CIFS del kernel.
- Mecanismo de falla: Un atacante local invoca la llamada al sistema request_key() para el tipo cifs.spnego inyectando una descripción forjada que contiene campos maliciosos controlados como pid, uid, creduid y la bandera upcall_target=app. Al procesarse la solicitud, el sistema invoca de manera automática al binario auxiliar /usr/sbin/cifs.upcall con privilegios de administrador (root). Al leer la bandera upcall_target=app, el binario ejecuta una transición de espacios de nombres (namespace switch) hacia el pid del atacante. Antes de soltar los privilegios finales (setuid), el binario realiza una consulta de cuentas a través del mecanismo Name Service Switch (NSS). Como el proceso ya se encuentra bajo el control del espacio de nombres del atacante, este suplanta el archivo /etc/nsswitch.conf local y fuerza la carga dinámica de una biblioteca maliciosa propia (ej. libnss_pwn.so.2), logrando la ejecución de comandos arbitrarios en el host de manera directa como root.
- Estado de explotación: Divulgación pública coordinada a finales de mayo de 2026. Se ha confirmado la disponibilidad de un exploit funcional de Prueba de Concepto (PoC) público en repositorios de GitHub, facilitando que actores maliciosos automaticen el ataque.
- Versiones afectadas: Vulnerabilidad presente en el Kernel de Linux desde 2007. Afecta sistemas con cifs-utils 6.14 o superior (o versiones con retro-puertos de namespace). Entre las distribuciones afectadas por defecto se encuentran Linux Mint 21.3/22.3, CentOS Stream 9, Rocky Linux 9, AlmaLinux 9, Kali Linux (2021.4–2026.1)

Impacto potencial:

- Compromiso total del sistema operativo anfitrión: Al lograr el escalamiento a privilegios de root (UID 0), un usuario malicioso de bajo nivel adquiere control absoluto sobre el hardware, sistemas de archivos, procesos y configuraciones del servidor afectado.
- Evasión de los controles tradicionales de integridad: Dado que la inyección de código dañino se realiza a través de la carga dinámica de módulos NSS en memoria, el ataque no requiere modificar binarios legítimos del sistema, lo que le permite evadir sistemas de detección de cambios de archivos estáticos.
- Ruptura de aislamiento en entornos compartidos: En servidores multiusuario, terminales de desarrollo corporativo, ejecutores de integración continua (CI Runners) o entornos de compilación de contenedores, un atacante local puede romper las barreras lógicas de aislamiento y comprometer la seguridad de otros inquilinos o del host subyacente.
- Facilidad de replicación interna mediante PoC público: La disponibilidad del código de explotación simplifica drásticamente la capacidad de integrarlo en vectores de ataque de múltiples etapas, donde un atacante primero obtiene acceso inicial limitado y usa "CIFSwitch" como la fase de consolidación definitiva.

Recomendaciones de mitigación:

1. Aplicación inmediata de parches de Kernel proporcionados por el distribuidor: Es imperativo actualizar el kernel a las compilaciones más recientes que incluyan el parche oficial (el cual restringe y rechaza las descripciones cifs.spnego si no son emitidas de forma interna por las credenciales privadas spnego_cred del cliente CIFS).
2. Desinstalación del paquete cifs-utils en sistemas no requeridos: Si los servidores o estaciones de trabajo no necesitan realizar montajes de red remotos a través de los protocolos SMB/CIFS autenticados con Kerberos, se aconseja purgar y eliminar por completo el software cifs-utils para remover el binario vulnerable del vector de ataque.
3. Negación de las reglas de petición de claves en la configuración local: Como contramedida de mitigación inmediata, se puede anular la regla por defecto de la utilidad modificando el archivo /etc/request-key.d/cifs.spnego.conf e inyectando la directiva de negación: create cifs.spnego * * /usr/sbin/keyctl negate %k 30 %S.
4. Endurecimiento de políticas LSM y deshabilitación de espacios de nombres: Asegurar el uso de políticas restrictivas en SELinux o AppArmor (las configuraciones Enforcing por defecto en plataformas modernas como Rocky Linux 10, Fedora 40+ y CentOS Stream 10 mitigan el ataque de forma nativa). Asimismo, se recomienda deshabilitar el uso de espacios de nombres de usuario sin privilegios (unprivileged user namespaces) mediante parámetros de sysctl si las aplicaciones del entorno no los requieren de forma crítica.

Prioridad: Urgente.

Ampliar información:

- https://blog.segu-info.com.ar/2026/06/cifswitch-vulnerabilidad-del-kernel-de.html
- https://www.suse.com/security/cve/CVE-2026-46243.html
- https://www.igorslab.de/en/cifswitch-linux-kernel-vulnerability-root-privileges/
- https://www.bleepingcomputer.com/news/security/new-cifswitch-linux-flaw-gives-root-on-multiple-distributions/
- https://heyitsas.im/posts/cifswitch/

MULTIPLE WEB SERVERS — CVE-2026-49975 (DENEGACIÓN DE SERVICIO REMOTA CRÍTICA — HTTP/2 BOMB)

Se ha divulgado una técnica de ataque de denegación de servicio remota denominada "HTTP/2 Bomb" que afecta a las configuraciones por defecto de los servidores web y proxies inversos más utilizados a nivel global. El exploit permite a un único atacante remoto, operando incluso desde una conexión doméstica estándar, agotar decenas de gigabytes de memoria RAM en el servidor en cuestión de segundos, comprometiendo por completo la disponibilidad de la infraestructura afectada.

Resumen técnico:

- Identificador principal: CVE-2026-49975 (específico para el componente mod_http2 de Apache httpd). El fallo también se relaciona de forma directa con vulnerabilidades de diseño previas como CVE-2016-6581, CVE-2025-53020, CVE-2016-8740 y CVE-2016-1546.
- Severidad: Crítica (CVSS v3.1: 9.8)
- Causa raíz: Un defecto de diseño en la especificación del protocolo RFC 7541 (HPACK) y RFC 9113. Los servidores web no contabilizan correctamente el consumo de memoria asociado al registro de metadatos administrativos (bookkeeping) para cabeceras vacías, y omiten el conteo de la fragmentación de Cookies (cookie crumbs) contra los límites estándar de campos de cabecera.
- Mecanismo de falla: El exploit combina una bomba de compresión HPACK con un bloqueo de control de flujo tipo Slowloris. El atacante introduce una cabecera en la tabla dinámica y genera miles de referencias indexadas, provocando amplificación de memoria mediante bloques de control reservados por el servidor. Luego anuncia una ventana de control de flujo de cero bytes y envía tramas WINDOW_UPDATE de 1 byte, restableciendo los temporizadores y manteniendo la memoria asignada de forma persistente sin liberar el flujo.

- Estado de explotación: Vulnerabilidad pública. Se ha confirmado la disponibilidad de scripts de prueba de concepto (PoC), entornos de laboratorio basados en Docker y análisis detallados de código. No se ha reportado una explotación masiva maliciosa previa a la mitigación, pero la publicación de los parches facilita la ingeniería inversa del exploit mediante herramientas automatizadas.
- Versiones afectadas: Nginx versiones anteriores a la 1.29.8; Apache HTTP Server versiones anteriores a la 2.4.67 (o implementaciones utilizando mod_http2 anteriores a v2.0.41); Microsoft IIS (incluyendo entornos bajo Windows Server 2025);

Impacto potencial:

- Agotamiento masivo y ultraveloz de la memoria RAM: Un único cliente malicioso es capaz de consumir e inmovilizar entre 32 GB y 64 GB de memoria física en un lapso de entre 10 y 45 segundos, dependiendo del software de servidor web objetivo.
- Degradación sistémica mediante el uso de memoria Swap: Si el ataque se calibra deliberadamente para mantener la presión de memoria justo por debajo del umbral del OOM-killer (mecanismo de eliminación de procesos por falta de memoria), forzará al sistema operativo anfitrión a escribir en disco (swap), provocando que todas las aplicaciones y peticiones legítimas del servidor caigan en un estado de inoperabilidad severa.
- Bypass de controles de inspección perimetral: Debido a que las solicitudes del exploit contienen cabeceras prácticamente vacías, las reglas clásicas de los sistemas de protección (WAF/IPS) basadas en la medición del tamaño máximo de cabecera decodificada no se activan, evadiendo los umbrales de mitigación estándar.
- Interrupción de arquitecturas de microservicios y nubes: Al afectar de forma directa a componentes críticos de infraestructura como Envoy y Cloudflare Pingora, un ataque exitoso tiene el potencial de tumbar balanceadores de carga y proxies de terminación, afectando de manera simultánea a múltiples servicios internos dependientes de esas puertas de enlace.

Recomendaciones de mitigación:

1. Actualización inmediata de binarios y módulos expuestos: Se urge a migrar a Nginx 1.29.8 o superior para beneficiarse de la introducción de la directiva max_headers (configurada con un techo por defecto de 1,000 cabeceras). En el caso de Apache, es mandatorio aplicar la actualización del módulo mod_http2 v2.0.41 o superior, que restringe los fragmentos de cookies dentro del límite de campos permitidos.
2. Desactivación temporal del protocolo HTTP/2: Para plataformas donde aún no existan parches oficiales de remediación completa al momento de esta edición (como Microsoft IIS o implementaciones específicas de proxies), se recomienda deshabilitar temporalmente el soporte de HTTP/2 de manera preventiva, forzando el uso exclusivo de HTTP/1.1 (http2 off; en configuraciones Nginx o Protocols http/1.1 en Apache).
3. Endurecimiento de los límites de memoria por proceso (Workers): Configurar restricciones estrictas de consumo de memoria a nivel del sistema operativo o del orquestador mediante el uso de cgroups, directivas ulimit -v o cuotas de memoria en contenedores. Es preferible que un proceso worker saturado sea finalizado por el OOM-killer y se reinicie limpiamente, a permitir que el ataque consuma los recursos globales del host.
4. Implementación de un cap perimetral en la cantidad de cabeceras: Desplegar una capa de inspección o proxy inverso delante de los servidores vulnerables que aplique un límite estricto e inflexible al número total de campos de cabecera permitidos por petición, asegurando que se contabilicen de manera explícita y separada las subdivisiones de cookies transmitidas en un mismo stream.

Prioridad: Crítica.

Ampliar información:

- https://www.securityweek.com/http-2-bomb-exploit-knocks-web-servers-offline-in-seconds/
- https://thehackernews.com/2026/06/new-http2-bomb-vulnerability-allows.html
- https://blog.calif.io/p/codex-discovered-a-hidden-http2-bomb
- https://cyberinsider.com/new-http-2-bomb-attack-can-exhaust-server-memory-in-seconds/
- https://cybersecuritynews.com/http-2-bomb-remote-dos-exploit/#google_vignette

CVE-2026-41101 – MICROSOFT 365 ANDROID APPS: "FLAGLEFT" (CONTROL DE ACCESO INADECUADO Y SECUESTRO SILENCIOSO DE CUENTAS M365)

Se ha descubierto un grave fallo de configuración y control de acceso bautizado como "FlagLeft" que afecta a múltiples aplicaciones del ecosistema Microsoft 365 en sistemas operativos Android. Debido a un descuido en el código de producción, cualquier aplicación maliciosa de terceros instalada de forma local en el mismo dispositivo móvil del usuario puede extraer de manera completamente silenciosa los tokens de autenticación corporativos, permitiendo un secuestro total de la cuenta de Microsoft 365 sin necesidad de interactuar con la víctima.

Resumen técnico:

- Identificadores principales: CVE-2026-41101 (Word para Android), CVE-2026-42832 (Excel para Android), CVE-2026-41102 (PowerPoint/Office para Android) y CVE-2026-41100 (Microsoft 365 Copilot para Android). El fallo también afecta a Microsoft Loop y OneNote, aunque no recibieron identificadores individuales separados en el boletín inicial.
- Severidad: Variable, alcanzando un nivel de riesgo Importante/Alto (CVSS máximo de 7.7 según la escala CVSS v3, bajo la métrica de control de acceso inapropiado CWE-284).
- Causa raíz: Un error de disciplina en el proceso de desarrollo e integración de software. El equipo de ingeniería dejó habilitada de manera errónea una bandera o flag de depuración (setIsDebugMode(true)) dentro de un kit de desarrollo de software (SDK) compartido por las principales aplicaciones productivas de la suite en la plataforma móvil.
- Mecanismo de falla: El ecosistema de Microsoft 365 en Android utiliza un mecanismo legítimo para compartir accesos y evitar que el usuario deba autenticarse repetidamente al saltar entre herramientas (Single Sign-On). En un escenario normal, el componente de entrega valida estrictamente si la app que solicita el token es un binario oficial y firmado por Microsoft. Sin embargo, al estar el modo de depuración activo de manera generalizada en producción, esta validación de confianza se salta por completo. Una aplicación no verificada de terceros solo requiere ejecutar un fragmento simple de código (alrededor de 15 líneas) pidiendo el acceso para que el SDK de Microsoft le entregue el token de forma automática.
- Estado de explotación: Vulnerabilidad de divulgación pública coordinada (publicada a inicios de junio de 2026 por la firma de ciberseguridad Enclave). Al tratarse de una falla de tipo local (local spoofing), se requiere que exista una app maliciosa en el dispositivo (por ejemplo, mediante una actualización fraudulenta de una app existente o un malware enmascarado). No se dispone de evidencia de

explotación activa y masiva previa al parche, pero la construcción de un exploit funcional es trivial.

- Versiones afectadas: Todas las compilaciones de Word, Excel, PowerPoint, OneNote, Loop y Copilot para Android distribuidas antes de las correcciones de mayo de 2026 (específicamente aquellas anteriores a la versión base de seguridad institucional 16.0.19822.20190). Aplicaciones como Microsoft Teams no se vieron comprometidas al tener el flag correctamente configurado en false.

Impacto potencial:

- Secuestro integral de datos y suplantación de identidad: Al obtener el token de acceso, la aplicación atacante adquiere la capacidad de realizar cualquier acción a nombre del usuario legítimo dentro de la suite corporativa. Esto incluye la lectura y envío de correos electrónicos en Outlook, la visualización de calendarios, la apertura y modificación de archivos en OneDrive/SharePoint, e incluso el acceso a interacciones internas de Copilot.
- Persistente a largo plazo vía tokens FOCI: Los elementos filtrados pertenecen a la familia de tokens FOCI (Family of Client IDs), un diseño de Microsoft que permite refrescar y extender los accesos de forma prolongada en el tiempo. El atacante puede reutilizar y renovar estos accesos durante semanas o meses de forma remota sin que expiren de manera convencional.
- Invisibilidad absoluta para el usuario afectado: La solicitud y exfiltración del token se procesa íntegramente en segundo plano a nivel de sistema operativo. Al usuario nunca se le despliega una pantalla de inicio de sesión, no se le solicita su contraseña ni se le pide confirmar ninguna ventana sospechosa de permisos de Android.
- Evasión de auditorías básicas de telemetría: Debido a que el token FOCI es un recurso legítimo del ecosistema de Microsoft, el tráfico generado por el atacante al consultar o refrescar las API de Azure o Entra ID se registra en los logs de la organización con un formato idéntico al comportamiento cotidiano de un empleado, dificultando drásticamente su detección temprana mediante reglas SIEM convencionales.

Recomendaciones de mitigación:

1. Despliegue y forzado inmediato de actualizaciones: Es crítico asegurar que todos los dispositivos que corren la suite de Office en la organización instalen las últimas versiones disponibles desde la Google Play Store. Las plataformas deben encontrarse obligatoriamente en la versión 16.0.19822.20190 o superior.
2. Automatización y auditoría mediante soluciones MDM: Los equipos de seguridad de la información administradores de flotas de dispositivos móviles institucionales o bajo políticas BYOD deben forzar la distribución masiva de estas actualizaciones utilizando sus consolas de Gestión de Dispositivos Móviles (MDM), bloqueando temporalmente el acceso a recursos corporativos a aquellos dispositivos rezagados.
3. Revocación manual y forzada de los Refresh Tokens vigentes: Debido a que la actualización de la aplicación cierra la brecha de extracción futura pero no invalida los tokens FOCI que un atacante ya pudiera haber recolectado previamente, se recomienda que los administradores de Microsoft Entra ID realicen una revocación explícita de las sesiones y tokens de actualización activos para las cuentas que operen de forma crítica en entornos Android, forzando un re-inicio de sesión global.
4. Robustecimiento de Políticas de Acceso Condicional (Conditional Access): Ajustar las reglas de acceso en el inquilino corporativo de Microsoft 365 para exigir de manera estricta que las conexiones originadas desde terminales móviles provengan exclusivamente de dispositivos marcados como "Seguros y en Cumplimiento" (Compliant Devices), restringiendo el uso de clientes no administrados.

Prioridad: Urgente.

Ampliar información:

- https://www.thecybersignal.com/microsoft-android-office-apps-debug-flag-account-token-exposure-2026/
- https://thehackernews.com/2026/06/microsoft-365-android-apps-let-any-app.html
- https://www.securityweek.com/exclusive-how-one-line-of-code-put-billions-of-microsoft-android-app-downloads-at-risk/
- https://www.darkreading.com/application-security/coding-gaffe-exposes-microsoft-365-accounts-takeover
- https://enclave.ai/blog/flagleft-microsoft-365-android-forgotten-flag-account-takeover

MALWARE

DESCKVB RAT – CAMPAÑA DE MALSPAM DE ALTA ESCALABILIDAD (TROYANO DE ACCESO REMOTO - RAT)

Se ha detectado una sofisticada campaña global de distribución de malware ("malspam") diseñada para desplegar el troyano de acceso remoto DesckVB RAT (activo en el mapa de amenazas desde febrero de 2026). La campaña destaca por emplear técnicas de evasión perimetral mediante el desvío de tráfico a través de dominios legítimos de alta reputación de Google, seguido de un kit de ingeniería social que automatiza la personalización estética del ataque según la empresa de la víctima, culminando en una ejecución puramente residente en memoria de componentes .NET.

Resumen técnico:

- Tipo de amenaza: Troyano de Acceso Remoto (RAT) basado en el framework .NET, empaquetado bajo múltiples capas de loaders y scripts obfuscados.
- Cadena de infección multi-etapa: El ataque se fragmenta en cinco fases para romper las firmas estáticas tradicionales:
- Acceso Inicial (HTML Malicioso): Envío de un correo con un archivo HTML adjunto (Bestellung_2026.html). Al abrirse, ejecuta un redireccionamiento inmediato mediante meta-refresh hacia una URL legítima de seguimiento de clics de Google DoubleClick Campaign Manager (ad.doubleclick[.]net).
- Kit de Suplantación Dinámica: DoubleClick desvía al navegador a un servidor intermedio que decodifica la dirección de correo de la víctima (provista en Base64 en la URL). El kit de entrega (startthewave[.]org) reescribe dinámicamente los títulos, logos corporativos y pies de página extrayendo en tiempo real el favicon y la identidad de la empresa de la víctima mediante llamadas a API externas (como Clearbit o logo.dev), simulando una descarga legítima de un archivo PDF.
- Carga Útil en JScript y PowerShell: Al presionar el botón de descarga, se sirve un archivo ZIP que contiene un script JScript (.js) altamente ofuscado y relleno de código basura. Al ejecutarse, el script valida su ubicación; si está en las carpetas Temp o Downloads, se auto-copia a C:\Users\Public\, evadiendo entornos sandbox, y extrae un script de PowerShell (nlbzl.ps1).
- PowerShell Stager y .NET Loader: El script de PowerShell realiza un barrido de herramientas de análisis (si detecta depuradores como Wireshark o Any.run, fuerza el reinicio inmediato del sistema con Restart-Computer) y descarga un cargador intermedio .NET oculto en un archivo de texto (03.txt).
- Inyección Final (Process Hollowing): Este cargador ensambla la carga final (bl.txt), deshabilita las defensas locales e inyecta reflexivamente el DesckVB RAT en memoria dentro de procesos legítimos y firmados por Microsoft como InstallUtil.exe o MSBuild.exe.

- Mecanismos de Evasión de Defensas: El malware realiza una desactivación agresiva de las características de Microsoft Defender (monitoreo en tiempo real, protección contra intrusiones, envío de muestras) y añade de forma automática todo el disco del sistema (C:\) como ruta de exclusión. Además, para cegar por completo la telemetría del sistema operativo, parcha a nivel de API nativa el componente AMSI (NtManageHotPatch en compilaciones de Windows 11 24H2) y desactiva el rastreo de eventos de Windows (ETW) sobrescribiendo los puntos de entrada de EtwEventWrite en ntdll.dll.
- Infraestructura de Comando y Control (C2): El RAT establece persistencia mediante tareas programadas cíclicas (cada 8-11 minutos) y claves de registro Run/RunOnce con nombres falsos de controladores de video NVIDIA. La comunicación con los servidores C2 (xtadts.ddns[.]net y afxwd.ddns[.]net) se realiza a través de sockets TCP crudos en el puerto no estándar 7211, utilizando mensajes serializados mediante Protobuf y cifrados bajo el algoritmo AES (con claves derivadas por PBKDF2 y un estricto pinning de certificados SHA-256).

Impacto potencial:

- Control remoto total del endpoint comprometido: Al consolidarse en el sistema, el atacante obtiene capacidades irrestrictas para ejecutar comandos arbitrarios en segundo plano, manipular el sistema de archivos, registrar pulsaciones de teclado (keylogging) y exfiltrar información confidencial de la organización.
- Ceguera absoluta en herramientas de monitoreo locales: El parcheo nativo de las funciones clave de AMSI y ETW neutraliza por completo la capacidad de generación de eventos y telemetría de Windows, lo que impide que las soluciones locales de Antivirus y de detección en el Endpoint (EDR/XDR) visualicen el comportamiento malicioso o registren las alertas en los tableros de control de seguridad.
- Potencial despliegue de cargas secundarias de alto impacto: La presencia del RAT actúa como un vector de entrada para intrusiones de manos libres (Hands-on-the-keyboard). Debido a que el malware realiza un perfilado específico buscando arquitecturas de tarjetas gráficas NVIDIA (GTX/RTX) y AMD (Radeon), existe un riesgo inminente de despliegue de criptomineros corporativos o ransomware.
- Alta tasa de éxito en ingeniería social corporativa: Dado que el kit malicioso de correo se rebrandea y adapta estéticamente al vuelo de acuerdo al dominio del correo electrónico del receptor (extrayendo logos y ubicaciones geográficas exactas vía IP), la probabilidad de que los usuarios finales confíen en el flujo fraudulento y ejecuten el archivo comprimido inicial es significativamente elevada.

Recomendaciones de mitigación:

1. Restricción de la ejecución de scripts por defecto mediante GPO: Implementar Objetos de Política de Grupo (GPO) en Active Directory para forzar que los archivos de script con extensiones potencialmente peligrosas, tales como .js, .vbs, .hta y .ps1, se abran de manera predeterminada con editores de texto plano (como Notepad o Notepad++) en lugar del motor de automatización de Windows de ejecución automática (WScript/CScript).
2. Endurecimiento del perímetro de correo y sandboxing de adjuntos: Configurar reglas estrictas en el Gateway de Seguridad de Correo (SEG) para bloquear, aislar o poner en cuarentena correos entrantes provenientes de fuentes externas que contengan adjuntos HTML o archivos comprimidos .zip que custodien scripts en su interior. Es mandatorio contar con políticas de inspección dinámica (Safe Attachments y Safe Links) que analicen el comportamiento al hacer clic.
3. Auditoría e inspección inmediata de exclusiones anómalas de Defender: Monitorear y generar alertas centralizadas prioritarias ante cualquier comando de PowerShell orientado a modificar la configuración de exclusiones de Microsoft Defender (Add-MpPreference -ExclusionPath), especialmente si se intenta excluir la raíz del sistema operativo o el perfil de usuario.
4. Procedimiento de respuesta ante incidentes (Endpoint Triage): En caso de confirmarse que un usuario abrió el adjunto HTML e interactuó con el archivo ZIP, se debe aislar el equipo inmediatamente de la red corporativa. La remediación no debe limitarse a borrar el archivo descargado; se requiere realizar un barrido completo de tareas programadas sospechosas creadas en intervalos de ~10 minutos, revisar las llaves Run de registro bajo el contexto de NVIDIA simulado y proceder a la revocación de sesiones globales y cambio de contraseñas de la cuenta afectada desde un dispositivo limpio.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/06/google-doubleclick-abused-in-new.html
- https://www.huntress.com/blog/malspam-to-deskcvb-rat-delivery-chain-analysis
- https://blog.gridinsoft.com/desckvb-rat-doubleclick-malspam/

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

ATAQUE A LA CADENA DE SUMINISTRO "MIASMA" COMPROMETE MÁS DE 30 PAQUETES NPM DE RED HAT

Se ha hecho pública una de las agresiones más sofisticadas del año contra el ecosistema de desarrollo de código abierto. Un actor de amenazas logró vulnerar el entorno de Integración y Despliegue Continuo (CI/CD) de Red Hat, inyectando un gusano avanzado de robo de credenciales denominado Miasma (una variante altamente evolucionada del malware Mini Shai-Hulud de código abierto) dentro del ámbito legítimo @redhat-cloud-services en el registro de npm. El incidente afectó directamente a 32 paquetes a lo largo de 96 versiones distintas, acumulando decenas de miles de descargas semanales en corporaciones globales antes de su remoción.

Resumen técnico:

- Vector de entrada ("Paciente Cero"): La infección se originó a partir del compromiso de las credenciales y las cookies de sesión de la cuenta de GitHub de un empleado de Red Hat (previamente expuestas en registros de malware infostealer). El atacante utilizó este acceso legítimo para evadir el proceso estándar de revisión de código (code review) e inyectar de manera directa commits huérfanos con modificaciones maliciosas (incluyendo un flujo de trabajo ci.yaml y un script _index.js) en dos repositorios de la organización RedHatInsights.
- Bypass de Publicación de Confianza (Trusted Publishing): El atacante abusó del permiso **id-token: write** en GitHub Actions para obtener un token OIDC de corta duración y publicarlo directamente en npm. Esto permitió distribuir versiones troyanizadas con firmas de proveniencia válidas **SLSA Nivel 3**, haciendo que el paquete pareciera auténtico e indetectable para los escáneres estáticos tradicionales de la cadena de suministro.

- Mecanismo del Payload en la Instalación: El ataque se gatilla de forma automática en el sistema de la víctima (estación de desarrollo o runner de CI/CD) mediante un script de ciclo de vida preinstall incorporado en el archivo package.json ("preinstall": "node index.js"), ejecutándose antes de que finalice el comando npm install. El archivo index.js legítimo de ~200 KB fue sustituido por un dropper ofuscado de 4.29 MB (un aumento de tamaño de 25x).
- Ofuscación y Evasión Avanzada: El malware implementa cuatro capas de protección: un arreglo de caracteres descifrado al vuelo mediante sustitución ROT-XX, desencriptación AES-128-GCM, ofuscación de cadenas tipo Obfuscator.io y un cifrado criptográfico personalizado basado en PBKDF2-HMAC-SHA-256 con 200,000 iteraciones. Una vez descifrado, el dropper descarga de forma autónoma el runtime de JavaScript Bun a directorios temporales y lo utiliza para ejecutar la carga útil principal. Esto genera una cadena anómala de procesos (node.exe → sh/cmd → bun.exe → payload.js) diseñada específicamente para evadir el monitoreo de telemetría centrado exclusivamente en Node.js. Adicionalmente, cuenta con un mecanismo de evasión perimetral que aborta silenciosamente si detecta entornos con configuraciones locales de idioma ruso (ru).
- Objetivos de Extracción de Datos: El malware ejecuta un recolector multi-plataforma que barre el sistema en busca de: secretos de CI/CD (incluyendo GITHUB_TOKEN y ACTIONS_RUNTIME_TOKEN), credenciales de nubes principales (identidades administradas y OAuth2 de Azure IMDS, metadatos y roles IAM de AWS IMDS/ECS, y cuentas de servicio de GCP), tokens de HashiCorp Vault, secretos de Kubernetes y archivos kubeconfig, tokens de publicación de npm y PyPI, llaves privadas SSH, credenciales de registros Docker, datos de billeteras criptográficas y archivos .env. Sorprendentemente, para evadir el enmascaramiento tradicional de secretos de GitHub, el malware escanea el directorio /proc en sistemas Linux para localizar el PID del proceso Runner.Worker de GitHub Actions y extrae los secretos directamente de la memoria en ejecución.

Impacto potencial:

- Compromiso sistémico de secretos corporativos y de nube: El robo masivo de identidades de nube (AWS, Azure, GCP) y secretos de orquestación (Kubernetes, Vault) otorga a los atacantes las llaves de acceso para pivotar de manera remota hacia la infraestructura de producción de las empresas que hayan descargado los paquetes afectados, facilitando intrusiones complejas a gran escala.
- Erosión del modelo de confianza en la proveniencia (SLSA): Al demostrarse que un pipeline comprometido internamente puede acuñar y firmar atestaciones válidas de Sigstore/SLSA sobre código malicioso, se debilita la confianza en los mecanismos modernos de firma de software, obligando a los defensores a depender de análisis de comportamiento dinámico en tiempo de ejecución en lugar de solo confiar en certificados de origen.
- Persistente a nivel de herramientas de desarrollo: Miasma no se limita al directorio del proyecto; inyecta ganchos de persistencia modificando configuraciones locales del usuario como el archivo ~/.claude/settings.json (para la herramienta Anthropic Claude Code) e insertando tareas automatizadas en .vscode/tasks.json configuradas para ejecutarse inmediatamente al abrir cualquier carpeta en Microsoft Visual Studio Code, lo que significa que borrar la carpeta node_modules no desinfecta el host.
- Gatillo destructivo contra remediaciones (Wiper Fail-Safe): El malware planta deliberadamente un token señuelo falso (honeytoken). Si detecta que un administrador de seguridad interactúa con él, intenta revocarlo o altera los archivos de configuración sin el orden adecuado, se activa un interruptor destructivo de "hombre muerto" que ejecuta un borrado total y forzado del directorio del usuario (rm -rf ~/ y ~/Documents).

Recomendaciones para mitigar el riesgo:

1. Aislamiento perimetral y contención inmediata de endpoints: Cualquier servidor, estación de trabajo de desarrollo o runner de CI/CD que haya ejecutado el comando npm install o npm ci utilizando el ámbito @redhat-cloud-services a partir del 1 de junio de 2026 debe ser aislado de inmediato de la red corporativa y ser sometido a un triage forense exhaustivo. Debido a las persistencias en herramientas de desarrollo, se recomienda el re-image del sistema.
2. Desactivación global de scripts de ciclo de vida (Mitigación Primaria): Configurar de manera estricta los entornos corporativos y pipelines para mitigar la ejecución automática de payloads en la instalación. Esto se logra forzando el uso del parámetro --ignore-scripts durante el despliegue (npm install --ignore-scripts) o estableciendo la directiva ignore-scripts=true dentro del archivo de configuración global .npmrc.
3. Rotación masiva y revocación de secretos expuestos: Es obligatorio iniciar un proceso de revocación global y regeneración de credenciales para todas las cuentas e infraestructuras potencialmente comprometidas en el entorno afectado, priorizando tokens de acceso personal (PAT) de GitHub, tokens de npm/PyPI, claves de acceso a nubes públicas, certificados de Kubernetes y llaves SSH institucionales.
4. Auditoría de persistencias locales y endurecimiento de flujos CI/CD: Realizar auditorías sobre los repositorios de la organización buscando la creación inesperada de ramas transitorias, archivos .github/setup.js o flujos de trabajo que demanden el permiso id-token: write. Asimismo, se deben implementar reglas de control de salida de red (Egress Filtering) en los entornos de ejecución de las pipelines para bloquear conexiones hacia destinos no autorizados, permitiendo únicamente el tráfico hacia el registro privado o proxies internos (como Artifactory).

Prioridad: Importante.

Ampliar Información:

- https://thehackernews.com/2026/06/miasma-supply-chain-attack-compromises.html
- https://es.aikido.dev/blog/red-hat-npm-packages-compromised-credential-stealing-worm
- https://unit42.paloaltonetworks.com/monitoring-npm-supply-chain-attacks/
- https://unaaldia.hispasec.com/un-ataque-a-paquetes-npm-de-red-hat-distribuye-el-malware-miasma/
- https://www.microsoft.com/en-us/security/blog/2026/06/02/preinstall-persistence-inside-red-hat-npm-miasma-credential-stealing-campaign/