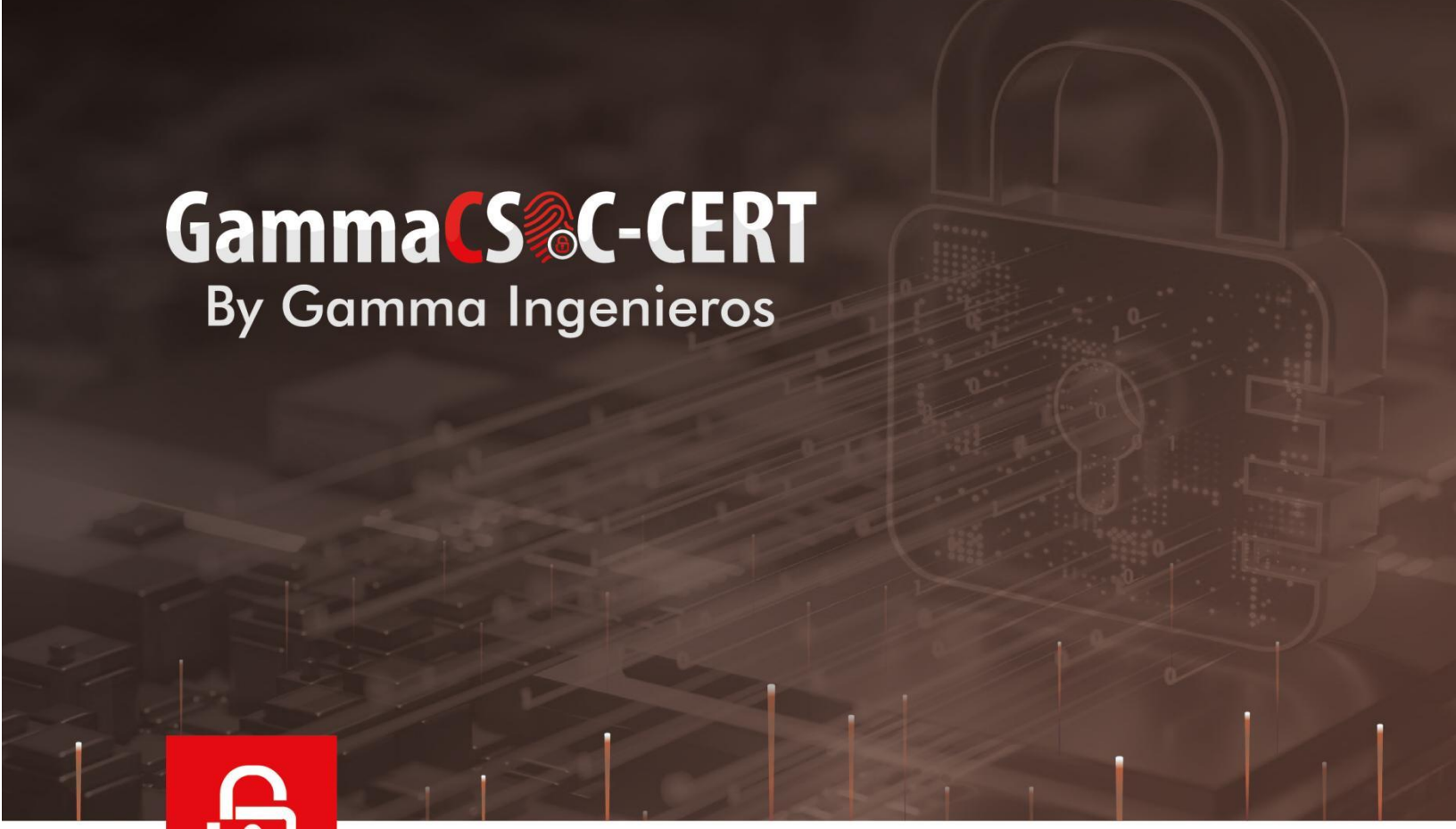
GammaCSOC-CERT
By Gamma Ingenieros



GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4026

TLP:GREEN
TRAFFIC LIGHT PROTOCOL
https://www.first.org/tlp/

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN °4026

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 para nuestros 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	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

FORTINET FORTIMAIL – VULNERABILIDAD CRÍTICA DE PATH TRAVERSAL Y BYTE NULO PERMITE ESCRITURA ARBITRARIA DE ARCHIVOS Y EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-104286)

Fortinet ha publicado un aviso de seguridad para corregir una vulnerabilidad de severidad crítica que combina un fallo de travesía de directorio (Path Traversal) con la neutralización incorrecta de caracteres de byte nulo en la interfaz web de FortiMail. La falla permite a un atacante remoto no autenticado escribir archivos arbitrarios en el sistema operativo subyacente mediante el envío de solicitudes HTTP o HTTPS especialmente manipuladas. Al tratarse de un gateway de correo perimetral expuesto, la explotación de esta debilidad permite comprometer la integridad del dispositivo, inyectar librerías maliciosas, establecer persistencia y potencialmente lograr la ejecución remota de código o comandos con máximos privilegios.

Resumen técnico:

- Identificador principal: CVE-2026-104286 (Boletín FG-IR-26-175).
- Severidad: Crítica (CVSS v3.1: 9.8 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Restricción inadecuada de un nombre de ruta a un directorio restringido (CWE-22) y neutralización incorrecta de caracteres de byte nulo (CWE-158) en la lógica de procesamiento de solicitudes de la función de Cifrado Basado en Identidad (IBE).
- Mecanismo de falla:
- Un atacante remoto sin autenticación transmite solicitudes HTTP o HTTPS manipuladas (como peticiones POST hacia la ruta /ibe que incluyen secuencias de travesía ../ y caracteres de byte nulo %00).
- La aplicación falla en validar de forma estricta la ruta de destino y en sanear el carácter de byte nulo, lo que permite eludir las restricciones de carpeta e indicar al sistema de archivos la creación o sobrescritura de archivos fuera de los directorios permitidos.
- El atacante utiliza esta capacidad de escritura arbitraria para desplegar archivos maliciosos (tales como /data/lib/liblog.so o la modificación de /data/etc/ld.so.preload), logrando inyectar código dinámico que se ejecuta en el contexto del sistema operativo.
- Estado de explotación: Divulgada oficialmente el 1 de octubre de 2026 (con actualizaciones de solución publicadas entre el 5 y el 7 de octubre). Se encuentra confirmada en explotación activa masiva en el entorno real e incluida en el catálogo KEV de la CISA. Se registran indicadores de compromiso que incluyen la creación no autorizada de cuentas de archivado remoto y tareas programadas cron maliciosas.
- Versiones afectadas: FortiMail en las ramas 8.0 (versiones 8.0.0 a 8.0.1), 7.6 (versiones 7.6.0 a 7.6.6), 7.4 (versiones 7.4.0 a 7.4.8) y 7.2 (versiones 7.2.0 a 7.2.9). (Los clientes de FortiMail Cloud fueron remediados automáticamente por el fabricante).

Impacto potencial:

- Escritura arbitraria de archivos y alteración del sistema: Permite modificar o depositar archivos arbitrarios en rutas críticas del sistema de archivos sin requerir credenciales ni interacción del usuario.
- Ejecución remota de código (RCE) no autorizada: Habilita la inyección de bibliotecas dinámicas compartidas y ejecutables modificados en la plataforma, derivando en el control total del dispositivo con privilegios administrativos (root).

- Establecimiento de persistencia y exfiltración de correo corporativo: Permite configurar tareas cron maliciosas o políticas de archivado remoto no autorizadas para redirigir y copiar el correo entrante y saliente hacia infraestructura atacante, como la IP 79.141.169.187.
- Compromiso total del perímetro de red y movimiento lateral: Permite capturar credenciales de administración, interceptar enlaces de restablecimiento de contraseña y utilizar el appliance perimetral como punto de pivote no detectado para ingresar a la red interna corporativa.

Recomendaciones de mitigación:

1. Actualización prioritaria del firmware de FortiMail: Desplegar inmediatamente la actualización del sistema a las versiones corregidas 8.0.2, 7.6.7 o 7.4.9 (o superiores). En el caso de instancias en la rama 7.2 (sin parche planificado), se debe migrar de manera obligatoria hacia la rama 7.4.9 o posterior.
2. Desactivación del servicio IBE (Mitigación temporal inmediata): En caso de no poder aplicar la actualización de forma inmediata, deshabilitar la funcionalidad Identity-Based Encryption mediante la interfaz gráfica (Encryption -> IBE -> IBE Service 'off') o ejecutando en la CLI:config system encryption ibe, set status disable, end.
3. Restricción de exposición y filtrado en WAF: Bloquear el acceso a la interfaz web/administración de FortiMail desde Internet público, limitando la conectividad a segmentos locales de administración o VPN de confianza. Configurar el WAF perimetral para bloquear peticiones POST entrantes hacia /ibe que contengan secuencias ../.
4. Auditoría forense y caza de amenazas (Threat Hunting): Inspeccionar los logs del sistema y el almacenamiento interno en busca de IoCs reportados, evaluando la presencia de cuentas de archivo anómalas (como archive234), modificaciones en /data/etc/ld.so.preload, ejecuciones de cron asociadas a /migadmin, y conexiones salientes hacia las direcciones IP 79.141.169.187 y 45.129.0.192.

Prioridad: Crítica.

Ampliar información:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-175
- https://www.hitcommunications.com/es-co/blog/fortimail-zero-day-cve-2026-104286-email-security
- https://csirt.telconet.net/comunicacion/boletines-servicios/cisa-agrega-vulnerabilidad-critica-de-fortinet-fortimail-al-catalogo-kev-tras-explotacion-activa/
- https://hard2bit.com/en/blog/fortimail-zero-day-cve-2026-104286-patch-iocs/
- https://socprime.com/blog/cve-2026-104286-critical-fortimail-zero-day-exploited-for-unauthenticated-file-writes/

GITLAB AI GATEWAY – VULNERABILIDAD CRÍTICA DE OMISIÓN DE SANDBOX Y ESCAPE DE PLANTILLAS PERMITE EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-90970)

GitLab ha publicado actualizaciones de seguridad de emergencia para corregir una vulnerabilidad de severidad crítica en el componente autoalojado de GitLab AI Gateway. La falla se debe a una neutralización inadecuada en el motor de plantillas de flujos personalizados. Bajo ciertas condiciones, un usuario autenticado con acceso a la plataforma Duo Agent Platform puede enviar una configuración de flujo manipulada para escapar del entorno aislado (sandbox) de la plantilla de instrucciones (prompt template) y ejecutar comandos arbitrarios en el sistema operativo del servidor.

Resumen técnico:

- Identificador principal: CVE-2026-90970.
- Severidad: Crítica (CVSS v3.1: 9.9 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).
- Causa raíz: Neutralización incorrecta de elementos especiales utilizados en un motor de plantillas (CWE-1336) dentro de las definiciones de flujos personalizados del AI Gateway.
- Mecanismo de falla:
- AI procesar flujos de trabajo personalizados en Duo Agent Platform, la aplicación evalúa plantillas de instrucciones configuradas por el usuario.
- La falta de saneamiento e insuficiente restricción de entrada en el motor de plantillas permite inyectar secuencias que omiten los límites de ejecución del sandbox.
- Esto permite que un atacante autenticado invoque intérpretes del sistema operativo (como consolas Unix/Shell) directamente en el contenedor del AI Gateway, logrando la ejecución de comandos con los privilegios del servicio.
- Estado de explotación: Divulgada oficialmente el 2 de octubre de 2026. No se registra evidencia de explotación activa en el entorno real ni disponibilidad de proof of concept (PoC) público masivo al momento de la divulgación. (Los servicios gestionados GitLab.com y GitLab Dedicated fueron corregidos previamente por el fabricante y no requieren acción).
- Versiones afectadas: Despliegues autoalojados de GitLab AI Gateway en versiones desde la 18.1.6 hasta anteriores a la 19.2.4, rama 19.3 anteriores a la 19.3.2, y rama 19.4 anteriores a la 19.4.1.

Impacto potencial:

- Ejecución remota de código (RCE) no autorizada: Otorga a un usuario autenticado la capacidad de ejecutar comandos arbitrarios en el servidor del AI Gateway.
- Exfiltración de credenciales y claves de firmado: Permite acceder a llaves de firmado de tokens JWT, secretos de integración con proveedores de modelos de IA y credenciales de acceso al servicio principal de GitLab.
- Movimiento lateral hacia la infraestructura de desarrollo: Facilita el pivoteo desde el contenedor del AI Gateway hacia repositorios de código fuente, flujos de CI/CD y servicios adyacentes de la organización.
- Interrupción de servicios y alteración de modelos: Habilita la manipulación de configuraciones de IA, corrupción de plantillas de prompts corporativas y posible denegación de servicio en la plataforma Duo Agent.

Recomendaciones de mitigación:

1. Actualización prioritaria del contenedor/despliegue de AI Gateway: Actualizar de inmediato las instancias autoalojadas del AI Gateway a las versiones corregidas 19.2.4, 19.3.2 o 19.4.1 (verificando la etiqueta de la imagen Docker o Helm chart desplegada, independientemente de la versión de la aplicación GitLab).
2. Restricción de permisos y auditoría de Duo Agent Platform: Auditar y restringir los accesos de usuarios a las funcionalidades de creación y edición de flujos personalizados (custom flows) en la plataforma Duo Agent.
3. Segmentación de red y aislamiento de carga (Zero Trust): Aplicar políticas de microsegmentación de red para restringir el tráfico de salida del AI Gateway únicamente hacia las APIs de modelos de IA autorizadas y servidores GitLab indispensables.
4. Monitoreo y detección de procesos anómalos: Implementar reglas de detección en EDR/SIEM para alertar sobre la creación de procesos secundarios inusuales (ej. /bin/sh, bash u otras consolas) generados desde el proceso contenedor del AI Gateway.

Prioridad: Crítica.

Ampliar información:

- https://aviatrix.ai/threat-research-center/gitlab-ai-gateway-rce-cve-2026-90970-2026/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-gitlab-ai-gateway-permite-ejecucion-remota-de-codigo/
- https://www.esecurityplanet.com/threats/news-gitlab-ai-gateway-cve-2026-90970/
- https://socradar.io/blog/cve-2026-90970-gitlab-ai-gateway-rce/
- https://thehackernews.com/2026/10/gitlab-patches-critical-self-hosted-ai.html

DELL CONTAINER STORAGE MODULES (CSM) – VULNERABILIDAD CRÍTICA DE FALTA DE AUTENTICACIÓN PERMITE LA EXTRACCIÓN DE CREDENCIALES ADMINISTRATIVAS DE ALMACENAMIENTO (CVE-2026-63688)

Dell ha publicado un aviso de seguridad (DSA-2026-448) para corregir múltiples vulnerabilidades críticas en Dell Container Storage Modules (CSM), destacando una falla de máxima severidad por falta de autenticación en funciones críticas dentro del servidor gRPC csm-authorization-storage. La vulnerabilidad permite a un atacante remoto no autenticado obtener las credenciales de administrador del backend de almacenamiento para todos los arreglos registrados (PowerStore, PowerScale, PowerFlex, PowerMax y Unity XT). Esta anulación completa del modelo de seguridad de csm-authorization concede control total sobre la infraestructura de almacenamiento conectada a clústeres de Kubernetes y Red Hat OpenShift.

Resumen técnico:

- Identificador principal: CVE-2026-63688 (Aviso de seguridad DSA-2026-448).
- Severidad: Crítica (CVSS v3.1: 10.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).
- Causa raíz: Falta de autenticación en funciones críticas (Missing Authentication for Critical Function - CWE-306) en el servidor gRPC csm-authorization-storage.
- Mecanismo de falla:
- El servicio csm-authorization-storage gestiona la autenticación y el control de acceso entre los controladores CSI/cargas de trabajo de Kubernetes y las plataformas de almacenamiento de Dell.
- La implementación del servidor gRPC falla en verificar y autenticar las solicitudes entrantes dirigidas a funciones sensibles de la API de almacenamiento.
- Un atacante remoto con conectividad de red hacia el puerto gRPC puede enviar solicitudes manipuladas sin credenciales para extraer directamente las claves y contraseñas de administrador de todos los arreglos de almacenamiento registrados.
- Estado de explotación: Divulgada oficialmente el 1 de octubre de 2026 (con revisiones del aviso publicadas el 5 y 6 de octubre). No se registra evidencia de explotación activa en el entorno real al momento de la publicación.
- Versiones afectadas: Dell Container Storage Modules (CSM) en todas las versiones anteriores a la 1.18.0 (afecta a las ramas previas a v1.17.0 y v1.18.0).

Impacto potencial:

- Extracción masiva de credenciales administrativas: Permite a un atacante no autenticado obtener las contraseñas de administración de todos los sistemas de almacenamiento Dell registrados (PowerStore, PowerScale, PowerFlex, PowerMax y Unity XT).
- Bypass completo del modelo de autorización y multitenencia: Invalida el aislamiento entre inquilinos (tenants), permitiendo a un atacante acceder, modificar, sobrescribir o eliminar volúmenes y datos pertenecientes a cualquier aplicación o usuario en el entorno.
- Escalada de privilegios a nivel de nodo y clúster: Al combinarse con otras fallas del mismo boletín (como CVE-2026-67269 o CVE-2026-67273), un atacante puede ejecutar código no autorizado, elevar privilegios a nivel root en los nodos de Kubernetes y leer Secrets en todo el clúster.
- Persistencia mediante claves cableadas y tokens forjados: La presencia de secretos criptográficos hardcodeados en módulos adyacentes permite la creación de tokens JWT administrativos válidos, garantizando la persistencia del atacante en el sistema.

Recomendaciones de mitigación:

1. Actualización prioritaria a Dell CSM 1.18.0: Actualizar de forma inmediata todas las instalaciones de Dell Container Storage Modules a la versión 1.18.0 o superior, dado que no existen parches virtuales ni soluciones temporales por configuración.
2. Rotación obligatoria de credenciales y claves criptográficas: Después de actualizar a la versión v1.18.0, cambiar inmediatamente las contraseñas de administrador de los arreglos de almacenamiento Dell conectados y reemplazar las claves de firmado JWT utilizadas por csm-authorization.
3. Aislamiento y segmentación de puertos gRPC: Restringir la exposición del servidor gRPC de autorización mediante políticas de red (Network Policies/Firewalls), limitando el tráfico exclusivamente a pods autorizados dentro del clúster de Kubernetes.
4. Auditoría de recursos y caza de amenazas (Threat Hunting): Inspeccionar los logs de auditoría del clúster en busca de la creación anómala de recursos personalizados ContainerStorageModule, modificaciones en roles RBAC y lectura no autorizada de Secrets por parte de cuentas de servicio.

Prioridad: Crítica.

Ampliar información:

- https://www.dell.com/support/kbdoc/en-us/000515771/dsa-2026-448-security-update-for-dell-container-storage-modules-multiple-vulnerabilities
- https://thehackernews.com/2026/10/dell-csm-flaws-enable-unauthenticated.html
- https://forkast.news/administrative-bypass-in-dell-csm-six-vulnerabilities-expose-storage-backend-credentials/
- https://fieldeffect.com/blog/dell-max-severity-vulnerabilities-container-storage-modules
- https://cyberexperts.com/2026-10-05-dell-csm/

MALWARE

CAMPAÑA MALFEX EN NPM – PAQUETES MALICIOSOS DE CADENA DE SUMINISTRO DISTRIBUYEN EL TROYANO OVERLORD RAT Y EL LADRÓN DE INFORMACIÓN MOVINLIKE AFECTANDO A ENTORNO DE DESARROLLO WINDOWS

Investigadores de ciberseguridad de Checkmarx y CloudSEK han documentado la campaña de ataque a la cadena de suministro de software denominada MALFEX, activa desde agosto de 2023 en el registro de paquetes npm. El operador de la amenaza, asociado al alias "Murizada", ha publicado al menos 12 paquetes (8 de los cuales contienen cargas maliciosas) logrando superar las 40.000 descargas acumuladas. La campaña utiliza varias rutas de ejecución durante la instalación (postinstall) o carga de los paquetes para desplegar en sistemas Windows el troyano de acceso remoto (RAT) de código abierto Overlord, el infostealer movinlike y cargadores secundarios orientados al robo de credenciales, tokens de Discord, sesiones de Telegram y monederos de criptomonedas.

Resumen técnico:

- Identificador principal: Campaña MALFEX (Paquetes npm: function-flag, cdn-img-fetch, function-color, img-to-native, native-runner, tlxbnhd, tldriver, mxdriver).
- Tipo de amenaza: Ataque a la cadena de suministro (Software Supply Chain) / Troyano de Acceso Remoto (RAT) / Ladrón de información (Infostealer) / Cargador de malware (Loader).
- Mecanismo de acceso e infección:
- Infección mediante ganchos del ciclo de vida npm (postinstall / preinstall): Durante la instalación de los paquetes mediante npm install, se ejecutan scripts maliciosos de JavaScript que descargan ejecutables de Windows disfrazados de archivos de imagen PNG/JPG o archivos autoextraíbles IExpress.
- Cadenas de dependencias y ejecución al cargar: Ciertos paquetes (como img-to-native y cdn-img-fetch) requieren librerías maliciosas intermedias que extraen ejecutables cifrados mediante AES ocultos al final de imágenes legítimas, desplegando el infostealer movinlike de 64 MB al cargarse el paquete en tiempo de ejecución.
- Ocultación y evasión en scripts: Se emplean técnicas como el uso de espacios masivos para desplazar el código malicioso fuera del área visible del editor, rutinas en funciones de arte ASCII y fallos silenciosos en sistemas macOS/Linux para concentrar la infección de forma desapercibida en entornos Windows.
- Capacidades operativas y canal de Comando y Control (C2):
- Overlord RAT: Implementado en Go, ofrece captura de pantalla, registro de pulsaciones de teclas (keylogging), monitoreo de ventanas, terminal remota, navegación de archivos y escritorio oculto (HVNC). Permite recuperar direcciones C2 mediante la lectura de memorandos cifrados en transacciones de la cadena de bloques Solana.
- Infostealer movinlike: Desarrollado en Node.js, extrae credenciales, cookies y datos de tarjetas de más de 7 navegadores web (Chrome, Edge, Brave, Opera, etc.), tokens de 8 clientes de Discord, sesiones de Telegram y claves de billeteras criptográficas (MetaMask, Phantom, Coinbase).

- Persistencia: Configura una tarea programada en Windows denominada \Maiden que ejecuta el malware cada 5 minutos, con fecha de inicio retroactiva (1 de enero de 2020) para evadir inspecciones rutinarias del registro.
- Estado de actividad: Campaña activa detectada y divulgada a principios de octubre de 2026. Diversos paquetes maliciosos (como function-flag con más de 37.000 descargas) continuaban estando disponibles para instalación sin alertas oficiales completas.
- Plataformas afectadas: Sistemas operativos Microsoft Windows (sistemas de desarrollo con Node.js y npm).

Impacto potencial:

- Control remoto completo y monitoreo sigiloso del equipo de desarrollo: Permite a los atacantes controlar interactivamente el sistema infectado a través de Overlord RAT, capturar pantallas, registrar pulsaciones de teclado y acceder a la consola de comandos.
- Compromiso y exfiltración masiva de credenciales y activos financieros: Facilita el robo sistemático de contraseñas guardadas en navegadores, cookies de sesión, tokens de autenticación de Discord/Telegram y claves privadas de monederos de criptomonedas.
- Infiltración en la cadena de suministro de código fuente y proyectos corporativos: Compromete los entornos de desarrollo de software, permitiendo la contaminación de repositorios, código fuente corporativo y secretos de integración (API keys y tokens de CI/CD).
- Persistencia prolongada y evasión de soluciones de seguridad: El uso de tareas programadas con metadatos retroactivos, ejecutables disfrazados de imágenes y la ausencia de avisos de seguridad en paquetes activos facilita la permanencia prolongada en los endpoints.

Recomendaciones de mitigación:

1. Auditoría e inspección urgente de dependencias npm: Auditar inmediatamente los archivos de bloqueo (package-lock.json, yarn.lock, pnpm-lock.yaml) e inventarios de proyectos en busca de los paquetes identificados (function-flag, function-color, cdn-img-fetch, img-to-native, native-runner, tlxbnhd, tldriver, mxdriver).
2. Restricción y deshabilitación de scripts de instalación npm: Desactivar la ejecución automática de scripts de ciclo de vida durante la instalación mediante la opción --ignore-scripts en la CLI de npm o configurando ignore-scripts=true en los archivos .npmrc de la organización.
3. Búsqueda de artefactos de host e Indicadores de Compromiso (IoCs): Inspeccionar los sistemas en busca de la tarea programada \Maiden, archivos en %APPDATA%\Microsoft\Windows\node_runtime_helper.exe o %APPDATA%\node.exe, y bloquear conexiones hacia los dominios y servidores identificados (cdnzona.discloud.app, 104.234.65.75, etc.).
4. Aislamiento de hosts afectados y rotación inmediata de credenciales: En caso de detectar instalaciones de estos paquetes, aislar de inmediato la estación de trabajo, rotar de forma urgente todas las contraseñas guardadas, revocar tokens de Discord/Telegram, y transferir los fondos de monederos criptográficos a nuevas billeteras seguras desde un equipo no comprometido.

Prioridad: Urgente.

Ampliar información:

- https://certi.news/es/article/15586
- https://thehackernews.com/2026/10/eight-malicious-npm-packages-downloaded.html
- https://aviatrix.ai/threat-research-center/malfex-npm-supply-chain-overlord-rat-2024/
- https://cybersecuritynews.com/malfex-npm-malware/
- https://techaiwire.com/articles/malfex-npm-malware-campaign-overlord-rat-solana/

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

DESMANTELAMIENTO DEL GRUPO DE RANSOMWARE KILLSEC – OPERACIÓN INTERNACIONAL KILLSWITCH DESMANTELA INFRAESTRUCTURA Y SERVIDORES VINCULADOS A MÁS DE 1.000 CIBERATAQUES

Una operación policial e internacional coordinada por Europol, Eurojust y las autoridades de Alemania (liderada por la Policía Criminal y Fiscalía de Hamburgo) con la participación de EE. UU. y varios países europeos ha logrado el desmantelamiento de la infraestructura del grupo cibercriminal de ransomware KillSec. La banda, activa desde 2024 y responsable de cerca de 1.000 ciberataques a nivel mundial, utilizaba esquemas de doble extorsión y herramientas de inteligencia artificial para seleccionar víctimas y gestionar sus servidores. La intervención culminó con la incautación de 5 servidores centrales, la toma de control de sus sitios de filtración en la dark web, la incautación de carteras de criptomonedas y la protección de más de 110 Terabytes de datos robados.

Resumen técnico:

- Identificador principal: Operación internacional KillSwitch (Operación ROTOMA en España) / Grupo cibercriminal KillSec.
- Tipo de amenaza: Ransomware como Servicio (RaaS) / Doble extorsión / Exfiltración y venta de datos confidenciales.
- Modo de operación: Explotación de vulnerabilidades de software y puntos de acceso mal protegidos (especialmente en entornos de almacenamiento en la nube); uso de inteligencia artificial para mapeo de víctimas y mantenimiento de infraestructura; exfiltración de información sensible seguida de extorsión económica bajo amenaza de divulgación pública en sitios web de la dark web.
- Estado de actividad: Desmantelado (servidores e infraestructura incautados, dominios redirigidos a un aviso policial y 3 detenciones provisionales clave ejecutadas el 30 de septiembre de 2026).
- Entidades y sectores afectados: Más de 280 víctimas confirmadas y 500 ataques exitosos en sectores críticos como salud, administración pública, finanzas y empresas privadas en Europa (España, Alemania, Reino Unido) y Estados Unidos.

Impacto potencial:

- Compromiso y exfiltración masiva de datos sensibles: Exposición de más de 110 TB de datos corporativos, gubernamentales y personales retenidos en la infraestructura del grupo criminal.
- Pérdidas financieras elevadas por extorsión e interrupción operativa: Exigencias de rescate en criptomonedas de hasta 500.000 euros/dólares e impactos económicos significativos en las organizaciones afectadas (con daños superiores al millón de euros en ataques individuales).
- Riesgo por dispersión de herramientas RaaS a afiliados: La comercialización del kit de ransomware a terceros incrementó el volumen global de ciberataques contra infraestructuras vulnerables.
- Incumplimiento regulatorio y daño reputacional: Divulgación pública no autorizada de información confidencial en la dark web, exponiendo a las organizaciones afectadas a sanciones regulatorias (GDPR/NIS2) y severo impacto a la reputación.

Recomendaciones para mitigar el riesgo:

1. Auditoría e inspección de servicios expuestos y almacenamiento en la nube: Identificar y corregir puntos de acceso deficientemente protegidos, cerrando puertos innecesarios y aplicando parches a vulnerabilidades en infraestructura perimetral y en la nube.
2. Implementación de autenticación multifactor (MFA) y mínimo privilegio: Forzar el uso de MFA en todas las interfaces administrativas y de acceso remoto, restringiendo estrictamente las políticas de acceso e identidades en entornos corporativos.
3. Estrategia de copias de seguridad inmutables y aisladas (Offline): Mantener respaldos periódicos desconectados de la red principal y verificar la capacidad de restauración para mitigar el impacto de ataques de cifrado.
4. Evaluación de compromiso y monitoreo de credenciales: Analizar la telemetría interna para verificar posibles interacciones pasadas con la infraestructura de KillSec y proceder con la rotación obligatoria de credenciales y claves de acceso que hayan podido ser expuestas.

Prioridad: Urgente.

Ampliar Información:

- https://www.infobae.com/america/agencias/2026/10/01/cae-killsec-el-grupo-de-ransomware-liderado-presuntamente-por-un-adolescente-de-16-anos/
- https://www.elcolombiano.com/tecnologia/killsec-desmantelado-operacion-killswitch-europol-grupo-liderado-por-adolescente-16-anos-LJ41848452#google_vignette
- https://web.guardiacivil.es/es/destacados/noticias/Un-detenido-en-Espana-en-una-operacion-internacional-contra-el-grupo-de-ransomware-KillSec/
- https://korben.info/es/desmantelan-killsec-presunto-administrador-16-anos.html
- https://mexicobusiness.news/es/cybersecurity/news/europa-arresta-presunto-lider-de-killsec-en-investigacion