GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º0726

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

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN º0726

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	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

DELL RECOVERPOINT FOR VIRTUAL MACHINES — CREDENCIAL EMBEBIDA CON ACCESO ROOT REMOTO (CVE-2026-22769)

Dell ha emitido una alerta crítica tras confirmarse la explotación activa de una vulnerabilidad de tipo zero-day en su solución RecoverPoint for Virtual Machines. El fallo, descubierto por Mandiant y Google Threat Intelligence Group (GTIG) durante investigaciones de respuesta a incidentes, ha sido aprovechado por el actor de amenazas UNC6201 —cluster con presuntos vínculos con la República Popular China y nexos con Silk Typhoon— desde al menos mediados de 2024, con el fin de moverse lateralmente, mantener acceso persistente y desplegar malware avanzado, incluyendo los backdoors BRICKSTORM, GRIMBOLT y el webshell SLAYSTYLE.

Resumen técnico:

- Identificador principal: CVE-2026-22769 (Advisory DSA-2026-079).
- Severidad: 10.0 (Crítica) en la escala CVSSv3.1.
- Causa raíz: Uso de credenciales embebidas (hardcoded) en el archivo de configuración del Apache Tomcat Manager (/home/kos/tomcat9/tomcat-users.xml), clasificado bajo CWE-798.
- Mecanismo de falla: Un atacante remoto no autenticado, con conocimiento de las credenciales por defecto del usuario admin, puede autenticarse en el Tomcat Manager de Dell RecoverPoint, cargar un archivo WAR malicioso mediante el endpoint /manager/text/deploy, y ejecutar comandos arbitrarios con privilegios de root sobre el appliance comprometido.
- Estado de explotación: Explotación activa confirmada en entornos reales desde mediados de 2024. La vulnerabilidad ha sido añadida al catálogo KEV (Known Exploited Vulnerabilities) de CISA, con mandato de parcheo urgente para agencias federales.
- VVersiones afectadas: Dell RecoverPoint for Virtual Machines versiones anteriores a 6.0.3.1 HF1, incluyendo 6.0, 6.0-sp1, 6.0-sp1_p1, 6.0-sp1_p2, 6.0-sp2, 6.0-sp2_p1, 6.0-sp3 y 6.0-sp3_p1.

Impacto potencial:

- Acceso root no autenticado: El atacante obtiene control total del sistema operativo subyacente del appliance sin necesidad de credenciales válidas del entorno víctima.
- Despliegue de malware persistente: UNC6201 ha utilizado esta vulnerabilidad para instalar los backdoors GRIMBOLT y BRICKSTORM, modificando el script legítimo convert_hosts.sh para garantizar la ejecución en cada reinicio del sistema.
- Pivoteo hacia infraestructura VMware: Los atacantes han creado "Ghost NICs" (interfaces de red temporales falsas) en máquinas virtuales ESXi para moverse sigilosamente hacia redes internas y entornos SaaS, eliminando los rastros tras su uso.
- Exfiltración y espionaje prolongado: La naturaleza de los actores involucrados, con tiempo de permanencia de cientos de días en redes comprometidas, eleva significativamente el riesgo de exfiltración de información sensible y compromiso de infraestructura crítica.

Recomendaciones de mitigación:

1. Actualización inmediata: Migrar de urgencia a la versión Dell RecoverPoint for Virtual Machines 6.0.3.1 HF1 o superior, aplicando los parches indicados en el advisory oficial DSA-2026-079.
2. Revisión de logs del Tomcat Manager: Inspeccionar el archivo /home/kos/auditlog/fapi_cl_audit_log.log en busca de solicitudes al endpoint /manager, especialmente PUT /manager/text/deploy?path=, como indicador temprano de compromiso.
3. Búsqueda de indicadores de persistencia: Verificar el contenido del script /home/kos/kbox/src/installation/distribution/convert_hosts.sh para detectar referencias a ejecutables no legítimos, y analizar los directorios /var/lib/tomcat9 y /var/cache/tomcat9/Catalina en busca de artefactos maliciosos.
4. Monitoreo de infraestructura VMware: Auditar la creación de interfaces de red inusuales en servidores ESXi y revisar la actividad de iptables en appliances vCenter comprometidos como indicadores de pivoteo de red.
5. Caza de amenazas con IOCs publicados: Correlacionar en plataformas SIEM los hashes y el C2 asociado a GRIMBOLT (wss://149.248.11.71/rest/apisession) contra telemetría de red y endpoints en el entorno.

Prioridad: Crítica.

Ampliar información:

- https://www.cybersecuritydive.com/news/zero-day-dell-recoverpoint-virtual-machines-exploited/812392/
- https://feedly.com/cve/CVE-2026-22769
- https://cyberpress.org/dell-zero-day-actively-abused-by-china-linked-threat-actors-to-install-malware/
- https://www.securityweek.com/dell-recoverpoint-zero-day-exploited-by-chinese-cyberespionage-group/
- https://cloud.google.com/blog/topics/threat-intelligence/unc6201-exploiting-dell-recoverpoint-zero-day

GOOGLE CHROME — USE-AFTER-FREE EN MOTOR CSS (CVE-2026-2441)

Google ha publicado una actualización de emergencia para Chrome que corrige CVE-2026-2441, el primer zero-day del año 2026 en el navegador y el de mayor uso a nivel global. El fallo, de alta severidad y con explotación activa confirmada en entornos reales, fue considerado lo suficientemente crítico como para emitir un parche fuera del ciclo de actualizaciones habitual, distribuyéndose directamente al canal Stable antes de la próxima versión mayor.

Resumen técnico:

- Identificador principal: CVE-2026-2441.
- Severidad: 8.8 - (Alta).
- Causa raíz: Vulnerabilidad de tipo use-after-free causada por un bug de invalidación de iteradores en el componente CSSFontFeatureValuesMap, vinculado al manejo de valores de características tipográficas dentro del motor de renderizado CSS (CWE-416).
- Mecanismo de falla: Chrome itera sobre un conjunto de valores de fuentes CSS mientras dicho conjunto es modificado simultáneamente, dejando el puntero del iterador apuntando a memoria ya liberada. Un atacante puede explotar esta condición mediante una página HTML especialmente diseñada para ejecutar código arbitrario dentro del sandbox del navegador, sin necesidad de interacción adicional del usuario más allá de visitar el sitio malicioso.
- Estado de explotación: Explotación activa confirmada in-the-wild. Google ha restringido los detalles técnicos completos del exploit y los indicadores de compromiso mientras se completa el despliegue del parche en la base de usuarios. No se ha publicado información sobre los actores de amenaza involucrados ni los objetivos específicos.
- Versiones afectadas: Google Chrome anteriores a 145.0.7632.75 (Linux) y 145.0.7632.75/76 (Windows y macOS). Los navegadores basados en Chromium — incluyendo Microsoft Edge, Brave y Opera— son igualmente susceptibles y recibirán parches equivalentes.

Impacto potencial:

- Ejecución de código arbitrario en el sandbox: El atacante puede ejecutar código malicioso en el contexto del proceso del navegador afectado, obteniendo capacidad de lectura y modificación de todo el contenido accesible desde esa pestaña, incluyendo credenciales de sesión activas, tokens de autenticación y datos de aplicaciones web.
- Riesgo de escape del sandbox: Si encadenado con una segunda vulnerabilidad de tipo sandbox escape, el atacante puede escalar al sistema operativo subyacente, con capacidad de instalar malware, moverse lateralmente o cifrar archivos.
- Exposición masiva por cuota de mercado: Con más del 60% de cuota de mercado global, Chrome representa uno de los vectores de ataque con mayor superficie de impacto en entornos corporativos y de usuario final.

Recomendaciones de mitigación:

1. Actualización inmediata: Verificar que Chrome esté en la versión 145.0.7632.75 o superior. Para actualizar manualmente, acceder al menú de tres puntos → Configuración → Acerca de Chrome. Aplicar la actualización y reiniciar el navegador para activar la protección. Chrome descarga las actualizaciones en segundo plano, pero requiere reinicio para aplicarlas.
2. Gestión corporativa de parches: En entornos empresariales, forzar la actualización mediante MDM o herramientas de gestión de endpoints y priorizar equipos con mayor exposición a sitios externos o perfiles de riesgo elevado.
3. Revisión de extensiones: Algunas extensiones del navegador pueden bloquear o retrasar el proceso de actualización. Auditar las extensiones instaladas para asegurar que ninguna interfiere con el ciclo de parcheo automático.
4. Vigilancia de comportamiento: En ausencia de IoCs públicos disponibles, monitorear picos anómalos de cierres inesperados del navegador o comportamientos inusuales en procesos de Chrome como señal complementaria de posible explotación.
5. Aplicar la misma acción en navegadores Chromium derivados: Los usuarios de Microsoft Edge, Brave u Opera deben verificar igualmente la disponibilidad de actualizaciones equivalentes para este fallo.

Prioridad: Crítica.

Ampliar información:

- https://www.3djuegos.com/tecnologia/noticias/google-confirma-primer-error-grave-chrome-2026-revela-que-puedes-solucionarlo
- https://www.malwarebytes.com/blog/news/2026/02/update-chrome-now-zero-day-bug-allows-code-execution-via-malicious-webpages
- https://ecosistemastartup.com/cve-2026-2441-vulnerabilidad-zero-day-en-chrome-guia/
- https://unaaldia.hispasec.com/2026/02/google-corrige-un-zero-day-de-chrome-cve-2026-2441-ya-explotado-en-ataques.html
- https://www.infobae.com/tecno/2026/02/18/manten-tu-navegador-al-dia-nueva-actualizacion-de-chrome-para-proteger-tu-informacion/

GRANDSTREAM GXP1600 SERIES — STACK BUFFER OVERFLOW NO AUTENTICADO EN API WEB (CVE-2026-2329)

Rapid7 Labs ha revelado una vulnerabilidad crítica de tipo zero-day en toda la serie de teléfonos VoIP Grandstream GXP1600, dispositivos ampliamente desplegados en pequeñas y medianas empresas, hoteles, call centers y organizaciones con presencia en más de 150 países. El fallo permite a un atacante remoto no autenticado ejecutar código arbitrario con privilegios de root sobre el dispositivo afectado, sin necesidad de credenciales ni interacción del usuario, comprometiendo tanto las comunicaciones de voz como la infraestructura de red en la que opera el teléfono.

Resumen técnico:

- Identificador principal: CVE-2026-2329.
- Severidad: 9.3 (Crítica) en la escala CVSSv4.
- Causa raíz: Stack-based buffer overflow (CWE-121) en el binario nativo gs_web (ARM 32 bits), que implementa el servicio web de administración y la API del dispositivo.
- Mecanismo de falla: El endpoint /cgi-bin/api.values.get, accesible sin autenticación en la configuración por defecto del dispositivo, acepta un parámetro HTTP POST llamado request con una cadena delimitada por dos puntos. La función de parseo itera carácter a carácter y copia cada identificador en un buffer de 64 bytes en la pila sin realizar ninguna verificación de longitud. Un atacante puede enviar un parámetro request con un identificador de longitud superior a 63 bytes para desbordar el buffer, corromper el stack frame adyacente y obtener control sobre el Program Counter (PC) cuando la función vulnerable retorna, logrando así ejecución de código arbitrario con privilegios de root.
- Estado de explotación: No se ha reportado explotación activa en entornos reales hasta la fecha de divulgación, pero Rapid7 ha desarrollado y publicado un módulo exploit funcional para Metasploit junto con un módulo de post-explotación para extracción de credenciales, lo que reduce significativamente la barrera de entrada para actores de amenaza.
- Versiones afectadas: Todos los modelos de la serie GXP1600 con firmware anterior a 1.0.7.81: GXP1610, GXP1615, GXP1620, GXP1625, GXP1628 y GXP1630 (todos comparten una imagen de firmware común).

Impacto potencial:

- Ejecución remota de código con root (RCE): El atacante obtiene control completo del sistema operativo del dispositivo sin necesidad de autenticación, con capacidad de ejecutar comandos arbitrarios de forma remota.
- Exfiltración de credenciales: Un módulo de post-explotación desarrollado por Rapid7 permite extraer credenciales de usuarios locales y cuentas SIP, incluyendo contraseñas en texto plano almacenadas en el dispositivo comprometido.
- Intercepción de llamadas VoIP: La RCE puede ser aprovechada para reconfigurar el teléfono y redirigir todo el tráfico SIP a través de un proxy controlado por el atacante, permitiendo la escucha pasiva y manipulación de llamadas activas.
- Pivoteo de red y movimiento lateral: En entornos con segmentación de red deficiente —habitual en pymes con redes planas donde teléfonos y equipos comparten VLAN— un teléfono comprometido puede convertirse en un punto de entrada para el movimiento lateral, escaneo interno de la red o como nodo de comando y control (C2).
- Superficie de ataque desatendida: Los teléfonos VoIP suelen operar fuera de los programas formales de gestión de endpoints, sin agentes EDR, sin monitoreo de logs y con ciclos de parcheo lentos, lo que prolonga significativamente el tiempo de exposición ante una vulnerabilidad de esta naturaleza.

Recomendaciones de mitigación:

1. Actualización inmediata de firmware: Migrar todos los dispositivos GXP1600 a la versión de firmware 1.0.7.81 o superior, disponible en la página oficial de descargas de Grandstream y detallada en la página PSIRT del fabricante.
2. Restricción de acceso a la interfaz web: Limitar el acceso al puerto TCP 80 del dispositivo exclusivamente a subredes de gestión de confianza, mediante reglas de firewall o listas de control de acceso (ACLs), reduciendo la superficie de ataque expuesta.
3. Segmentación de la infraestructura VoIP: Aislar los teléfonos VoIP en una VLAN dedicada, separada de segmentos de usuarios generales y redes no confiables, para contener el impacto potencial de un dispositivo comprometido.
4. Monitoreo de intentos de explotación: Revisar los logs de red en busca de solicitudes HTTP POST inusuales dirigidas al endpoint /cgi-bin/api.values.get con valores del

parámetro request de longitud anómala, como indicador de posibles intentos de explotación.

5. Rotación preventiva de credenciales: Tras la aplicación del parche, rotar todas las contraseñas de cuentas locales y credenciales de cuentas SIP almacenadas en los dispositivos GXP1600 como medida de precaución ante posibles compromisos previos no detectados.

Prioridad: Crítica.

Ampliar información:

- https://darkwebinformer.com/critical-rce-vulnerability-in-grandstream-gxp1600-voip-phones-allows-root-access-without-authentication/
- https://www.darkreading.com/threat-intelligence/grandstream-bug-voip-security-blind-spot
- https://thehackernews.com/2026/02/grandstream-gxp1600-voip-phones-exposed.html
- https://www.rapid7.com/blog/post/ve-cve-2026-2329-critical-unauthenticated-stack-buffer-overflow-in-grandstream-gxp1600-voip-phones-fixed/

MALWARE

MALWARE — KEENADU: BACKDOOR PREINSTALADO EN FIRMWARE ANDROID VÍA ACTUALIZACIONES OTA FIRMADAS

Kaspersky ha documentado Keenadu, una plataforma de backdoor descubierta embebida en el firmware de dispositivos Android de múltiples fabricantes, incluyendo Alldocube. El malware no requiere ninguna acción del usuario: se introduce durante la compilación del firmware como una dependencia maliciosa vinculada a la biblioteca crítica del sistema libandroid_runtime.so, garantizando su ejecución en cada arranque y su inyección en todas las aplicaciones activas. En varios casos documentados, el firmware comprometido fue distribuido mediante actualizaciones OTA con firmas digitales válidas, apuntando a un compromiso temprano de la cadena de suministro.

Resumen técnico:

- Familia de malware: Keenadu (HEUR:Backdoor.AndroidOS.Keenadu.* y variantes).
- Primer hallazgo: Tableta Alldocube iPlay 50 mini Pro, firmware del 18 de agosto de 2023. Todos los firmwares posteriores del mismo modelo resultaron igualmente infectados.
- Vector primario: Ataque a la cadena de suministro. La biblioteca maliciosa libVndxUtils.a fue introducida en el repositorio de código fuente del firmware, vinculándose durante la compilación con libandroid_runtime.so.
- Vectores adicionales: Integración en aplicaciones del sistema (reconocimiento facial, launcher); instalación por el backdoor BADBOX; y distribución mediante apps troyanizadas en Google Play (apps de cámaras IP con más de 300.000 descargas, ya retiradas).
- Arquitectura cliente-servidor: AKServer opera en el proceso system_server con privilegios máximos gestionando el C2, mientras AKClient se inyecta en todas las aplicaciones activas como proxy mediante el mecanismo IPC nativo de Android (binder).
- Evasión: Aborta si detecta entorno chino (idioma o zona horaria), ausencia de Google Play Services, o aplicaciones de sistema de Google o carriers. El C2 no entrega cargas útiles hasta 2,5 meses después del primer registro del dispositivo.
- Alcance: 13.715 usuarios detectados globalmente. Principales países afectados: Rusia, Japón, Alemania, Brasil y Países Bajos. España figura entre los diez con mayor número de detecciones.

Impacto potencial:

- Nulificación del sandboxing de Android: Al inyectarse en el proceso Zygote, accede a los datos de cualquier aplicación instalada, haciendo ineficaz el modelo de aislamiento del sistema operativo.
- Control ilimitado del dispositivo: Puede conceder o revocar permisos arbitrarios, instalar APKs sin consentimiento, obtener geolocalización y exfiltrar archivos multimedia, mensajes, credenciales bancarias y búsquedas en Chrome incluso en modo incógnito.
- Fraude publicitario activo: Módulos identificados que secuestran el motor de búsqueda en Chrome, interactúan con elementos publicitarios y monetizan instalaciones de aplicaciones engañando a plataformas de anuncios.
- Persistencia extrema: Al estar embebido en la partición de sistema (montada en modo solo lectura), no puede eliminarse sin reemplazar el firmware completo del dispositivo.

Recomendaciones de mitigación:

1. Verificar actualizaciones de firmware limpias del fabricante y, tras instalarlas, analizar el dispositivo con una solución de seguridad para confirmar la eliminación de la amenaza.
2. Activar y mantener actualizado Google Play Protect en todos los dispositivos Android del entorno.
3. Si el firmware sigue infectado, evitar el uso del dispositivo para operaciones sensibles (credenciales, banca, comunicaciones corporativas) hasta su reemplazo o actualización.
4. Si se detecta el cargador en una aplicación del sistema, desactivarla mediante ADB: adb shell pm disable --user 0 %PACKAGE% y reemplazarla por una alternativa limpia si existe.
5. Para organizaciones que adquieren dispositivos Android en volumen, implementar verificación de integridad del firmware antes del despliegue.

Prioridad: Urgente.

Ampliar información:

- https://www.infobae.com/america/agencias/2026/02/17/alertan-sobre-keenadu-el-malware-preinstalado-en-algunos-nuevos-dispositivos-android-para-fraude-publicitario/
- https://thehackernews.com/2026/02/keenadu-firmware-backdoor-infects.html
- https://securelist.lat/keenadu-android-backdoor/100771/
- https://applicantes.com/keenadu-malware-android/
- https://www.news4hackers.com/android-tablet-security-threat-keenadu-firmware-backdoor-via-signed-ota-updates/

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

INVESTIGADORES DEMUESTRAN QUE MICROSOFT COPILOT Y GROK PUEDEN USARSE COMO PROXY C2

Investigadores de Check Point Research han demostrado mediante una prueba de concepto (PoC) cómo asistentes de inteligencia artificial con capacidades de navegación web —concretamente Microsoft Copilot y Grok de xAI— pueden ser abusados como canales encubiertos de comando y control (C2). La técnica, denominada AI as a C2 Proxy, permite a un atacante enrutar comunicaciones maliciosas a través de estas plataformas, camuflándolas como tráfico legítimo hacia dominios de alta reputación y eludiendo los controles de seguridad corporativos tradicionales.

Resumen técnico:

- Técnica: Abuso de las capacidades de búsqueda y recuperación de URLs de asistentes de IA para establecer un canal C2 bidireccional. El malware en el endpoint comprometido instruye al agente de IA para que visite una URL controlada por el atacante, recupere su contenido y devuelva la respuesta —que contiene el comando a ejecutar— al propio malware.
- Plataformas afectadas: Microsoft Copilot y Grok (xAI), ambas accesibles sin necesidad de cuenta registrada ni clave API, lo que anula medidas de bloqueo tradicionales como la revocación de claves o la suspensión de cuentas.
- Implementación técnica: Los investigadores desarrollaron un implante en C++ utilizando el componente WebView2 (preinstalado en Windows 11 y ampliamente distribuido en Windows 10) para interactuar de forma invisible con la interfaz web de las plataformas de IA. El malware recopila información del sistema, la codifica en los parámetros de la URL de un sitio C2 controlado por el atacante y solicita al agente de IA que "resuma" dicha página. Los comandos del operador se incrustan en el HTML del sitio y son retornados al implante a través de la respuesta del modelo.
- Estado: Prueba de concepto publicada. Los hallazgos fueron comunicados de forma responsable a los equipos de seguridad de Microsoft y xAI. No se ha confirmado explotación activa en entornos reales.
- Prerrequisito: El atacante debe haber comprometido previamente el sistema por otros medios e instalado el implante inicial.

Impacto potencial:

- Evasión de controles perimetrales: El tráfico C2 fluye cifrado (HTTPS) hacia dominios de confianza como microsoft.com o x.ai, ampliamente autorizados en entornos corporativos y raramente inspeccionados por soluciones de seguridad.
- Canal C2 sin credenciales: Al no requerir API key ni cuenta registrada, las contramedidas tradicionales de bloqueo resultan ineficaces, convirtiendo esta técnica en una variante especialmente resiliente de los ataques Living-Off-Trusted-Sites (LOTS).
- Evolución hacia malware impulsado por IA: Check Point advierte que esta misma arquitectura puede evolucionar hacia implantes que deleguen decisiones operativas en el modelo de IA en tiempo real: selección de objetivos, evasión de sandboxes, priorización de archivos para cifrado o exfiltración, y adaptación táctica autónoma durante una intrusión

Recomendaciones para mitigar el riesgo:

1. Monitoreo del tráfico hacia plataformas de IA: Tratar los dominios de IA como puntos de egreso de alto valor, implementando inspección y registro del tráfico saliente hacia servicios como Copilot o Grok, con especial atención a patrones automatizados, frecuencia inusual o procesos no humanos como origen de las comunicaciones.
2. Políticas de uso de IA corporativa: Restringir el acceso a herramientas de IA externas a usuarios y sistemas con necesidad justificada, limitando la exposición de endpoints críticos a estas plataformas.
3. Actualización de reglas de detección: Incorporar en SIEM y soluciones EDR reglas específicas para identificar comunicaciones periódicas automatizadas hacia APIs o interfaces web de IA originadas desde procesos inusuales o no interactivos.
4. Integración en playbooks de respuesta: Incluir el análisis del tráfico hacia servicios de IA en los procedimientos de hunting e investigación de incidentes, especialmente en entornos que han desplegado Copilot de forma generalizada.

Prioridad: Urgente.

Ampliar Información:

- https://www.betterworldtechnology.com/post/ai-assistants-like-copilot-and-grok-abused-as-covert-malware-command-channels
- https://www.infosecurity-magazine.com/news/ai-assistants-covert-c2-relays/
- https://research.checkpoint.com/2026/ai-in-the-middle-turning-web-based-ai-services-into-c2-proxies-the-future-of-ai-driven-attacks/
- https://thehackernews.com/2026/02/researchers-show-copilot-and-grok-can.html
- https://www.ciberplaneta.org/articles/780/