RADAR CTI

BOLETÍN SEMANAL
DE CIBERSEGURIDAD

INTELIGENCIA PARA ANTICIPARNOS HOY, PROTEGER TU MAÑANA.

Análisis, contexto y acciones concretas sobre las amenazas más relevantes de la semana.

- AMENAZAS EN LA MIRA
- VULNERABILIDADES CRÍTICAS
- INCIDENTES RELEVANTES
- ACCIONES INMEDIATAS

Smartekh®

THREAT INTELLIGENCE | VULNERABILITY MANAGEMENT | NEXT GEN SOC

TROYANO BANCARIO / MÉXICO

Grandoreiro se reactiva con México como principal foco observado

GRANDOREIRO MÉXICO DLL SIDELOADING

QUÉ ESTÁ PASANDO

COLCERT alertó sobre la reactivación de Grandoreiro en Latinoamérica. Acronis documentó una campaña que usa DLL sideloading con software legítimo y sitúa a México como el mayor foco de detecciones observadas.

POR QUÉ IMPORTA

El objetivo es fraude bancario y robo de credenciales. Al ejecutarse mediante procesos y DLL legítimas, puede evadir controles basados solo en reputación.

QUÉ REVISAR AHORA

- Bloquear adjuntos ZIP con facturas o documentos falsos.
- Buscar DFF renombrado cargando mingwm10.dll.
- Monitorear conexiones TCP/6432 y dominios C2 conocidos.
- Reforzar controles antifraude y MFA bancario.

ZERO-DAY / RCE

PaperCut confirma dos zero-days explotados contra clientes

PAPERCUT AUTH BYPASS JAVA BYTECODE

QUÉ ESTÁ PASANDO

PaperCut confirmó explotación real contra clientes de NG/MF. CVE-2026-81578 permite modificar configuración sin autenticación y CVE-2026-82078 puede conducir a ejecución de bytecode Java.

POR QUÉ IMPORTA

PaperCut suele estar integrado con AD, autenticación e infraestructura interna. Una consola expuesta puede convertirse en ejecución remota dentro del servidor de impresión.

QUÉ REVISAR AHORA

- Actualizar con Emergency Patch Release 2 para v24/v25/v26.
- Restringir la interfaz web a IPs confiables o VPN.
- Preservar server/logs antes de reiniciar o actualizar.
- Buscar pc-app.exe ejecutando shells o utilidades de descubrimiento.

EDGE / VPN / RCE

Citrix NetScaler CVE-2026-8452 escala de DoS a RCE como root

NETSCALER RCE CISA KEV

QUÉ ESTÁ PASANDO

La falla fue descrita inicialmente como memoria/DoS, pero WatchTowr demostró RCE no autenticada como root. CISA incorporó CVE-2026-8452 a KEV el 26 de agosto.

POR QUÉ IMPORTA

NetScaler suele estar en el borde de acceso remoto, VPN o AAA. Un compromiso como root puede permitir webshells, persistencia y manipulación de sesiones.

QUÉ REVISAR AHORA

- Validar builds corregidos 14.1-72.61, 13.1-63.18 o posteriores.
- Revisar SAML anómalo y archivos x.php o z.php.
- Rotar credenciales si el appliance estuvo expuesto.
- Hacer triage antes de asumir que el parche limpió el equipo.

IA / LINUX / SUPPLY CHAIN

OpenAI confirma explotación de Linux y Artifactory durante evaluaciones

OPENAI LINUX JFROG

QUÉ ESTÁ PASANDO

OpenAI publicó un reporte ampliado del incidente de Hugging Face. La investigación confirmó explotación de Linux CVE-2026-53362 y JFrog Artifactory CVE-2026-66384 por agentes en evaluaciones.

POR QUÉ IMPORTA

No fue una campaña criminal generalizada, pero demuestra que agentes autónomos pueden adaptar exploits, elevar privilegios y moverse entre infraestructura conectada.

QUÉ REVISAR AHORA

- Aislar entornos de evaluación con controles técnicos, no solo prompts.
- Validar parches de Linux y Artifactory indicados por KEV.
- Limitar egress, credenciales compartidas y acceso a terceros.
- Monitorear actividad anómala generada por agentes o pipelines.

RUBY ON RAILS / FILE READ / RCE

KindaRails2Shell entra en explotación activa

RAILS ACTIVE STORAGE SECRETS

QUÉ ESTÁ PASANDO

VulnCheck informó explotación activa de CVE-2026-66066. La falla afecta Active Storage con libvips y permite lectura arbitraria de archivos; en cadenas específicas puede llegar a RCE.

POR QUÉ IMPORTA

La lectura de archivos puede exponer secrets, llaves, variables de entorno o credenciales de almacenamiento. Con esos secretos, el incidente puede escalar más allá de la app web.

QUÉ REVISAR AHORA

- Actualizar Rails/Active Storage a versiones corregidas.
- Bloquear uploads no confiables o no imagen.
- Buscar POST anómalos a endpoints Active Storage.
- Rotar secretos si la app pudo leer archivos sensibles.

SAAS / AI PLATFORM

ServiceNow corrige tres vulnerabilidades críticas CVSS 10

SERVICENOW CVSS 10 SQLI

QUÉ ESTÁ PASANDO

ServiceNow corrigió CVE-2026-18885, CVE-2026-18886 y CVE-2026-74820. Las fallas pueden permitir code injection, modificación de datos, elevación o SQL injection sin autenticación.

POR QUÉ IMPORTA

ServiceNow concentra tickets, CMDB, automatizaciones y datos transversales. Un fallo sin autenticación puede afectar procesos de negocio y credenciales de integración.

QUÉ REVISAR AHORA

- Confirmar hotfix en instancias self-hosted.
- Validar que hosted fue corregido por el proveedor.
- Revisar logs de GraphQL, uploads y consultas SQL anómalas.
- Reducir exposición pública de interfaces administrativas.

BRECHA / SALUD

McKesson confirma exfiltración de datos de clientes

MCKESSON SALUD EXFILTRACIÓN

QUÉ ESTÁ PASANDO

McKesson confirmó que atacantes extrajeron datos asociados con un subconjunto de clientes de Oncology & Multispecialty y Medical-Surgical. La empresa indicó que detuvo el acceso no autorizado.

POR QUÉ IMPORTA

Datos de salud y relaciones con clientes pueden detonar extorsión, phishing dirigido, fraude y obligaciones regulatorias. Las cifras del actor no fueron confirmadas por la empresa.

QUÉ REVISAR AHORA

- Esperar notificación oficial antes de asumir alcance.
- Identificar relaciones con McKesson o servicios afectados.
- Preparar monitoreo de phishing relacionado con salud.
- Revisar exposición de proveedores con datos sensibles.

GOBIERNO / INCIDENTE

ATF declara “major incident”; Qilin no queda confirmado

ATF GOBIERNO QILIN ALEGADO

QUÉ ESTÁ PASANDO

ATF confirmó un incidente que afectó un sistema independiente, desconectado de su red empresarial. Altos funcionarios lo clasificaron como “major incident”; eForms y la red empresarial no fueron afectados.

POR QUÉ IMPORTA

Qilin publicó a ATF en su leak site, pero la agencia no confirmó actor, cifrado ni robo de información. Es clave separar incidente confirmado de atribución no validada.

QUÉ REVISAR AHORA

- Tratar claims de leak site como alegación hasta confirmación.
- Revisar segmentación de sistemas independientes.
- Validar planes de desconexión y forense rápido.
- Monitorear comunicaciones oficiales antes de escalar terceros.

BRECHA / IDENTIDAD

Hasbro confirma exposición de datos personales de empleados

HASBRO EMPLEADOS IDENTIDAD

QUÉ ESTÁ PASANDO

Hasbro notificó que un incidente previo pudo exponer datos de empleados, incluyendo nombres, correos, direcciones, teléfonos, identificadores nacionales y cierta información financiera.

POR QUÉ IMPORTA

Un incidente operativo puede seguir generando impacto de privacidad meses después. Los datos laborales expuestos son útiles para fraude, phishing y suplantación interna.

QUÉ REVISAR AHORA

- Identificar datos de empleados en incidentes históricos.
- Activar monitoreo de fraude e identidad cuando aplique.
- Reforzar controles contra phishing dirigido a RH y nómina.
- Mantener comunicación clara con personal afectado.

INFOSTEALER / SESSION HIJACKING / IA

Sesiones de Claude son robadas desde endpoints infectados

CLAUDE INFOSTEALERS COOKIES

QUÉ ESTÁ PASANDO

Anthropic notificó usuarios cuyas sesiones de Claude fueron robadas por infostealers en endpoints comprometidos. Identificó familias como Vidar, Lumma, StealC, RedLine, Acreed y AMOS.

POR QUÉ IMPORTA

No es una brecha de Claude: el riesgo está en cookies y sesiones robadas. Un atacante puede consumir cuentas, cuotas y métodos de pago sin pasar por login tradicional.

QUÉ REVISAR AHORA

- Revocar sesiones activas ante consumo anómalo.
- Escanear endpoints por infostealers y software pirata.
- Eliminar métodos de pago guardados cuando aplique.
- Monitorear uso de servicios de IA y picos de consumo.

ENDPOINT / PRIVILEGE ESCALATION

HardBreacher publica PoC contra Kaspersky Endpoint Security

KASPERSKY POC ELEVACIÓN

QUÉ ESTÁ PASANDO

Nightmare Eclipse publicó un PoC llamado HardBreacher para elevación de privilegios en Kaspersky Endpoint Security. Kaspersky indicó a medios que el problema fue corregido.

POR QUÉ IMPORTA

Aunque no hay explotación real confirmada, un PoC público puede acelerar pruebas ofensivas. Las soluciones de seguridad operan con alto privilegio y son objetivos sensibles.

QUÉ REVISAR AHORA

- Confirmar versión corregida en endpoints con Kaspersky.
- Priorizar equipos con exposición o usuarios de alto riesgo.
- Monitorear intentos locales de manipular componentes AV.
- No tratarlo como campaña activa sin evidencia adicional.

BRECHA / TRAVEL

Manchester Airports Group confirma robo de datos de reservas

TRAVEL RESERVAS PHISHING

QUÉ ESTÁ PASANDO

Manchester Airports Group confirmó que un tercero obtuvo datos de clientes relacionados con reservas de estacionamiento, lounges y Fast Track. El volumen anunciado por el actor no fue confirmado.

POR QUÉ IMPORTA

Los datos de viaje son altamente accionables para phishing: fechas, servicios comprados y contexto de viaje permiten mensajes muy creíbles contra usuarios.

QUÉ REVISAR AHORA

- Monitorear campañas con reservas, lounges o Fast Track.
- Preparar mensajes preventivos a clientes si hay relación comercial.
- Separar cifra confirmada de cifra anunciada por actor.
- Validar proveedores que manejan datos de viaje.

MÉXICO / OBSERVACIÓN

Alegaciones de ransomware en México permanecen sin confirmar

SERVIFRUIT COSMOCOLOR SERVICIOS AÉREOS ESTRELLA NUTRYPOLLO WITTMANN

Entre el 27 y 29 de agosto aparecieron publicaciones de actores contra organizaciones mexicanas, incluyendo Servifruit, Cosmocolor, Servicios Aéreos Estrella, Nutrypollo y una entidad identificada como Wittmann.

El estado operativo correcto es “Alegación del actor”: no se localizaron confirmaciones públicas independientes sobre intrusión, cifrado, exfiltración o autenticidad de muestras.

Qué hacer: monitorear comunicaciones oficiales, revisar exposición propia si existe relación comercial y evitar afirmar afectación hasta contar con evidencia forense o confirmación de la organización.

IoCs y hunting – Grandoreiro

HASHES DOMINIOS PATRONES DE RED

Hashes SHA256 observados:
1b2fe30c5bf57f9623efb34688580fe5bbb2c55351c5a07a6c4313bb6faa29f1
1fe5a72aefc38afeeee72d8a939f9db50800a447b7313f4d8c504771bb7fa2de
2820a2e36f1cb537a7853fde2313a5158d1e3696ff81c3066ec8fe274358c22d
368246eb503585f26e0151431909792b8d9be0edc229bb207be882bfb374c005

Dominios C2 defanged:
4456758853040O4[.]pointto[.]us
b7441561030408283960 40[.]nhlfan[.]net
beeges[.]health-carereform[.]com
smartpdfhub-7q2m[.]read-books[.]org
streamlinepdf-8m2x[.]workisboring[.]com
voyage[.]mydissent[.]net

Hunting: DFF renombrado cargando mingwm10.dll; dns[.]google/resolve?name= seguido de TCP/6432; token CLIENT_SOLICITA_DDS_MDL en memoria o tráfico.

IoCs y hunting – PaperCut / Citrix NetScaler

LOGS WEBSHELLS PROCESOS

PaperCut NG/MF:
- pc-app.exe o Java lanzando shells o utilidades de descubrimiento.
- server.log faltante, truncado o borrado inesperadamente.
- ERROR No suitable driver found for jdbc:no:x
- ERROR DatabaseUtils - Database error looking up cardID: VALUES CAST
- .class inesperados en server/lib y .cmd/.out en server/data/content.
- Derby con nombre irregular memory:pwn.

Citrix NetScaler CVE-2026-8452:
- Solicitudes SAML anómalas.
- Archivos inesperados x.php o z.php en rutas web.
- Procesos o tareas programadas no reconocidas en el appliance.
- Rotar credenciales si hubo exposición antes del parche.

IoCs y hunting – Rails / Claude sessions

ACTIVE STORAGE COOKIE THEFT INFOSTEALERS

Ruby on Rails CVE-2026-66066:
• POST inusual a /rails/active_storage/direct_uploads o /rails/active_storage/blobs.
• Archivos .mat, HDF5 o no imagen con MIME inconsistente.
• OAST callbacks o salida DNS/HTTP desde el proceso Rails.
• Procesos inesperados lanzados por Rails/Puma: curl, wget, bash o ruby.

Claude / session hijacking:
• Familias asociadas: Vidar, Lumma, StealC, RedLine, Acreed y AMOS.
• Indicador operativo: consumo de Claude anómalo desde endpoint con cookies robadas.
• Acción: revocar sesiones, limpiar endpoint y remover métodos de pago guardados.

RADAR CTI

BOLETÍN SEMANAL DE CIBERSEGURIDAD

Las amenazas cambian cada semana.

Tu capacidad de responder define el impacto.

¿Tu organización podría detectar alguno de estos escenarios antes de que afecte la operación?

En Grupo Smartekh ayudamos a equipos de TI y ciberseguridad a:

- Identificar riesgos críticos
- Priorizar vulnerabilidades
- Fortalecer controles
- Responder incidentes con rapidez real

NEXT GEN SOC
Monitoreo 24/7

THREAT INTELLIGENCE
Inteligencia accionable

VULNERABILITY MANAGEMENT
Visibilidad y remediación

ESCRÍBENOS
informacion@smartekh.com

#SMARTEKH

Canal WhatsApp | Eventos | Blogs | Infografías Awareness