RADAR CTI

BOLETÍN SEMANAL
DE CIBERSEGURIDAD

INTELIGENCIA PARA ANTICIPARNOS HOY, PROTEGER TU MAÑANA.

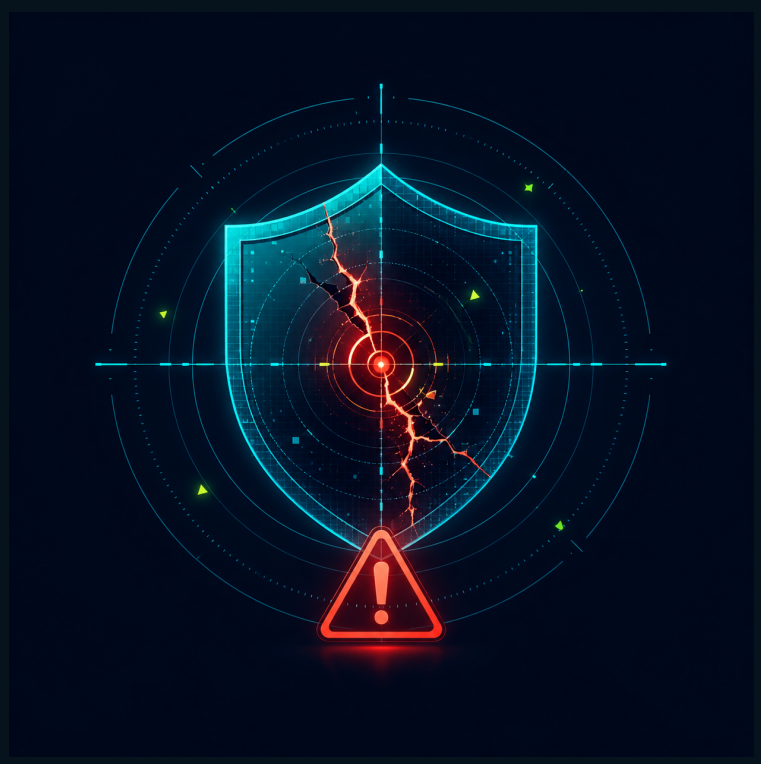
Análisis, contexto y acciones concretas sobre las amenazas más relevantes de la semana.

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

Grupo Smartekh

THREAT INTELLIGENCE | VULNERABILITY MANAGEMENT | NEXT GEN SOC

VULNERABILIDADES CRÍTICAS



SPLUNK | KEV | RCE

Splunk Enterprise: explotación limitada y cadena hacia RCE

Splunk actualizó su aviso el 18 de junio tras observar explotación limitada de CVE-2026-20253. El punto delicado está en el endpoint del PostgreSQL Sidecar: un atacante no autenticado puede crear o truncar archivos, y la investigación técnica mostró que el abuso puede escalar hasta ejecución de código.

Impacto: En muchas empresas Splunk concentra telemetría sensible, credenciales de integración y visibilidad del SOC. Si el servidor está expuesto o mal segmentado, el impacto no se queda en el log: puede abrir una ruta para manipular archivos, ejecutar código y borrar huellas.

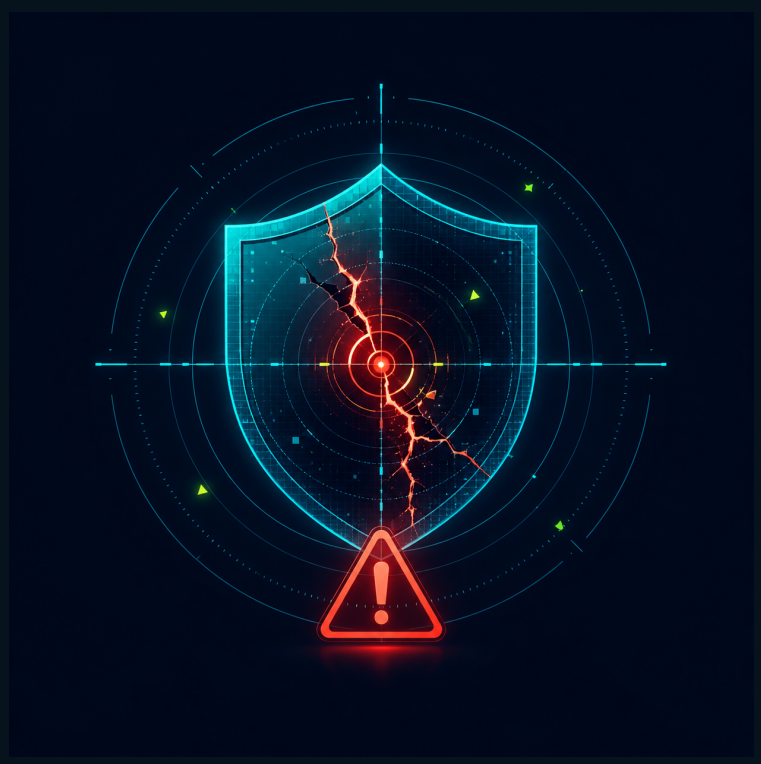
Qué hacer ahora

- Actualizar Splunk Enterprise a la versión corregida por el fabricante para CVE-2026-20253.
- Limitar exposición de Splunk y del sidecar PostgreSQL a redes confiables.
- Buscar archivos creados/truncados, procesos anómalos y actividad inusual del usuario de Splunk.

URL oficial: splunk.com / cisa.gov / watchtowr.com

Fuentes: Splunk, CISA KEV, watchTowr

VULNERABILIDADES CRÍTICAS



JOOMLA | JCE | WEBSHELL

Joomla JCE: CVSS 10 usado para subir webshells

CISA agregó CVE-2026-48907 al catálogo KEV. La falla afecta Joomla Content Editor y permite que un atacante no autenticado cree perfiles de editor que habilitan carga y ejecución de PHP. Ya se reportó abuso automatizado para dejar webshells en sitios expuestos.

Impacto: Es una falla de bajo ruido y alto impacto: el atacante no necesita una cuenta válida y puede convertir un sitio Joomla en punto de persistencia, phishing, distribución de malware o pivote hacia otros servicios del mismo hosting.

Qué hacer ahora

- Actualizar Joomla Content Editor a 2.9.99.5 o superior.
- Buscar perfiles de editor creados recientemente, tareas de importación raras y archivos PHP nuevos.
- Revisar webshells, cambios de permisos y conexiones salientes desde el servidor web.

URL oficial: cisa.gov / joomlacontenteditor.net

Fuentes: CISA KEV, JCE, medios especializados

VULNERABILIDADES CRÍTICAS

FORTINET | SANDBOX | RCE

FortiSandbox: reportan explotación de fallas críticas

Investigadores reportaron explotación de CVE-2026-39813, CVE-2026-39808 y CVE-2026-25089 en FortiSandbox. La cadena mezcla path traversal y command injection mediante solicitudes HTTP. Al cierre, Fortinet aún no confirmaba explotación pública como nueva campaña oficial.

Impacto: FortiSandbox suele recibir archivos sospechosos y conectar con otros controles Fortinet. Si el appliance cae, el atacante puede usarlo como punto de ejecución, robo de artefactos, movimiento lateral o salida hacia internet bajo apariencia legítima.

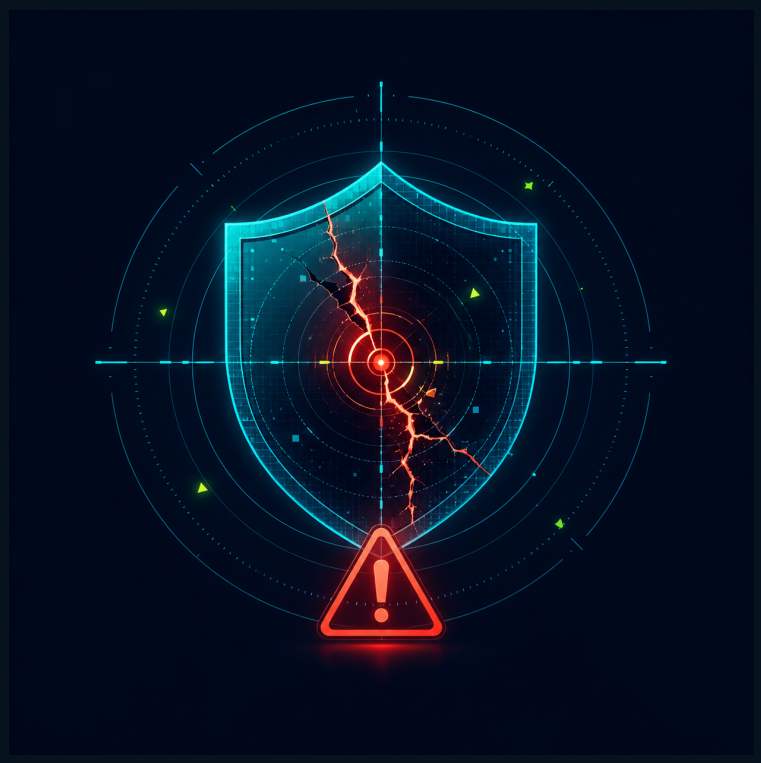
Qué hacer ahora

- Aplicar los builds corregidos de FortiSandbox publicados para esas CVE.
- Aislar la administración del appliance y revisar accesos HTTP fuera de horario.
- Buscar comandos ejecutados, artefactos subidos, conexiones salientes y credenciales reutilizadas.

URL oficial: fortinet.com / advisories

Fuentes: Fortinet PSIRT, reportes técnicos de explotación

VULNERABILIDADES ALTAS



CISCO | SD-WAN | KEV

Cisco SD-WAN Manager: escritura arbitraria con riesgo root

Cisco reconoció explotación de CVE-2026-20262 en Catalyst SD-WAN Manager. La falla requiere credenciales con permisos de escritura, pero permite modificar archivos y puede terminar en elevación a root. CISA la añadió a KEV por explotación observada.

Impacto: Aunque no es pre-auth, en SD-WAN una cuenta privilegiada comprometida tiene mucho valor. Un cambio malicioso puede propagarse hacia routers edge, alterar rutas o dejar persistencia en la administración de red.

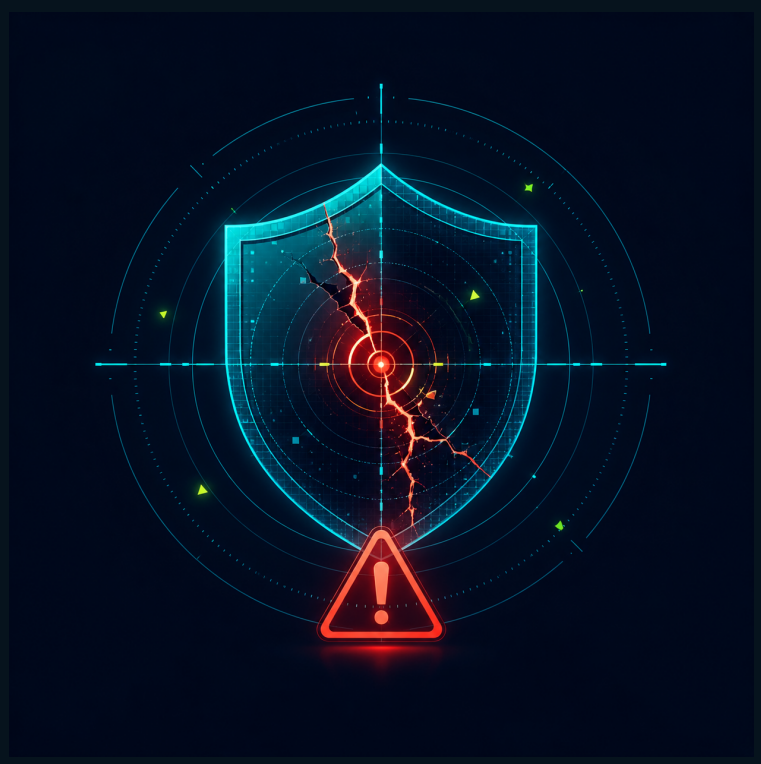
Qué hacer ahora

- Actualizar Cisco Catalyst SD-WAN Manager a la versión corregida indicada por Cisco para CVE-2026-20262.
- Revisar cuentas netadmin, cambios de configuración y pushes recientes hacia routers edge.
- Comparar backups de configuración y buscar archivos modificados fuera del flujo normal.

URL oficial: cisco.com / cisa.gov

Fuentes: Cisco, CISA KEV

VULNERABILIDADES ALTAS



MICROSOFT | POC | LPE

Microsoft Defender: RoguePlanet eleva privilegios a SYSTEM

Durante la semana se publicó PoC para CVE-2026-50656, una condición de carrera en Microsoft Defender conocida como RoguePlanet. El escenario requiere acceso local previo, pero permite subir privilegios a SYSTEM en endpoints vulnerables.

Impacto: No es la puerta de entrada inicial, pero sí puede ser el paso que convierte una intrusión menor en control total del equipo. Es especialmente relevante para estaciones de administración, servidores con EDR y equipos donde el atacante ya logró ejecutar código.

Qué hacer ahora

- Aplicar actualizaciones de Defender y Microsoft Malware Protection Engine en cuanto estén disponibles.
- Monitorear explotación local post-compromiso, cambios de servicios y ejecución anómala con SYSTEM.
- Priorizar equipos de administradores, servidores críticos y endpoints con señales previas de intrusión.

URL oficial: msrc.microsoft.com / microsoft.com

Fuentes: Microsoft, PoC público, medios especializados

VULNERABILIDADES CRÍTICAS

NGINX | EDGE WEB

F5 NGINX: parches fuera de ciclo para fallas críticas

F5 publicó parches fuera de ciclo para CVE-2026-42530 y CVE-2026-42055 en NGINX. Las fallas pueden provocar reinicio remoto no autenticado y, bajo condiciones específicas como bypass o falta de ASLR, abrir una ruta hacia ejecución de código.

Impacto: NGINX vive al borde de la red: reverse proxies, WAF, ingress controllers y gateways Kubernetes. Una falla ahí puede afectar disponibilidad, exposición de aplicaciones internas o el primer punto que toca el tráfico de clientes.

Qué hacer ahora

- Actualizar NGINX Plus, NGINX OSS o Gateway Fabric a los builds corregidos publicados por F5.
- Priorizar reverse proxies expuestos, ingress controllers y gateways Kubernetes.
- Validar ASLR, reglas WAF, reinicios inesperados y solicitudes anómalas contra endpoints edge.

URL oficial: f5.com / nginx.org

Fuentes: F5, NGINX, medios especializados

VULNERABILIDADES CRÍTICAS

CISCO | ISE | IAM

Cisco ISE: fallas críticas en plataforma de identidad

Cisco corrigió CVE-2026-20181 y CVE-2026-20190 en ISE / ISE-PIC. La principal permite ejecución de código y escalamiento a root a un atacante remoto autenticado con privilegios administrativos; otra permite divulgación de información sin autenticación.

Impacto: ISE no es un servidor cualquiera: toma decisiones de acceso, segmentación y postura. Si un administrador es comprometido o se expone información sensible, el impacto puede tocar VPN, NAC, redes corporativas y acceso de terceros.

Qué hacer ahora

- Actualizar Cisco ISE / ISE-PIC a las versiones corregidas por Cisco para esas CVE.
- Auditar cuentas admin, sesiones API, exportaciones, backups y cambios de configuración.
- Restringir exposición del portal administrativo y separar accesos de operadores y terceros.

URL oficial: cisco.com/security/advisories

Fuentes: Cisco Security Advisories

VULNERABILIDADES ALTAS

MULTIMEDIA | SUPPLY CHAIN

FFmpeg PixelSmash: RCE desde archivos multimedia

CVE-2026-8461 afecta el decodificador MagicYUV de FFmpeg/libavcodec. Un archivo multimedia malicioso puede detonar ejecución de código en aplicaciones que generan thumbnails, transcodifican o reproducen contenido subido por usuarios.

Impacto: El riesgo no está solo en reproductores. También toca Nextcloud, Immich, PhotoPrism, Jellyfin, Emby, Kodi y pipelines automáticos que procesan videos o imágenes. Un archivo subido por un usuario puede terminar ejecutándose del lado servidor.

Qué hacer ahora

- Actualizar FFmpeg a 8.1.2 o superior, o aplicar el backport del proveedor de Linux.
- Aislar transcodificación y generación de thumbnails de contenido no confiable.
- Revisar servidores de media/upload por crashs, procesos ffmpeg anómalos y payloads recientes.

URL oficial: ffmpeg.org / libavcodec advisories

Fuentes: FFmpeg, reportes técnicos, medios especializados

VULNERABILIDADES ALTAS

WEB | PROXY | WORDPRESS

Squidbleed y Gravity SMTP: fugas en proxy y WordPress

Dos riesgos web destacaron por exposición práctica: Squidbleed, CVE-2026-47729, permite fuga de datos HTTP claros en escenarios de proxy compartido; y Gravity SMTP, CVE-2026-4020, fue explotado masivamente para exponer configuración, API keys, tokens y detalles del servidor.

Impacto: Aunque Gravity SMTP tiene severidad media, el abuso masivo lo vuelve prioritario. En ambos casos el peligro está en secretos que quedan visibles: tokens, configuraciones internas, datos de proxy o llaves usadas para correo y automatización.

Qué hacer ahora

- Actualizar Squid a 7.6 o superior y deshabilitar FTP si no se usa.
- Actualizar Gravity SMTP a 2.1.5 o superior.
- Rotar API keys, OAuth tokens y credenciales expuestas en WordPress o proxies corporativos.

URL oficial: squid-cache.org / wordpress.org

Fuentes: Squid, Defiant/Wordfence, medios especializados

LATINOAMÉRICA

MÉXICO | PERÍMETRO

Operation Escaneo: campaña con foco en México y LATAM

CloudSEK describió Operation Escaneo como una campaña contra agencias federales mexicanas, instituciones financieras mexicanas y objetivos de infraestructura en LATAM. La actividad se apoya en appliances expuestos, especialmente Fortinet FortiOS SSL-VPN e Ivanti Connect Secure.

Impacto: No hay confirmación pública gubernamental, pero el valor operativo es claro: los TTPs encajan con intrusiones de perímetro, reconocimiento automatizado, persistencia y exfiltración. Para México, esto merece hunting si hay exposición Fortinet o Ivanti.

Qué hacer ahora

- Mapear Fortinet/Ivanti expuestos y revisar CVE-2022-42475, CVE-2024-21762, CVE-2023-46805, CVE-2024-21887 y CVE-2025-0282.
- Buscar accesos VPN raros, shells, cuentas nuevas, exfiltración y persistencia en appliances.
- Priorizar gobierno, finanzas, telecom, energía, logística y proveedores de esas verticales.

URL oficial: cloudsek.com / medios especializados

Fuentes: CloudSEK, GBHackers, CyberSecurityNews

LATINOAMÉRICA

FORTINET | CREDENCIALES

FortiBleed: robo masivo de credenciales Fortinet

FortiBleed tomó más peso durante el corte porque no se trata solo de una lista filtrada: los reportes describen 73,932 URLs de Fortinet/FortiGate con usuarios, correos y contraseñas en claro. Fortinet sostiene que sería reutilización de datos previos y fuerza bruta, no una vulnerabilidad nueva, pero operativamente las credenciales pueden seguir funcionando.

Impacto: Para México el riesgo es directo por el uso extendido de FortiGate en VPN, terceros, sucursales y proveedores. Si las credenciales siguen vigentes, el atacante no necesita explotar nada nuevo: puede iniciar sesión, tocar AD/RADIUS, abrir RDP o usar accesos MSP ya confiables.

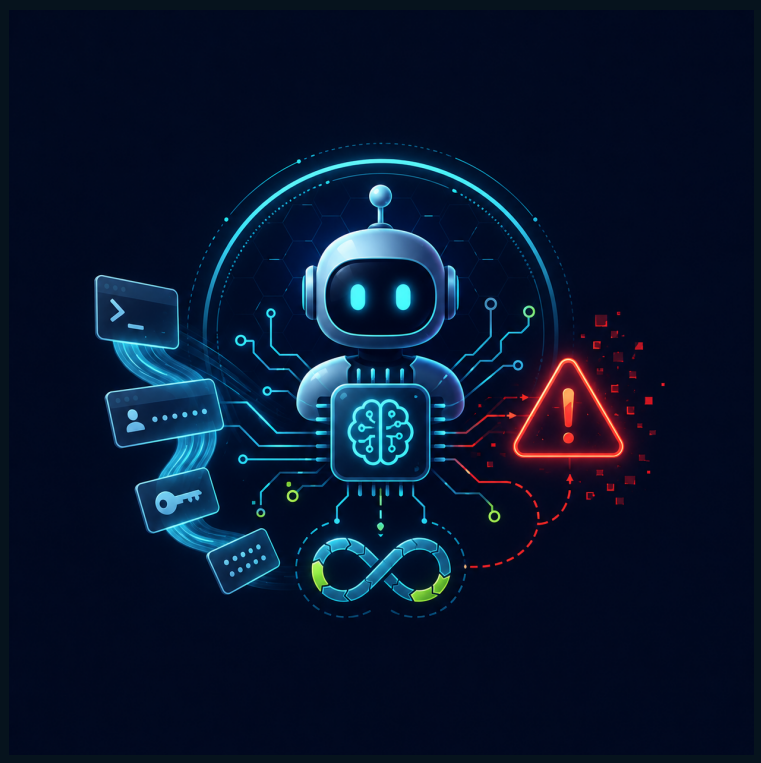
Qué hacer ahora

- Terminar sesiones activas, rotar credenciales Fortinet/FortiGate y forzar MFA resistente a phishing.
- Revisar SSL-VPN, RADIUS, AD, RDWeb, RDP y accesos de terceros/MSP desde junio y semanas previas.
- Buscar logins exitosos con credenciales válidas, cambios de configuración, cuentas nuevas y rutas persistentes.

URL oficial: fortinet.com / techradar.com / bleepingcomputer.com

Fuentes: Fortinet, TechRadar, BleepingComputer, SecurityWeek, Hudson Rock

ACONTECIMIENTOS CRÍTICOS



IA | NPM | SUPPLY CHAIN

Mastra/npm: Sapphire Sleet apunta al ecosistema de IA

Microsoft atribuyó a Sapphire Sleet una campaña contra más de 140 paquetes npm asociados a Mastra, framework TypeScript usado para agentes de IA, RAG, MCP, workflows y proveedores LLM. El paquete malicioso easy-day-js se ejecutaba en postinstall y afectaba Windows, macOS y Linux.

Impacto: Una ventana corta puede bastar para comprometer runners y estaciones de desarrollo. Si un paquete @mastra fue instalado o actualizado el 17 de junio durante la ventana reportada, conviene tratar ese entorno como potencialmente tocado.

Qué hacer ahora

- Revisar instalaciones de paquetes @mastra y easy-day-js realizadas el 17 de junio.
- Limpiar caches npm, revisar lockfiles y rotar tokens npm, GitHub, cloud y LLM.
- Inspeccionar runners CI/CD y workstations de desarrolladores por postinstall sospechoso.

URL oficial: microsoft.com/security/blog / npmjs.com

Fuentes: Microsoft, npm, medios especializados

ACONTECIMIENTOS CRÍTICOS

SAAS | SALESFORCE | OAUTH

Klue/Salesforce: robo de datos vía integración SaaS

Klue confirmó un incidente que afectó su integración con Salesforce entre el 11 y 12 de junio, con impacto comunicado durante esta semana. Los reportes apuntan a credenciales heredadas comprometidas y robo de tokens OAuth de integraciones.

Impacto: El incidente vuelve a mostrar que el riesgo SaaS no termina en el login del usuario. Una integración con permisos amplios puede leer, exportar o sincronizar datos de múltiples clientes si sus tokens quedan expuestos o no se rotan.

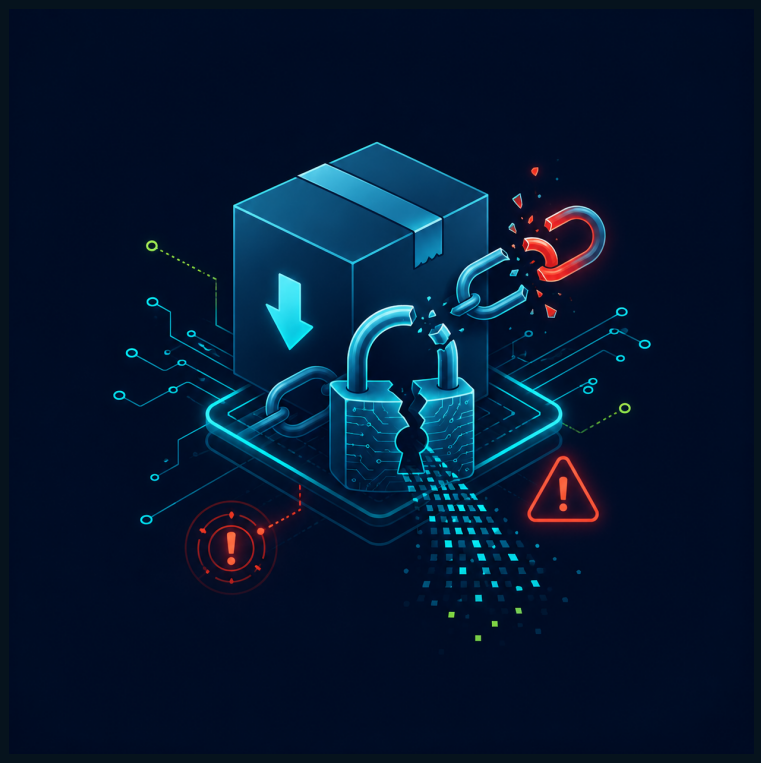
Qué hacer ahora

- Auditar integraciones Klue/Salesforce y cualquier app conectada con permisos amplios.
- Revocar tokens OAuth innecesarios y revisar exportaciones masivas entre el 11 y 23 de junio.
- Validar cuentas de integración, permisos heredados y accesos desde IPs o países inusuales.

URL oficial: klue.com / salesforce.com / medios especializados

Fuentes: Klue, Salesforce ecosystem reports, medios especializados

ACONTECIMIENTOS CRÍTICOS



MALWARE | SOCGHOLISH

Operation Endgame golpea infraestructura de SocGholish

Autoridades europeas y neerlandesas reportaron acciones contra infraestructura de SocGholish, un ecosistema usado para acceso inicial y vinculado a Evil Corp. La policía neerlandesa informó la remediación de 14,971 sitios infectados que distribuían falsas actualizaciones de navegador.

Impacto: SocGholish importa porque se esconde en sitios legítimos comprometidos. Un usuario puede caer en una falsa actualización de Chrome o Edge desde una página aparentemente confiable, y eso puede convertirse en loader, acceso inicial y, en algunos casos, ransomware.

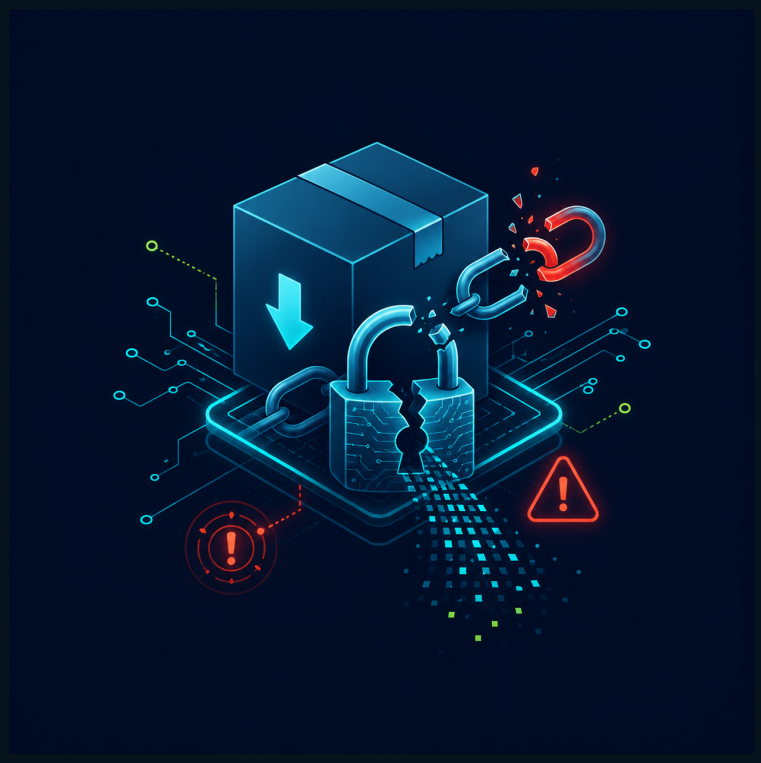
Qué hacer ahora

- Bloquear y monitorear descargas de supuestas actualizaciones de navegador desde sitios no oficiales.
- Buscar scripts inyectados, redirecciones y loaders asociados a sitios legítimos comprometidos.
- Reforzar detección de fake updates, PowerShell/JScript sospechoso y ejecución desde descargas del navegador.

URL oficial: politie.nl / europol.europa.eu / securityweek.com

Fuentes: Operation Endgame, Europol, Policía neerlandesa, SecurityWeek

ACONTECIMIENTOS CRÍTICOS



MOBILE | BANKING TROJAN

Rokarolla: troyano Android contra banca y cripto

Zimperium reportó Rokarolla, un troyano Android distribuido desde sitios falsos y tiendas no oficiales. Se disfraza de Chrome o TikTok, simula Google Play Protect y usa permisos de accesibilidad para montar overlays contra más de 200 apps bancarias y de criptomonedas.

Impacto: No hay foco mexicano confirmado, pero el riesgo aplica a banca móvil, usuarios BYOD y empleados que instalan APKs fuera de tiendas oficiales. El malware puede robar credenciales, PIN, patrón de desbloqueo, SMS, contactos, WhatsApp y hasta bloquear llamadas de alerta.

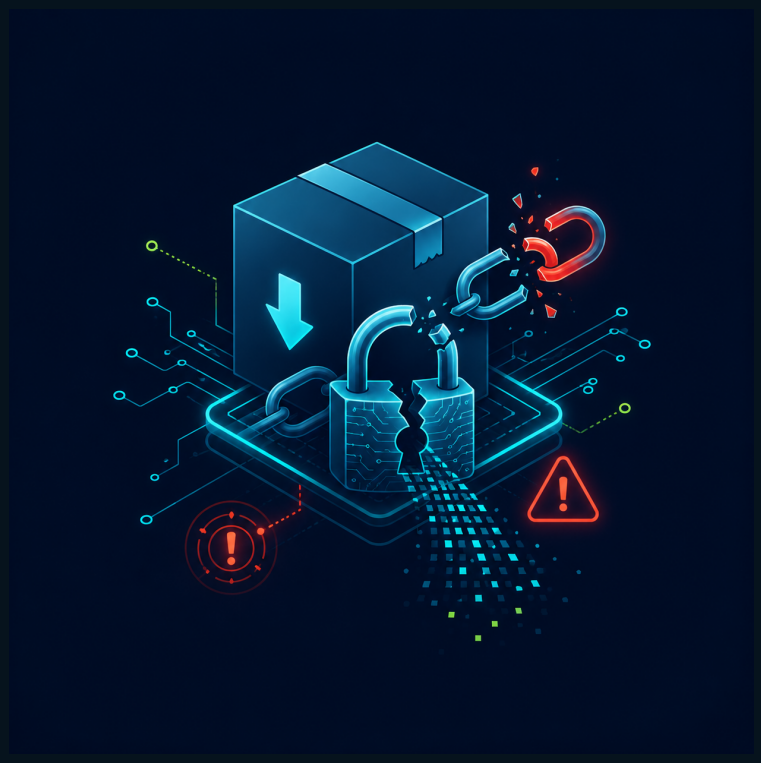
Qué hacer ahora

- Bloquear sideloading Android en dispositivos corporativos y reforzar MDM/Play Protect.
- Detectar abuso de Accessibility Services, overlays, apps ocultas y permisos de SMS/llamadas.
- Reforzar awareness contra APKs de Chrome, TikTok o apps populares descargadas fuera de tiendas oficiales.

URL oficial: zimperium.com / bleepingcomputer.com / techradar.com

Fuentes: Zimperium, BleepingComputer, TechRadar, Tom’s Guide

ACONTECIMIENTOS CRÍTICOS



BOTNET | ROUTERS | NAS

AryStinger: routers y NAS antiguos como red proxy

QiAnXin XLab reportó AryStinger, una botnet que compromete routers D-Link y Linksys antiguos, además de NAS QNAP, para convertirlos en infraestructura proxy y de reconocimiento. La campaña ya suma al menos 4,300 routers infectados, sin contar los NAS afectados.

Impacto: Aunque la concentración principal está en Asia, el patrón es relevante para México por sucursales, proveedores, oficinas pequeñas y equipos SOHO que siguen expuestos años después de quedar fuera de soporte. Un router olvidado puede terminar como pivote silencioso dentro de la red.

Qué hacer ahora

- Inventariar routers D-Link/Linksys y NAS QNAP antiguos en sucursales, terceros y redes pequeñas.
- Actualizar firmware o retirar equipos sin soporte; revisar exposición de administración remota.
- Buscar conexiones salientes a C2, binarios raros en /tmp/bin y procesos como syswapd0h o syswapd0w.

URL oficial: qianxin.com / thehackernews.com / techradar.com

Fuentes: QiAnXin XLab, The Hacker News, TechRadar

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

Grupo Smartekh

NEXT GEN SOC	THREAT INTELLIGENCE	VULNERABILITY MANAGEMENT	ESCRÍBENOS
Monitoreo 24/7	Inteligencia accionable	Visibilidad y remediación	informacion@smartekh.com

#SMARTEKH

Canal WhatsApp | Eventos | Blogs | Infografías Awareness