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

GOBIERNO / WEB COMPROMISE

Brasil detecta compromiso de servidores .gov.br para SEO poisoning

BRASIL GOV.BR CLOAKING

QUÉ ESTÁ PASANDO

CTIR.Gov confirmó una campaña activa contra servidores web .gov.br. Los atacantes inyectan rutas dinámicas y módulos que muestran enlaces de apuestas y fraudes solo a crawlers como Googlebot.

POR QUÉ IMPORTA

El portal puede verse normal para ciudadanos, pero la reputación del dominio oficial queda convertida en infraestructura de fraude y posicionamiento malicioso.

QUÉ REVISAR AHORA

- Reconstruir servidores afectados desde imagen limpia.
- Rotar credenciales y revisar integridad de módulos.
- Buscar cloaking, rutas dinámicas y cambios web no autorizados.
- Validar CMS, frameworks y extensiones expuestas.

FRAUDE FINANCIERO / MÉXICO

CONDUSEF reporta 11 instituciones financieras mexicanas suplantadas

MÉXICO BRAND ABUSE CRÉDITOS FALSOS

QUÉ ESTÁ PASANDO

CONDUSEF informó que 11 entidades financieras notificaron uso indebido de nombre, logotipo y datos institucionales para aparentar créditos o servicios financieros durante agosto.

POR QUÉ IMPORTA

El fraude no requiere intrusión bancaria. El actor explota confianza, marca y necesidad de crédito para obtener dinero o información de usuarios.

QUÉ REVISAR AHORA

- Monitorear dominios, anuncios, redes y WhatsApp con marca falsa.
- Revisar números telefónicos y documentos apócrifos.
- Publicar canales oficiales de validación para clientes.
- Coordinar alertas antifraude y brand protection.

IDENTIDAD / MICROSOFT 365

Passkey phishing permite comprometer identidades y extraer datos de M365

PASSKEY GRAPH SHAREPOINT

QUÉ ESTÁ PASANDO

Microsoft documentó intrusiones que inician con llamadas o mensajes de falso helpdesk. La víctima “actualiza” passkey, MFA o SSO y termina autorizando AiTM o device-code authentication.

POR QUÉ IMPORTA

Después del acceso, los atacantes agregan MFA, enumeran el tenant con Graph y descargan datos de SharePoint, OneDrive y Exchange con identidad legítima.

QUÉ REVISAR AHORA

- Buscar device-code events y nuevos métodos MFA.
- Revisar consentimientos, apps y sesiones anómalas.
- Correlacionar descargas masivas de SharePoint/OneDrive.
- Capacitar: TI no guía alta de passkeys por llamada.

IA / CLOUD / CREDENCIALES

Google observa agentes que roban miles de credenciales en menos de seis horas

AGENTIC AI CLOUD HARVESTING

QUÉ ESTÁ PASANDO

GTIG reportó un caso donde, tras comprometer un recurso cloud, un actor usó un sistema multiagente para planear, construir y ejecutar harvesting masivo de credenciales en menos de seis horas.

POR QUÉ IMPORTA

La IA comprime el tiempo entre acceso inicial, tooling y operación a escala. El SOC tiene menos ventana para detectar y cortar abuso de credenciales.

QUÉ REVISAR AHORA

- Limitar egress y permisos de workloads cloud.
- Detectar creación rápida de tooling y rotación de infraestructura.
- Monitorear uso anómalo de secretos y tokens.
- Revisar repositorios PyPI, npm y Docker utilizados por agentes.

EXPLOIT KIT / ZERO-DAY

BlueMoon combina Chrome y Windows zero-days entre actores de espionaje

CHROME WINDOWS ESPIONAJE

QUÉ ESTÁ PASANDO

Proofpoint identificó cuatro clústeres de espionaje usando BlueMoon. La cadena combina CVE-2026-85046 en Chrome, CVE-2026-87491 para sandbox escape y CVE-2026-85880 en Windows.

POR QUÉ IMPORTA

Una capacidad avanzada pasó a varios actores en días. No basta asumir que un exploit kit pertenece a un solo grupo ni que el riesgo terminó con un parche parcial.

QUÉ REVISAR AHORA

- Actualizar Chrome/Chromium y Windows sin demora.
- Priorizar endpoints de sectores sensibles a espionaje.
- Revisar navegación dirigida y payloads posteriores.
- Monitorear procesos renderer y comportamientos post-exploit.

FIREWALL MANAGEMENT / RANSOMWARE

Cisco FMC es usado para robo de credenciales, espionaje y Qilin

CISCO FMC ROOT QILIN

QUÉ ESTÁ PASANDO

Cisco Talos publicó explotación activa de CVE-2026-20079 y CVE-2026-20316. Observó webshells, Cyclops Blink, exfiltración de credenciales y una cadena que termina en Qilin.

POR QUÉ IMPORTA

FMC tiene control y visibilidad sobre firewalls. Comprometerlo permite mapear dominio, DC, ADFS, Exchange, file servers, bases de datos y credenciales.

QUÉ REVISAR AHORA

- Aplicar fixes de Cisco FMC on-premises.
- Buscar webshells, JAR ejecutores y reverse shells.
- Revisar túneles, cuentas y credenciales extraídas.
- No sobreatribuir Cyclops Blink sin evidencia adicional.

VPN / FIREWALL / RCE

Check Point publica dos RCE críticas en el flujo de certificados VPN

CHECK POINT VPN CVSS 9.8

QUÉ ESTÁ PASANDO

Check Point publicó CVE-2026-85102 y CVE-2026-85103. Ambas afectan el flujo de certificados VPN y pueden permitir RCE remota sin autenticación en configuraciones aplicables.

POR QUÉ IMPORTA

El vector impacta directamente el perímetro VPN. Aunque no hay explotación pública al cierre, el riesgo es crítico para gateways con Remote Access o Site-to-Site VPN.

QUÉ REVISAR AHORA

- Aplicar actualizaciones de emergencia por rama afectada.
- Identificar gateways con Remote Access o S2S VPN.
- Restringir exposición de administración y VPN donde aplique.
- Revisar logs de negociación VPN y certificados anómalos.

EMAIL GATEWAY / RCE

Cisco Secure Email Gateway es explotado para obtener root

CISCO SEG SQLI ROOT

QUÉ ESTÁ PASANDO

Cisco confirmó explotación activa de CVE-2026-76461 en Secure Email Gateway. Un correo especialmente manipulado puede aprovechar la falla durante su procesamiento y terminar en ejecución de comandos como root, sin autenticación ni interacción del usuario. Además, Talos ya había observado a actores APT comprometiendo estos appliances para instalar backdoors y crear túneles hacia otros segmentos de la red.

POR QUÉ IMPORTA

Al comprometer el gateway de correo, el atacante obtiene control sobre un punto por donde pasa una parte crítica de la comunicación de la empresa. Esto puede facilitar intercepción de mensajes, robo de credenciales, manipulación del flujo de correo y acceso posterior a otros sistemas, además de dificultar la detección al operar desde un dispositivo de seguridad legítimo.

QUÉ REVISAR AHORA

- Actualizar a 15.5.5-014, 16.0.4-302 o 16.5.0-780.
- Revisar indicadores de compromiso provistos por Cisco.
- Aislar y preservar evidencia si hay sospecha.
- Validar Secure Email Cloud con avisos directos del proveedor.

DEVOPS / FILE DISCLOSURE

GitLab CVE-2026-85706 permite leer archivos sin autenticación

GITLAB CVSS 10 KEV

QUÉ ESTÁ PASANDO

GitLab corrigió una falla CVSS 10 en CE/EE self-managed. El path traversal en Repository Commits API permite leer archivos arbitrarios sin autenticación bajo condiciones específicas.

POR QUÉ IMPORTA

Archivos locales de GitLab pueden contener configuración, secretos y credenciales que habilitan compromisos posteriores de repositorios y CI/CD.

QUÉ REVISAR AHORA

- Actualizar a 19.3.2, 19.2.6 o 19.1.8.
- Buscar intentos LFI contra gitlab.yml y metadata.path.
- Rotar secretos si hubo exposición previa.
- Confirmar que self-managed no quede publicado sin controles.

SUPPLY CHAIN / ARTIFACTS

JFrog Artifactory encadena tokens anónimos hacia privilegios admin

ARTIFACTORY ADMIN BACKDOORS

QUÉ ESTÁ PASANDO

Wiz confirmó explotación activa de CVE-2026-42018 y CVE-2026-42016. La cadena obtiene un token interno anónimo y lo eleva a permisos administrativos.

POR QUÉ IMPORTA

Artifactory concentra builds, artefactos y relaciones de confianza. Una cuenta admin puede comprometer la cadena de suministro de software.

QUÉ REVISAR AHORA

- Aplicar versiones corregidas en Artifactory self-hosted.
- Buscar cuentas nuevas, tokens admin y plugins Groovy.
- Revisar webshells, comandos de shell y backdoor Rust.
- Rotar credenciales de registries y pipelines expuestos.

IA / CYBER OPERATIONS

Anthropic documenta uso de Claude para explotación y robo de datos

CLAUDE MULTIAGENTE EXFILTRACIÓN

QUÉ ESTÁ PASANDO

Anthropic publicó actividad observada y bloqueada entre diciembre de 2025 y agosto de 2026. Describe grupos estatales y criminales usando workflows multiagente para reconocimiento, explotación y exfiltración.

POR QUÉ IMPORTA

La IA está pasando de asistente a orquestador operativo. Puede reconstruir tooling, escalar harvesting y apoyar explotación SaaS con menos intervención humana.

QUÉ REVISAR AHORA

- Gobernar agentes como identidades privilegiadas.
- Limitar herramientas, conectores y egress de modelos.
- Monitorear automatización de reconocimiento y extracción.
- Separar entornos de prueba ofensiva de Internet real.

ROUTER / SSH / TAKEOVER

MikroTrick permite tomar control de MikroTik RouterOS expuesto por SSH

MIKROTIK SSH OPS

QUÉ ESTÁ PASANDO

CERT Polska confirmó explotación de MikroTrick contra RouterOS. La cadena combina fallas SSH para obtener control administrativo de routers expuestos a redes públicas.

POR QUÉ IMPORTA

MikroTik es común en ISP, sucursales, pymes y redes administradas. Un router comprometido puede servir como pivote, proxy, persistencia o intercepción.

QUÉ REVISAR AHORA

- Actualizar RouterOS y cerrar SSH desde Internet.
- Buscar cuenta privilegiada ops y cambios de usuarios.
- No confiar solo en ausencia del marcador Flagged.
- Rotar credenciales y revisar reglas, túneles y DNS.

IOCS / IDENTIDAD Y CLOUD

IoCs y hunting – M365, GitLab y Artifactory

DEVICE CODE GRAPH LFI TOKENS

Microsoft 365:
• Eventos de device-code authentication y nuevos métodos MFA sin ticket.
• Uso anómalo de Microsoft Graph con python-httpx o Node.js.
• Descargas sostenidas de SharePoint, OneDrive y Exchange REST API.

GitLab:
• Intentos LFI contra gitlab.yml.
• Parámetros sospechosos en metadata.path dentro de Repository Commits API.

JFrog Artifactory:
• Cuentas administrativas nuevas, tokens internos anómalos y plugins Groovy.
• Webshells, comandos de shell y backdoor Rust posterior a elevación de privilegios.

IOCS / EDGE Y APPLIANCES

IoCs y hunting – Cisco, Check Point y MikroTik

FMC SEG VPN ROUTEROS

Cisco FMC:
• Buscar webshells, ejecutores JAR, reverse shells, proxies SOCKS5 y túneles SSH no autorizados.
• Correlacionar actividad asociada a UAT-12197, UAT-11823 y UAT-11988; en este último, revisar señales de robo de credenciales, Impacket, Invoke-TheHash y AV killers previas al posible despliegue de Qilin.

Cisco Secure Email Gateway:
• Buscar indicadores del PSIRT, correos preparados y ejecución de comandos con privilegios root.
• Priorizar appliances físicos o virtuales sin versión corregida.

MikroTik RouterOS:
• Cuenta privilegiada ops.
• Cambios de usuarios, reglas, túneles, DNS o SSH expuesto.
• El marcador Flagged ayuda, pero su ausencia no descarta compromiso.

IOCS / AI Y EXPLOTACIÓN

IoCs y hunting – IA ofensiva y BlueMoon

AGENTIC AI BLUEMOON CHROME

Google GTIG / agentes:
• Creación acelerada de tooling tras acceso cloud.
• Harvesting masivo de credenciales en ventanas cortas.
• Automatización de reconocimiento, errores y rotación de infraestructura.

BlueMoon:
• Cadena: CVE-2026-85046 + CVE-2026-87491 + CVE-2026-85880.
• Priorizar telemetría de Chrome/Chromium y Windows con señales post-exploit.

Anthropic:
• Workflows multiagente usados para reconocimiento, explotación y exfiltración.
• Revisar agentes con conectores, herramientas y salida a Internet.

OBSERVACIÓN / MÉXICO Y LATAM

Alegaciones y OSINT no verificado

NO CONFIRMADO NO SOBREAFIRMAR

Tender / Krybit – México:
Krybit incluyó a Tender / Carnicería Tender en su portal el 13 de septiembre. No existe confirmación pública de intrusión, cifrado, exfiltración, tipo de información o impacto. Mantener como alegación del actor.

SIPA Argentina / BogotaLeaks:
El actor afirmó poseer 38M registros del SIPA argentino. Ransomware.mx y Dark Web Informer lo clasifican como no verificado; no hay metodología, fecha de acceso ni confirmación oficial.

Tratamiento recomendado:
• No atribuir ni afirmar brecha sin evidencia independiente.
• Mantener seguimiento en fuentes oficiales, regulatorias y muestras verificadas.

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