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

BRASIL / MALWARE

PhantomEnigma: gov.br como canal para malware

BRASIL | GOV.BR | MALWARE

El dominio legítimo no garantiza seguridad cuando la infraestructura fue abusada.

QUÉ ESTÁ PASANDO

ANY.RUN documentó que PhantomEnigma usó más de 20 portales gubernamentales brasileños y buzones legítimos para distribuir malware. Los correos podían pasar SPF, DKIM y DMARC porque salían desde infraestructura real. La cadena usó señuelos policiales/notariales, Inno Setup y un backdoor Node.js modular.

POR QUÉ IMPORTA

Un mensaje desde un dominio gubernamental puede parecer confiable para usuarios y controles de reputación. Esto eleva el riesgo de infección en banca, gobierno y áreas legales.

FUENTES SUGERIDAS

ANY.RUN · The Hacker News

QUÉ REVISAR AHORA

- Validar adjuntos por comportamiento, no solo por dominio.
- Revisar correos .gov.br con instaladores o ejecutables.
- Bloquear Inno Setup sospechoso y Electron no autorizado.
- Buscar conexiones Node.js hacia C2 o dominios recientes.

VULNERABILIDAD CRÍTICA

Microsoft: zero-days en SharePoint/ADFS

SP ADFS KEV

La urgencia no termina al parchear: puede haber claves IIS robadas y persistencia.

QUÉ ESTÁ PASANDO

Microsoft corrigió zero-days explotados en AD FS y SharePoint Server on-premises. CISA alertó que atacantes encadenaban fallas de SharePoint para omitir autenticación, ejecutar código, robar machine keys de IIS, desplegar malware y mantener acceso después del compromiso.

POR QUÉ IMPORTA

SharePoint y AD FS están cerca de identidad, contenido interno y flujos administrativos. Si el atacante roba claves o tokens, puede conservar acceso aunque el servidor ya esté actualizado.

FUENTES SUGERIDAS

Microsoft · CISA KEV · BleepingComputer · SecurityWeek

QUÉ REVISAR AHORA

- Aplicar parches de julio en granjas SharePoint y AD FS.
- Rotar machine keys y revisar IIS tras exposición.
- Buscar webshells, procesos anómalos y archivos recientes.
- Restringir Central Administration y acceso externo.

ERP / PAGOS

Oracle EBS: falla en pagos entra a CISA KEV

ORACLE | EBS | KEV

Un ERP vulnerable puede convertir un problema técnico en riesgo financiero y operativo.

QUÉ ESTÁ PASANDO

CISA añadió CVE-2026-46817 a KEV por explotación activa contra Oracle E-Business Suite. La falla afecta Oracle Payments File Transmission y puede permitir compromiso vía HTTP sin autenticación. El parche existía desde mayo, pero la explotación real cambió la prioridad.

POR QUÉ IMPORTA

Oracle EBS concentra pagos, proveedores, finanzas e integraciones críticas. Una intrusión puede exponer datos financieros, credenciales y procesos de negocio.

FUENTES SUGERIDAS

CISA KEV · NVD · Oracle · BleepingComputer

QUÉ REVISAR AHORA

- Confirmar parche de Oracle EBS y módulos de Payments.
- Identificar exposición HTTP/Internet del componente.
- Buscar accesos no autenticados y cargas anómalas.
- Revisar integraciones financieras y cuentas técnicas.

VPN / ACCESO REMOTO

SonicWall SMA1000 atacado con dos zero-days

VPN | SMA | KEV

Los appliances de acceso remoto son una puerta directa hacia la red interna.

QUÉ ESTÁ PASANDO

SonicWall confirmó explotación activa de CVE-2026-15409 y CVE-2026-15410 en SMA1000. Una falla permite SSRF preautenticación y la otra ejecución de comandos por inyección en la consola de administración. El fabricante publicó hotfix e indicadores.

FUENTES SUGERIDAS

SonicWall PSIRT · CISA KEV · SecurityWeek

POR QUÉ IMPORTA

Si el acceso remoto cae, el atacante puede pivotar hacia usuarios, servidores y proveedores. El riesgo aumenta si la administración del appliance está expuesta.

QUÉ REVISAR AHORA

- Aplicar hotfix de SMA1000 de inmediato.
- Revisar IOCs y logs de Appliance Work Place/AMC.
- Limitar administración a redes confiables.
- Rotar credenciales si hubo exposición o señales de acceso.

SEGURIDAD PERIMETRAL

FortiSandbox: fallas críticas explotadas en el SOC

FORTI RCE KEV

Una herramienta de análisis comprometida puede volverse un punto ciego del SOC.

QUÉ ESTÁ PASANDO

CISA incorporó CVE-2026-39808 y CVE-2026-25089 de FortiSandbox a KEV por explotación activa. Ambas pueden permitir ejecución remota de código o comandos sin autenticación bajo ataques de baja complejidad. Las correcciones ya estaban disponibles.

POR QUÉ IMPORTA

FortiSandbox procesa archivos sospechosos e integra controles de seguridad. Si se compromete, el atacante puede tocar una zona sensible de análisis y telemetría.

FUENTES SUGERIDAS

CISA KEV · Fortinet · BleepingComputer

QUÉ REVISAR AHORA

- Actualizar FortiSandbox a versiones corregidas.
- Revisar exposición de consola y APIs.
- Buscar comandos, jobs o archivos anómalos.
- Validar integraciones con SIEM, EDR y correo.

SAAS / IA

ServiceNow AI Platform: RCE bajo observación

IA | RCE | NOW

La IA empresarial también concentra workflows, datos y credenciales de integración.

QUÉ ESTÁ PASANDO

ServiceNow corrigió CVE-2026-6875, un escape de sandbox con posible ejecución remota sin autenticación bajo ciertas condiciones. Las instancias alojadas fueron actualizadas y los clientes self-hosted recibieron parches. Defused reportó explotación en Internet el 17 de julio.

POR QUÉ IMPORTA

ServiceNow puede concentrar CMDB, tickets, automatizaciones y cuentas de integración. Un RCE en esa plataforma puede tener alcance transversal en la empresa.

FUENTES SUGERIDAS

ServiceNow · NVD · BleepingComputer

QUÉ REVISAR AHORA

- Confirmar parche en instancias self-hosted.
- Revisar integraciones y cuentas con privilegios.
- Buscar ejecuciones o cambios anómalos en workflows.
- Validar conectores de IA y accesos externos.

CMS / RCE

WP2Shell: RCE en WordPress ya tiene exploits

WP | RCE | CMS

El escaneo automatizado comienza rápido cuando el objetivo es WordPress.

QUÉ ESTÁ PASANDO

WordPress publicó actualizaciones para CVE-2026-60137 y CVE-2026-63030. Al encadenarse, las fallas de REST API e inyección SQL pueden llegar a ejecución remota de código. Después de la divulgación aparecieron exploits públicos e intentos en Internet.

POR QUÉ IMPORTA

WordPress sostiene comercio, medios, blogs corporativos y portales públicos. Un sitio vulnerable puede terminar con webshells, malware, redirecciones o robo de datos.

FUENTES SUGERIDAS

WordPress · GitHub Advisories · BleepingComputer · SecurityWeek

QUÉ REVISAR AHORA

- Confirmar actualización automática o parche manual.
- Revisar logs REST API y SQL anómalos.
- Buscar webshells y archivos PHP recientes.
- Validar plugins, temas y respaldos limpios.

SUPPLY CHAIN

AsyncAPI: npm comprometido vía GitHub Actions

NPM | CI/CD | TOKENS

Desactivar scripts de instalación no siempre basta si el payload corre al importar.

QUÉ ESTÁ PASANDO

Microsoft identificó cinco versiones maliciosas de paquetes @asyncapi publicadas durante unos 90 minutos. El origen fue un flujo vulnerable de GitHub Actions que expuso credenciales de publicación. El loader se ejecutaba al importar el módulo, no solo durante instalación.

POR QUÉ IMPORTA

Una dependencia legítima puede llegar a aplicaciones, builds y entornos de desarrollo. El impacto puede incluir robo de información, RAT y exposición de secretos de CI/CD.

FUENTES SUGERIDAS

Microsoft Security Research · GitHub Advisories · BleepingComputer

QUÉ REVISAR AHORA

- Revisar lockfiles, cachés y builds de AsyncAPI.
- Rotar tokens npm, GitHub y secretos de pipeline.
- Buscar paquetes instalados en la ventana afectada.
- Revisar dependencias transitivas y artefactos publicados.

INFOSTEALER / IDENTIDAD

ACR Stealer: ClickFix roba tokens y documentos

CLICKFIX | M365 | TOKENS

El atacante no necesita explotar un servidor si convence al usuario de ejecutar el comando.

QUÉ ESTÁ PASANDO

Microsoft documentó campañas de ACR Stealer que empiezan con señuelos ClickFix. Las cadenas usan WebDAV, PowerShell, Python, MSHTA, blockchain y payloads ocultos en imágenes para robar contraseñas, cookies, tokens, PDF y documentos de Microsoft 365.

POR QUÉ IMPORTA

Cookies y tokens robados pueden permitir acceso a nube sin la contraseña. El resultado puede ser BEC, fraude, exfiltración y movimiento lateral.

FUENTES SUGERIDAS

Microsoft Security Research · BleepingComputer

QUÉ REVISAR AHORA

- Bloquear instrucciones ClickFix en awareness y filtros.
- Monitorear PowerShell/MSHTA/WebDAV desde usuario.
- Invalidar sesiones ante indicios de robo.
- Buscar accesos M365 desde países o dispositivos inusuales.

IA / CLOUD

NadMesh busca servicios de IA expuestos

IA | CLOUD | BOTNET

Los laboratorios de IA publicados para pruebas también entran al radar de botnets.

QUÉ ESTÁ PASANDO

Una investigación atribuida a XLab describió NadMesh, un botnet en Go que usa fuentes como Shodan para encontrar servicios expuestos. Apunta a ComfyUI, Ollama, n8n, Open WebUI, Gradio, Docker, Jenkins y otros, buscando tokens Kubernetes, claves cloud y configuraciones MCP.

POR QUÉ IMPORTA

Servicios de IA sin autenticación pueden exponer secretos y convertirse en pivote hacia cloud, pipelines o redes internas.

FUENTES SUGERIDAS

XLab · The Hacker News

QUÉ REVISAR AHORA

- Inventariar interfaces de IA y automatización expuestas.
- Exigir autenticación, VPN o allowlist.
- Buscar secretos en contenedores y logs.
- Segmentar laboratorios de IA respecto de producción.

IA / BRECHA

Hugging Face: intrusión conducida por agentes autónomos

HF | DATASET | TOKENS

Los datasets no confiables pueden convertirse en una cadena real de intrusión.

QUÉ ESTÁ PASANDO

Hugging Face confirmó que un dataset malicioso abusó de dos rutas de ejecución en su pipeline de procesamiento. El actor escaló a nodos internos, obtuvo credenciales cloud y de clúster y se movió lateralmente con un framework autónomo que ejecutó miles de acciones.

POR QUÉ IMPORTA

El caso une datos no confiables, ejecución de código, tokens y automatización ofensiva. Afecta la forma en que se gobiernan modelos, datasets y pipelines de IA.

FUENTES SUGERIDAS

Hugging Face · BleepingComputer

QUÉ REVISAR AHORA

- Rotar tokens de Hugging Face y revisar actividad.
- Separar procesamiento de datasets de credenciales cloud.
- Revisar permisos de workers y clústeres.
- Aplicar sandboxing estricto a cargas no confiables.

RANSOMWARE / OT

Fairlife: ransomware detiene producción de Coca-Cola

RANSOM | OT | FOOD

El impacto del ransomware puede medirse en líneas de producción detenidas, no solo en datos.

QUÉ ESTÁ PASANDO

Coca-Cola informó a la SEC que Fairlife detectó acceso no autorizado relacionado con ransomware en sistemas, incluidos componentes vinculados a producción. La empresa activó continuidad de negocio y suspendió temporalmente producción en instalaciones de Estados Unidos.

POR QUÉ IMPORTA

El incidente confirma impacto operativo en manufactura y alimentos. Una interrupción similar puede afectar distribución, inventario, ingresos y confianza de clientes.

FUENTES SUGERIDAS

The Coca-Cola Company / SEC · BleepingComputer

QUÉ REVISAR AHORA

- Validar segmentación entre IT, OT y producción.
- Probar continuidad operativa y restauración offline.
- Revisar accesos remotos a plantas y proveedores.
- Monitorear ransomware en servidores de producción.

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