



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

VULNERABILIDAD CRÍTICA / PERÍMETRO

Citrix NetScaler: explotación activa de dos zero-days y persistencia

CITRIX NETSCALER ZERO-DAY

**QUÉ ESTÁ PASANDO**

Citrix confirmó explotación de CVE-2026-88771/88772 y Unit 42 observó webshells y persistencia.

POR QUÉ IMPORTA

NetScaler suele estar publicado en Internet y da acceso remoto o publica aplicaciones. El riesgo continúa después del parche si el atacante ya dejó webshells, cuentas o cambios persistentes.

QUÉ REVISAR AHORA

- Identificar appliances expuestos y su función (VPN, Gateway, LB).
- Parchear y comprobar que quedaron en versión corregida.
- Revisar /vpn/scripts/linux/ y LogonPoint/custom/.
- Buscar actividad previa al parche y preservar evidencia si aparece un webshell.

VULNERABILIDAD CRÍTICA / SD-WAN

Cisco Catalyst SD-WAN Manager: bypass de autenticación con privilegios de admin

CISCO SD-WAN CVSS 9.8



QUÉ ESTÁ PASANDO

Cisco publicó CVE-2026-76504 (CVSS 9.8). Una petición especialmente construida puede saltarse la autenticación de SD-WAN Manager y llegar a la API con privilegios de administrador.

POR QUÉ IMPORTA

vManage concentra la administración de la WAN. Un acceso administrativo no autorizado puede traducirse en cambios de conectividad, rutas o configuración en varios sitios desde un solo punto.

QUÉ REVISAR AHORA

- Validar versión y si el management plane estuvo expuesto a Internet.
- Revisar serviceproxy-access.log y vmanage-server.log.
- Buscar j_security_check codificado y usuarios viptela-reserved-*.
- Si hay indicios, recolectar admin-tech y escalar a Cisco TAC.

EMAIL GATEWAY / ZERO-DAY

FortiMail CVE-2026-104286: zero-day con escritura arbitraria

FORTIMAIL ZERO-DAY KEV



QUÉ ESTÁ PASANDO

Fortinet reveló un zero-day de FortiMail (CVE-2026-104286) explotado activamente. La falla permite escritura arbitraria de archivos sin autenticación mediante HTTP/HTTPS y puede terminar en ejecución de código o comandos.

POR QUÉ IMPORTA

FortiMail está en una posición privilegiada frente al correo corporativo. Un appliance comprometido puede servir para persistencia, manipulación del flujo de correo y acceso posterior a otros recursos.

QUÉ REVISAR AHORA

- Identificar versiones afectadas y exposición de la interfaz de administración.
- Buscar `/data/lib/liblog.so`, `/data/bin/webconsole` y `/data/bin/mailservice`.
- Revisar `/data/etc/ld.so.preload`, `/bin/smit` y `/data/migadmin.tar.gz`.
- Correlacionar conexiones con `79.141.169[.]187` y `45.129.0[.]192`.

EMAIL / COMMAND INJECTION

Zimbra CVE-2026-73570: command injection en servidores de correo

ZIMBRA RCE WEBSHELL



QUÉ ESTÁ PASANDO

Microsoft publicó evidencia de explotación de CVE-2026-73570 en Zimbra. Los atacantes ejecutaron comandos sin autenticación, desplegaron webshells JSP y reverse shells y realizaron reconocimiento y preparación de datos para posible extracción.

POR QUÉ IMPORTA

El servidor de correo concentra mensajes, credenciales y relaciones internas. La actividad observada también muestra persistencia mediante cron/systemd y movimiento entre nodos del clúster.

QUÉ REVISAR AHORA

- Confirmar Zimbra 10.1.20 o superior y retirar zimbra-snmp si no es necesario.
- Buscar webshells JSP, zimlog.service y chronyd-helper.service.
- Revisar 45.32.30[.]235:8080/8081, 193.42.40[.]135 y 3.209.137[.]175.
- Correlacionar zmslapcat, wget/curl, azcopy y archivos .kworker_sys.

Zammad: RCE y escalamiento local tras una investigación de compromiso

ZAMMAD RCE LPE



QUÉ ESTÁ PASANDO

La investigación de DIVD derivó en CVE-2026-102489 y CVE-2026-102490. La primera permite RCE en Zammad 6.5 o anteriores; la segunda es una escalada local a root y requiere acceso previo al servidor..

POR QUÉ IMPORTA

El riesgo depende de la versión y del nivel de acceso ya obtenido. Una explotación de RCE puede exponer tickets, sesiones y datos operativos; la LPE aumenta el impacto si el servidor ya fue comprometido.

QUÉ REVISAR AHORA

- Identificar Zammad 6.5 o anteriores y priorizar actualización.
- Confirmar que 7.0+ no es vulnerable a CVE-2026-102489.
- Revisar exposición, sesiones y cuentas administrativas.
- Si existe actividad previa, investigar primero el acceso al servidor antes de atribuir la LPE.

KUBERNETES / STORAGE

Dell Container Storage Modules: CVSS 10 sobre Kubernetes y storage

DELL CSM KUBERNETES CVSS 10



QUÉ ESTÁ PASANDO

Dell publicó múltiples fallas críticas en Container Storage Modules. CVE-2026-63688 y CVE-2026-63692 tienen CVSS 10.0; el conjunto incluye bypass de autenticación, exposición de credenciales de storage y escalamiento a root en nodos Kubernetes. No hay explotación pública confirmada.

POR QUÉ IMPORTA

CSM conecta Kubernetes con almacenamiento empresarial. Un compromiso puede afectar secretos, RBAC, tenants y acceso a cabinas, ampliando el impacto desde un clúster hacia la capa de almacenamiento.

QUÉ REVISAR AHORA

- Inventariar CSM y confirmar versiones desplegadas.
- Priorizar actualización y revisión de secretos/JWT.
- Auditar credenciales de storage y cambios de RBAC.
- Revisar Custom Resources y accesos administrativos anómalos.

CYBERESPIONAGE / PHISHING

Star Blizzard: RedFlick reduce la fricción para desplegar CosmicPulse

STAR BLIZZARD REDFLICK COSMICPULSE



QUÉ ESTÁ PASANDO

Microsoft publicó la evolución de Star Blizzard. RedFlick reduce la interacción del usuario: un ZIP/VHDX puede terminar en tareas programadas que despliegan CosmicPulse. Microsoft ha observado estas variantes desde enero de 2026.

POR QUÉ IMPORTA

La técnica desplaza el foco desde el clic inicial hacia persistencia y ejecución programada. Una campaña de phishing puede pasar desapercibida si solo se inspeccionan mensajes y no el comportamiento posterior del endpoint.

QUÉ REVISAR AHORA

- Buscar ZIP/RAR protegidos, LNK y VHDX recibidos por correo.
- Revisar tareas nuevas como Internet Quality Test Connection y System Health Monitor.
- Buscar CosmicPulse, msiexec/control.exe anómalos y WebDAV.
- Correlacionar los IP/dominios publicados por Microsoft con tráfico de endpoints.

PHISHING / RMM ABUSE

MSP360 + ScreenConnect: RMM legítimo usado para persistencia

MSP360 SCREENCONNECT RMM

**QUÉ ESTÁ PASANDO**

Microsoft reportó campañas en las que un instalador legítimo de MSP360 RMM se distribuye con nombres engañosos y después instala ScreenConnect. El objetivo es mantener un segundo canal de acceso; Microsoft no observó explotación de ScreenConnect.

POR QUÉ IMPORTA

El atacante se apoya en software que puede parecer legítimo para TI. La combinación de dos RMM permite conservar acceso aunque uno de los canales sea detectado o eliminado.

QUÉ REVISAR AHORA

- Inventariar MSP360 y ScreenConnect autorizados.
- Revisar instalaciones nuevas, servicios y reglas de firewall asociadas.
- Buscar la cadena RMM.Agent.exe → PowerShell → ScreenConnect.
- Correlacionar hashes y dominios de la campaña con telemetría histórica.

MÉXICO / ACTUALIZACIÓN DE INCIDENTE

Aeroméxico: datos de pasajeros potencialmente expuestos

MÉXICO DATOS PERSONALES TERCEROS



QUÉ ESTÁ PASANDO

Aeroméxico reiteró que la investigación está relacionada con un incidente de 2025 en una plataforma de un tercero. La base ofrecida en Telegram contenía más de 15 millones de registros; la autoridad analizó una muestra de 100,092.

POR QUÉ IMPORTA

La información bajo revisión puede incluir nombre, fecha de nacimiento, nacionalidad, género, correo, teléfono, ruta preferida, número de pasaporte y número de viajero frecuente. Aeroméxico señaló que no identificó datos financieros ni contraseñas de Rewards.

RANSOMWARE / INITIAL ACCESS

Warlock: SharePoint como punto de entrada contra infraestructura crítica

WARLOCK SHAREPOINT TOOL SHELL



QUÉ ESTÁ PASANDO

Un reporte publicado durante el corte documentó a Warlock explotando vulnerabilidades de SharePoint para obtener acceso inicial. En los casos analizados se observó reconocimiento posterior, intentos de deshabilitar controles de seguridad y despliegue de ransomware.

POR QUÉ IMPORTA

SharePoint puede convertirse en puente hacia infraestructura crítica y sistemas administrativos. El mayor riesgo no es solo perder el portal, sino que el acceso inicial termine en movimiento lateral y cifrado.

QUÉ REVISAR AHORA

- Identificar SharePoint Server expuesto y validar ToolShell/parches.
- Buscar webshells y procesos anómalos posteriores a la explotación.
- Revisar intentos de deshabilitar EDR/AV.
- Correlacionar reconocimiento interno y conexiones hacia servidores críticos.

INITIAL ACCESS / MALWARE / LATAM

BraZetsu: toolkit de Initial Access Brokers dirigido a LATAM

BRAZETSU EXILWARE LATAM



QUÉ ESTÁ PASANDO

Group-IB publicó BraZetsu, un framework Windows en Python atribuido con alta confianza a Exilware. Recopila credenciales y certificados, enumera el equipo y convierte sistemas comprometidos en accesos que pueden venderse a otros actores.

POR QUÉ IMPORTA

El impacto regional está en el modelo de negocio: un endpoint comprometido no necesariamente termina en fraude o ransomware de inmediato; puede convertirse primero en un acceso comercial para otro atacante.

QUÉ REVISAR AHORA

- Buscar Python no autorizado y ejecución de cmd.exe desde el framework.
- Revisar acceso a PFX/P12, OneDrive y recursos compartidos.
- Buscar enumeración de procesos, ERP, VPN/RDP y aplicaciones financieras.
- Correlacionar dominios de BraZetsu/Exilware con tráfico de endpoints.

RANSOMWARE / LAW ENFORCEMENT

Operation KillSwitch: desmantelamiento de KillSec

KILLSEC KILLSWITCH RANSOMWARE



QUÉ ESTÁ PASANDO

Europol confirmó Operation KillSwitch contra KillSec: tres arrestos, ocho registros y control de servidores y leak site. Se aseguraron al menos 110 TB y Europol vincula la operación con alrededor de 1,000 ataques.

POR QUÉ IMPORTA

Es una disrupción real de una operación RaaS, no una alegación del actor. La presencia documentada de víctimas en Brasil y Colombia hace relevante revisar exposición histórica de organizaciones LATAM.

QUÉ REVISAR AHORA

- Revisar si la organización apareció en infraestructura histórica de KillSec.
- Correlacionar incidentes anteriores con sus IOCs conocidos.
- Revisar RDP, aplicaciones expuestas y credenciales comprometidas.
- Validar si terceros con acceso a datos sensibles estuvieron involucrados.

Indicadores y hunting – Citrix NetScaler y Cisco SD-WAN



CITRIX NETSCALER

- IPs: 66.135.19[.]18 · 167.99.111[.]203 · 142.93.85[.]227
- IPs: 104.248.74[.]206 · 193.149.176[.]207
- /vpn/scripts/linux/nsgclient18.deb · /vpn/scripts/linux/nsg64.deb
- **SHA256:**
ae22ef2517b5c0fb47f78745b9cb5260acee0e751b89bcd354640ff8bc8d29ec

CISCO SD-WAN

- /%6a_security_check
- serviceproxy-access.log / vmanage-server.log
- Usuarios viptela-reserved-* desde IPs no autorizadas

Indicadores y hunting – Zimbra y MSP360 / ScreenConnect



ZIMBRA – IOCs PUBLICADOS POR MICROSOFT

- 117.107.25[.]243:7071 · 192.255.193[.]111:9004
- 45.32.30[.]235:8080/8081 · 193.42.40[.]135:443
- transzimbra[.]linkpc[.]net · psk1zim[.]abrdns[.]com
- tls[.]psk1zim[.]abrdns[.]com · wslogzimbra[.]linkpc[.]net
- **SHA256:**
dee5af1c0f76b45d28bafd6e60c07bb8e391d98addf81ef8f13d073acdb3c48a
- **SHA256:**
b594a42b8f1c6f090327bb9a3361c2d3515537fb7ac8da6b9061b9a3f330e159

MSP360 / SCREENCONNECT

- **SHA256:**
108ef7e628d7a20bd6241a5b57149e27a6061f467123eb64061975559f8f73dc
- **Dominios:** adswre[.]cfd · trews[.]cfd · sdfghj[.]rd-team[.]ru

Indicadores y hunting – FortiMail, RedFlick y BraZetsu

BRAZETSU KILLSEC CSM



FORTIMAIL – IOCs

- 79[.]141[.]169[.]187 · 45[.]129[.]0[.]192
- /data/lib/liblog.so – SHA256
8015f34dc84922b03688399d7f9fe7a00361789f7e420c7e2a2cdb23e75cef84
- /data/bin/webconsole · /data/bin/mailservice
- /data/etc/ld.so.preload · /bin/smit · /data/etc/httpd.conf

STAR BLIZZARD / REDFLICK

- 103.245.231[.]248 · 2.57.241[.]246 · 45.84.59[.]66
- secure-dns-hub[.]com · gliderrompercycl[.]com · ruten[.]observer

BRAZETSU / EXILWARE

- infect[.]online · c2[.]installcenter[.]com
- **Revisar certificados PFX/P12, OneDrive y enumeración de procesos**

OBSERVACIÓN / RANSOMWARE REGIONAL

Claims regionales: señales de presión, no evidencia de compromiso

MÉXICO LATAM NO CONFIRMADO



Se observaron nuevas publicaciones contra organizaciones de México y Brasil.

MÉXICO:

- Econ-Tec / SafePay
- COAL / Akira
- Grupo Industrial Tauro / Lamashtu.

LATAM:

- Soma / M3RX
- Terca Zilli / RansomHouse
- La Ponderosa / Emperador
- Jampac / Akira
- Paes Soluções / Panzer.

Claims en México: qué dicen tener los actores

MÉXICO CLAIMS NO CONFIRMADO



ECON-TEC / SAFEPLAY – 30-SEP

- El grupo amenaza con publicar información sensible; las fuentes revisadas no detallan un inventario fiable de archivos.

COAL / AKIRA – 3-OCT

- El claim menciona 77 GB y datos de pasaportes, información financiera y registros de estudiantes/clientes. No está verificado.

GRUPO INDUSTRIAL TAURO / LAMASHTU – 5-OCT

- El actor lo presenta como víctima; no publica un detalle verificable del tipo o volumen de datos en las fuentes revisadas.

Los tres casos deben mantenerse como alegaciones del actor.

Claims en LATAM: datos y alcance alegados

LATAM CLAIMS NO CONFIRMADO



JAMPAC ALIMENTOS / AKIRA – 2-OCT

- Se amenaza con publicar 35 GB y se mencionan pasaportes, pagos, información financiera y datos de clientes. No está verificado.

LA PONDEROSA / EMPERADOR – 1-OCT

- Se alegan varios miles de documentos de personal y clientes, con un volumen declarado de 3.4 GB. No está verificado.

PAES SOLUÇÕES / PANZER – 2-OCT

- El actor amenaza con publicar toda la información sensible; no se detallan categorías verificadas.

SOMA / M3RX – 29-SEP · TERCA ZILLI / RANSOMHOUSE – 1-OCT

- No hay inventario público fiable de los datos supuestamente obtenidos. En Soma existe una posible credencial administrativa expuesta previamente, pero su relación con el claim no está confirmada.



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

