
CYBER_CORE
CYBER_CORE
CYBER_CORE
QUANTUM_AENIS
DATA_FLOW
CYBER_FLOW
STORAGE_VAULT
BOLETÍN DE CIBERSEGURIDAD
EDICIÓN JUNIO 2026

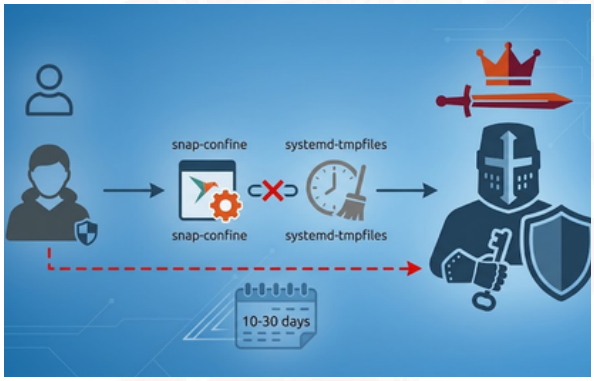
BOLETÍN DE CIBERSEGURIDAD, JUNIO DE 2026

QUE EL ÚNICO GOL DEL MES SEA A FAVOR DE NUESTRA SEGURIDAD DIGITAL.

La Copa Mundial es el evento global más grande, uniendo a millones de personas bajo una misma pasión. Sin embargo, esta enorme atención masiva también enciende las alertas en el terreno digital, convirtiéndolo en el escenario perfecto para los ciberdelincuentes. Durante el torneo, las estafas de phishing, los enlaces de transmisiones falsas y los ataques a la infraestructura se multiplican exponencialmente. Los atacantes aprovechan la distracción y la emoción generalizada para intentar vulnerar tanto a los usuarios como a las redes institucionales. Por ello, en este boletín te invitamos a vivir la gran fiesta del fútbol, pero manteniendo siempre nuestra seguridad digital con la guardia en alto.

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.

ALERTA EN LINUX: VULNERABILIDAD EN UBUNTU PERMITE ACCESO DE ADMINISTRADOR (ROOT)



Se identificó la vulnerabilidad de alta gravedad CVE-2026-3888 (CVSS: 7.8) que afecta a los sistemas predeterminados de Ubuntu Desktop 24.04 y versiones superiores. El fallo radica en una interacción imprevista entre el gestor de entornos aislados snap-confine y el servicio de limpieza automática systemd-tmpfiles. Un atacante local sin privilegios puede aprovechar este comportamiento manipulando de forma precisa la sincronización de los ciclos de eliminación en el directorio /tmp/.snap.

Aunque la complejidad de la explotación es elevada debido a que requiere esperar un periodo de entre 10 y 30 días, el impacto final es el compromiso total del host. Una vez eliminado el directorio legítimo, el atacante introduce cargas maliciosas que se ejecutan bajo los máximos privilegios cuando el entorno snap se reinicializa. Canonical ya ha mitigado el riesgo y se insta a los administradores a actualizar el paquete snapd a las versiones corregidas 2.73 o superiores de inmediato.

FUENTE: THE HACKER NEWS

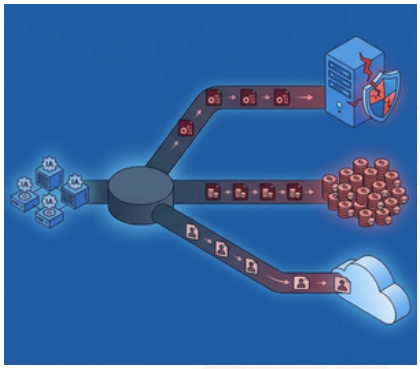
ALERTA EN LA RED: DETECTAN SITIOS FALSOS QUE SUPLANTAN A LA FIFA PARA EL MUNDIAL 2026

A las puertas de la Copa Mundial 2026, investigadores de ciberseguridad identificaron cinco sitios web falsos que imitan a la perfección el diseño, los colores y la experiencia de usuario de la página oficial de la FIFA. Utilizando técnicas de typosquatting (creación de dominios con variaciones sutiles en la URL como extensiones .shop, .store o .site), los estafadores atraen a los fanáticos mediante la supuesta venta de entradas y merchandising oficial de las selecciones.

El engaño se propaga a través de anuncios en redes sociales y resultados patrocinados en buscadores; sin embargo, en lugar de recibir los productos o tickets, las víctimas terminan entregando su dinero, información confidencial y datos bancarios a los ciberdelincuentes. Ante esto, la FIFA recuerda que los boletos se venden de manera exclusiva en su plataforma oficial (FIFA.com/tickets) y los expertos recomiendan evitar intermediarios, revisar minuciosamente las URL y desconfiar de ofertas excesivamente atractivas.

FUENTE: WELIVESECURITY.COM

FORTINET REVELA QUE EL CIBERCRIMEN YA OPERA COMO UN ECOSISTEMA INDUSTRIALIZADO IMPULSADO POR IA



El Reporte de Amenazas 2026 de Fortinet revela que los hackers han dejado de lanzar campañas aisladas para operar como empresas semiestructuradas que usan agentes de IA. Gracias a estas herramientas, el tiempo de explotación de vulnerabilidades críticas se redujo drásticamente a un rango de entre 24 y 48 horas. Además, las víctimas confirmadas de ransomware crecieron un 389% debido a kits basados en IA como WormGPT y FraudGPT, afectando principalmente a los sectores de manufactura y finanzas.

Ante este escenario, Fortinet subraya la urgencia de adoptar defensas industrializadas impulsadas por IA y destaca operaciones como 'Tarjeta Roja 2.0', que logró desmantelar redes criminales globales.

FUENTE: FORTINET.COM

OLA DE CIBERATAQUES GOLPEA A LOS GOBIERNOS DE AMÉRICA LATINA CON FRECUENCIAS RÉCORD

Las agencias gubernamentales de América Latina sufren una oleada de ciberataques sin precedentes, registrando un promedio de 4,200 ofensivas semanales, una cifra que supera ampliamente la media global de otros sectores. Durante marzo de 2026, la crisis se intensificó con incidentes críticos, incluyendo el hackeo masivo con inteligencia artificial a nueve instituciones en México —exponiendo 195 millones de registros—, más de 23 millones de ataques contra el sector salud en Colombia y la parálisis del sistema de licencias de conducir en Puerto Rico.

Los expertos señalan que las principales vías de entrada son el robo de credenciales mediante phishing por correo electrónico y la explotación de sistemas públicos obsoletos, un panorama agravado por la escasez estructural de unos 350,000 profesionales de ciberseguridad en la región.

FUENTE: DARKREADING.COM

TARJETA ROJA: RECOMENDACIONES MUNDIAL 2026

PARA USUARIOS:

- Comprar boletos únicamente en plataformas oficiales.
- Verificar URLs antes de ingresar credenciales.
- No abrir enlaces sospechosos
- Activar autenticación multifactor (MFA)

PARA INSTITUCIONES:

- Implementar monitoreo continuo
- Actualizar sistemas y parches
- Capacitar al personal contra phishing
- Fortalecer protección DDoS
- Revisar accesos remotos y VPN

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.