Mainsoft®

BOLETÍN INFORMATIVO

#219 | Mayo 2026

Los hackers utilizaron IA para desarrollar el primer método conocido de evasión de autenticación de dos factores (2FA) de día cero para la explotación masiva.

Google reveló el lunes que identificó a un actor de amenazas desconocido que utilizaba una vulnerabilidad de día cero, la cual, según indicó, probablemente fue desarrollada con un sistema de inteligencia artificial (IA).

ver artículo >>

El troyano bancario TCLBANKER ataca plataformas financieras a través de gusanos de WhatsApp y Outlook.

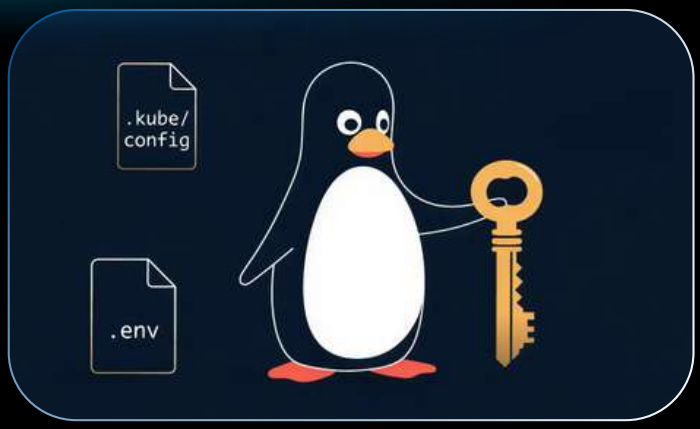
Los expertos en seguridad informática han detectado un troyano bancario brasileño, hasta ahora no documentado, denominado TCLBANKER , capaz de atacar 59 plataformas bancarias, de tecnología financiera y de criptomonedas.

ver artículo >>

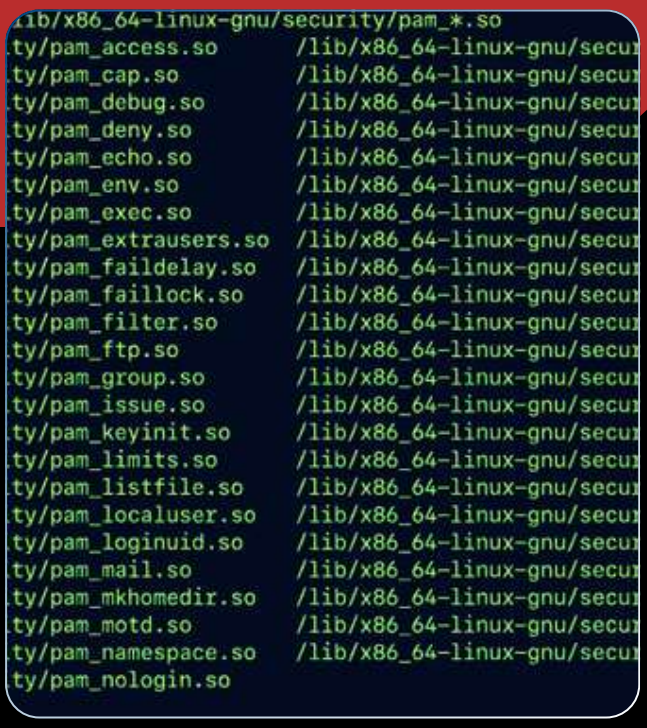
El troyano de acceso remoto Quasar Linux roba credenciales de desarrolladores para comprometer la cadena de suministro de software.

Un implante de Linux previamente no documentado, con nombre en clave Quasar Linux RAT (QLNX), está dirigido a los sistemas de los desarrolladores para establecer una base silenciosa y facilitar una amplia gama de funcionalidades posteriores a la intrusión, como la obtención de credenciales, el registro de pulsaciones de teclas, la manipulación de archivos, la monitorización del portapapeles y la creación de túneles de red.

ver artículo >>



INCIDENTES DE SISTEMAS



Una nueva puerta trasera para Linux, PamDOORa, utiliza módulos PAM para robar credenciales SSH.

Investigadores de ciberseguridad han revelado detalles de una nueva puerta trasera para Linux llamada PamDOORa , que está siendo anunciada en el foro ruso de ciberdelincuencia Rehub por 1.600 dólares por un actor de amenazas llamado "darkworm".

ver artículo >>

cPanel y WHM lanzan correcciones para tres nuevas vulnerabilidades: ¡Aplica el parche ahora!

cPanel ha publicado actualizaciones para solucionar tres vulnerabilidades en cPanel y Web Host Manager (WHM) que podrían ser explotadas para lograr la escalada de privilegios, la ejecución de código y la denegación de servicio.

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

Los desarrolladores de Linux sopesan la posibilidad de un "interruptor de apagado" de emergencia para funciones vulnerables del kernel.

Los desarrolladores del kernel de Linux están revisando una propuesta para un mecanismo de mitigación de riesgos de emergencia ("Killswitch") que permitiría a los administradores deshabilitar las funciones vulnerables del kernel en tiempo de ejecución.

ver artículo >>

Verdad envenenada: La silenciosa amenaza a la seguridad que se esconde tras la IA empresarial.

Los sistemas de IA empresariales pueden verse comprometidos por datos contaminados accidentalmente, ataques malintencionados o malas prácticas de higiene. La mayoría de las organizaciones desconocen la magnitud de esta superficie de ataque, o si ya están expuestas.

ver artículo >>

Resumen semanal: Rootkit de Linux, ladrón de criptomonedas de macOS, skimmers de WebSocket y más

Alguien volvió a envenenar una descarga de confianza, otro convirtió servidores en la nube en viviendas sociales, y algunos equipos siguen accediendo a sistemas con errores que deberían haber desaparecido hace años: las mismas vulnerabilidades de siempre, las mismas rutas de acceso deficientes, la misma sensación de "¿cómo es posible que esto siga abierto?".

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

El siguiente paso tras Mythos: Defenderse en un mundo donde se espera compromiso

Los sistemas basados en IA, como Mythos, están acelerando el descubrimiento de vulnerabilidades y reduciendo el tiempo entre la exposición y la explotación. Este blog analiza cómo deben adaptarse las estrategias de seguridad, centrándose en la detección temprana, la contención rápida y la limitación del impacto de las amenazas.

ver artículo >>

Guía de seguridad de claves de API de AWS Bedrock, parte 2: detección, prevención y respuesta.

Esta investigación, que constituye la segunda parte de una guía completa sobre la seguridad de las claves API de AWS Bedrock, se basa en los riesgos de las claves API de AWS Bedrock presentados en la primera parte para abarcar la detección, la prevención, la respuesta a incidentes y la migración a STS.

ver artículo >>

Red Hat Summit 2026: Impulsando operaciones inteligentes y automatizadas en cargas de trabajo de IA y nube híbrida.

Red Hat Summit es el evento insignia de Red Hat para líderes de TI, ingenieros de plataforma, desarrolladores y equipos de operaciones que crean y escalan entornos de nube híbrida modernos.

ver artículo >>

BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

HAZ CLICK

EVENTOS CERCANOS DE NUESTROS PARTNERS

DARKTRACE

Más Información

BeyondTrust

Más Información

IBM Gold Partner

Más Información