BOLETÍN INFORMATIVO N°197

SEPTIEMBRE 2025

ScarCruft utiliza el malware RokRAT en la Operación HanKook Phantom dirigida a académicos surcoreanos.

Investigadores de ciberseguridad han descubierto una nueva campaña de phishing realizada por el grupo de piratería informática vinculado a Corea del Norte llamado ScarCruft (también conocido como APT37) para distribuir un malware conocido como RokRAT.

Los atacantes abusan de la herramienta forense Velociraptor para implementar Visual Studio Code para la tunelización C2

Los investigadores de ciberseguridad han llamado la atención sobre un ciberataque en el que actores de amenazas desconocidos desplegaron una herramienta forense digital y de monitoreo de puntos finales de código abierto llamada Velociraptor , lo que ilustra el abuso continuo de software legítimo con fines maliciosos.

Amazon desmantela la campaña APT29 que abusa de la autenticación del código de dispositivo de Microsoft

Amazon dijo el viernes que detectó e interrumpió lo que describió como una campaña oportunista de abrevadero orquestada por los actores de APT29 vinculados a Rusia como parte de sus esfuerzos de recopilación de inteligencia.

Click Studios corrige vulnerabilidad de omisión de autenticación de Passwordstate en la página de acceso de emergencia

Click Studios, el desarrollador de la solución de gestión de contraseñas centrada en empresas Passwordstate, dijo que ha lanzado actualizaciones de seguridad para abordar una vulnerabilidad de omisión de autenticación en su software.

Investigadores descubren una falla en VS Code que permite a los atacantes republicar extensiones eliminadas con los mismos nombres

Investigadores de ciberseguridad han descubierto una vulnerabilidad en Visual Studio Code Marketplace que permite a los actores de amenazas reutilizar nombres de extensiones previamente eliminadas.

WhatsApp corrige un exploit de clic cero dirigido a dispositivos iOS y macOS

WhatsApp ha abordado una vulnerabilidad de seguridad en sus aplicaciones de mensajería para Apple iOS y macOS que, según dice, podría haber sido explotada en conjunto con una falla de Apple revelada recientemente en ataques de día cero dirigidos.

RECOMENDACIONES

LECTURA DE SEGURIDAD

GenAI está impulsando un fraude más inteligente, pero el trabajo en equipo fallido es el verdadero problema

Más del 80 % de las grandes empresas estadounidenses fueron blanco de fraudes de ingeniería social el año pasado, según el Informe de Fraude y Riesgos de Ingeniería Social 2025 de Trustmi . Casi la mitad de estas organizaciones reportaron pérdidas financieras directas, y muchos incidentes costaron más de $500,000.

Las técnicas APT del tifón salino se revelan en un nuevo informe

Un aviso detalla las actividades y técnicas utilizadas por el grupo de ciberespionaje Salt Typhoon, patrocinado por el Estado chino, que ha violado proveedores de telecomunicaciones, redes militares y agencias gubernamentales en los últimos años.

NOTICIAS DE

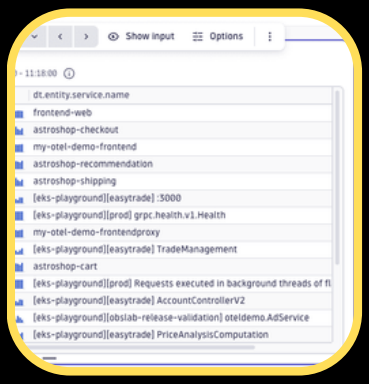
NUESTROS PARTNERS

IBM y AMD unen fuerzas para construir el futuro de la informática

Las empresas buscan fusionar aceleradores de IA, computadoras cuánticas y computación de alto rendimiento para ayudar a resolver una amplia gama de los problemas más difíciles del mundo.

Comprender el riesgo de correo electrónico empresarial (BEC): Por qué el correo electrónico sigue siendo el principal punto de entrada

Los actores de amenazas no necesitan exploits avanzados, solo un punto de entrada confiable: tu bandeja de entrada. Una vez que los atacantes obtienen acceso al correo electrónico, pueden eludir una autenticación de dos factores (A2F) débil, secuestrar el restablecimiento de contraseñas y suplantar identidades para robar dinero o datos confidenciales.



Novedades de la versión 1.322 de Dynatrace SaaS

Esta página presenta las nuevas funciones, cambios y correcciones de errores de la versión 1.322 de Dynatrace SaaS.

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