BOLETÍN INFORMATIVO N°206

NOVIEMBRE 2025

Investigadores descubren los troyanos para Android BankBot-YNRK y DeliveryRAT que roban datos financieros

Investigadores de ciberseguridad han arrojado luz sobre dos troyanos diferentes para Android, llamados BankBot-YNRK y DeliveryRAT , que son capaces de recopilar datos confidenciales de dispositivos comprometidos.

Un nuevo exploit "Brash" provoca el cierre instantáneo de los navegadores Chromium con una sola URL maliciosa

Una grave vulnerabilidad descubierta en el motor de renderizado Blink de Chromium puede ser explotada para provocar el bloqueo de muchos navegadores basados en Chromium en cuestión de segundos.

Investigadores exponen GhostCall y GhostHire: las nuevas cadenas de malware de BlueNoroff

Se ha observado que agentes de amenazas vinculados a Corea del Norte están atacando los sectores de Web3 y blockchain como parte de dos campañas gemelas conocidas como GhostCall y GhostHire .

INCIDENTES DE

SISTEMAS

Las vulnerabilidades gráficas de Windows permiten a atacantes remotos ejecutar código arbitrario.

Múltiples vulnerabilidades en la interfaz de dispositivo gráfico (GDI) de Microsoft, un componente central del sistema operativo Windows responsable de la representación gráfica.

Múltiples vulnerabilidades de Jenkins: omisión de la autenticación SAML y permisos del plugin del servidor MCP

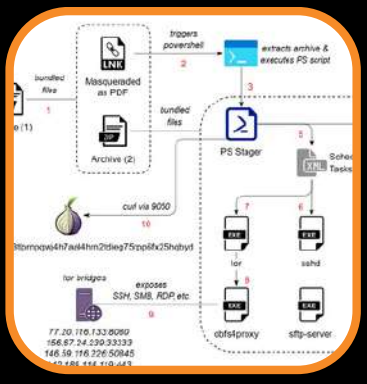
El proyecto Jenkins publicó el Aviso de Seguridad 2025-10-29 el 28 de octubre de 2025, revelando múltiples vulnerabilidades en 13 complementos que impulsan el popular servidor de automatización de código abierto.

La actualización 24H2/25H2 de Windows 11 provoca que el Administrador de tareas permanezca activo después de cerrarlo.

Microsoft ha publicado una actualización no relacionada con la seguridad para las versiones 24H2 y 25H2 de Windows 11 que introduce un error inusual que afecta a una de las utilidades más esenciales del sistema operativo.

RECOMENDACIONES

LECTURA DE SEGURIDAD



Una campaña de ciberespionaje que imita las tácticas, técnicas y procedimientos (TTP) del ataque Sandworm afecta a las fuerzas armadas rusas y bielorrusas.

Investigadores de seguridad de Cyble y Seqrite han detectado una campaña de spear-phishing dirigida a comprometer a personal militar ruso y bielorruso utilizando documentos de temática militar como señuelo.

Resumen semanal: Lazarus ataca Web3, se filtran las TEE de Intel/AMD, herramienta de filtración de la Dark Web y más

Los ciberataques son cada vez más sofisticados y difíciles de detener. Esta semana, los hackers utilizaron herramientas engañosas, manipularon sistemas de confianza y aprovecharon rápidamente nuevas vulnerabilidades de seguridad, algunas apenas unas horas después de haber sido detectadas.

Una nueva forma de concebir el enfoque de confianza cero para cargas de trabajo

Las credenciales estáticas han sido un punto débil en la seguridad de la nube durante años. Un nuevo estudio de investigadores de SentinelOne aborda directamente este problema con un modelo práctico para autenticar cargas de trabajo sin secretos de larga duración.

NOTICIAS DE

NUESTROS PARTNERS

Aplique parches de forma más inteligente, no más ardua: Ahora, empoderamos a los equipos de seguridad con agentes de contexto de amenazas alineados con el negocio.

Este blog presenta las nuevas innovaciones de Darktrace / Gestión Proactiva de la Exposición, que aportan precisión y claridad a la priorización de vulnerabilidades.

Presentación de aplicaciones de Dynatrace®: Observabilidad de Phenisys MS Teams

Phenisys, una consultora de TI francesa y socio Premier de ventas de Dynatrace®, se ha dedicado a la observabilidad de TI y de aplicaciones durante más de 20 años.

Las misteriosas vías de privilegios que acechan en su entorno de TI... y cómo combatirlas.

Los ciberdelincuentes son cada vez más sigilosos en la forma en que explotan identidades y privilegios, a menudo a través de rutas ocultas e indirectas.

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