BOLETÍN INFORMATIVO

#233 | Octubre 2026

Los atacantes de GhostAction instalan un programa malicioso para robar credenciales, disfrazado de fuente tipográfica, en 94 repositorios de GitHub.



El responsable del ataque a la cadena de suministro de GhostAction ha ampliado sus operaciones, pasando de inyectar flujos de trabajo maliciosos de GitHub Actions en proyectos comprometidos a realizar ataques de phishing contra desarrolladores de código abierto e instalar un malware de robo de datos disfrazado dentro de un archivo de fuente falso.

ver artículo >>



Investigadores demuestran una vulnerabilidad de OpenBSD Root que explota un fallo de memoria compartida de 37 años de antigüedad.

Una vulnerabilidad de escalada de privilegios local publicada hoy obtiene acceso de administrador en OpenBSD 7.9 al combinar un desbordamiento de enteros de aproximadamente 37 años de antigüedad con una falla de kernel independiente, eludiendo la aleatorización de direcciones de kernel KARL de OpenBSD y sus protecciones de hardware SMAP y SMEP.

ver artículo >>

Hackers vinculados a China explotaron una vulnerabilidad de día cero de BeyondTrust para tomar el control de los servidores de soporte remoto.



El grupo de ciberespionaje vinculado a China, conocido como Armory Castle (anteriormente UNC5221 o Warp Panda), explotó una vulnerabilidad de seguridad recientemente descubierta en BeyondTrust Remote Support (anteriormente Bomgar) como una vulnerabilidad de día cero a finales de agosto de 2026.

ver artículo >>



INCIDENTES DE SISTEMAS



Google corrige 10 vulnerabilidades de Chrome, incluyendo un fallo de corrupción de memoria detectado en la IA Claude.

Google lanzó una actualización de seguridad estable para Chrome que corrige 10 vulnerabilidades en Windows, Mac y Linux, incluyendo una falla de corrupción de memoria DOM de alta gravedad reportada por Xinyang Ge de Anthropic con Claude AI.

ver artículo >>



Se ha publicado una prueba de concepto (PoC) para explotar una vulnerabilidad crítica de ejecución remota de código (RCE) en GitLab (CVE-2026-97229).

Una prueba de concepto pública (PoC) para CVE-2026-97229, publicada por el investigador Jonah Burgess, muestra cómo se podría utilizar un fallo en el compilador de expresiones regulares de CI/CD de GitLab para ejecutar comandos en un servidor vulnerable.

ver artículo >>



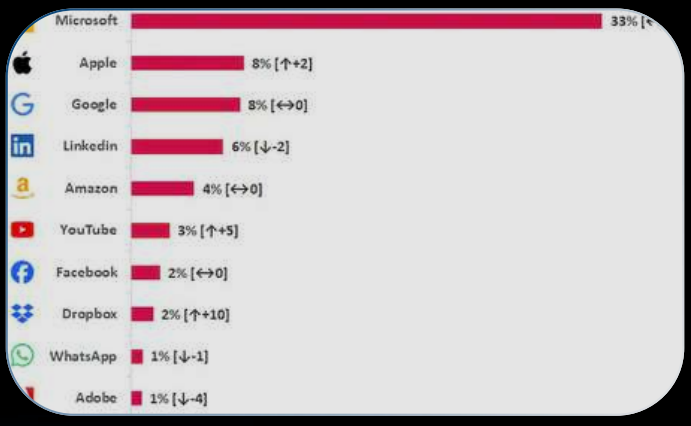
RECOMENDACIONES DE LECTURA DE SEGURIDAD

La presión del ransomware ahora llega a los hogares y familias de los empleados.

Los atacantes de ransomware amenazaron a familiares o amigos de los empleados en el 37 % de las organizaciones encuestadas para el Informe de Riesgos de Ransomware 2026 de Semperis . La encuesta abarcó a 1200 profesionales de TI y seguridad en organizaciones que habían sufrido al menos un ataque de ransomware exitoso

ver artículo >>





Los ciberdelincuentes prefieren Microsoft a Apple y Google en los ataques de phishing de marca.

Microsoft representó el 33% de los intentos de suplantación de marca registrados por Check Point Research en el tercer trimestre de 2026, un aumento con respecto al 23% del trimestre anterior y aproximadamente cuatro veces la cuota de cualquier otra marca

ver artículo >>

Resumen semanal: 98 vulnerabilidades de día cero, agentes de IA descontrolados, robo de criptomonedas por valor de 100 millones de dólares, 700 supermercados afectados y más.

Los peores problemas no siempre vienen con aviso. A veces surgen a través de un servicio en el que todos confían, un dispositivo que alguien compró o un sistema que nadie se molestó en revisar. Cuando algo empieza a fallar, el daño puede ser irreparable.

ver artículo >>





NOTICIAS DE NUESTROS PARTNERS



Bot CikaBika: Dentro de un RAT de Discord

Investigadores de Darktrace investigan CikaBika Bot, un troyano de acceso remoto basado en Rust que se distribuye mediante un señuelo con temática de documento. El malware utiliza un cargador Nim, elude el UAC de PowerShell y manipula el orden de búsqueda de DLL antes de aprovechar Discord para el comando y control (C2), el reconocimiento, la ejecución remota y la exfiltración de datos a través de ngrok, según la actividad maliciosa observada.

ver artículo >>

ARMORY CASTLE y BT26-05: Lo que los equipos de seguridad deben saber.

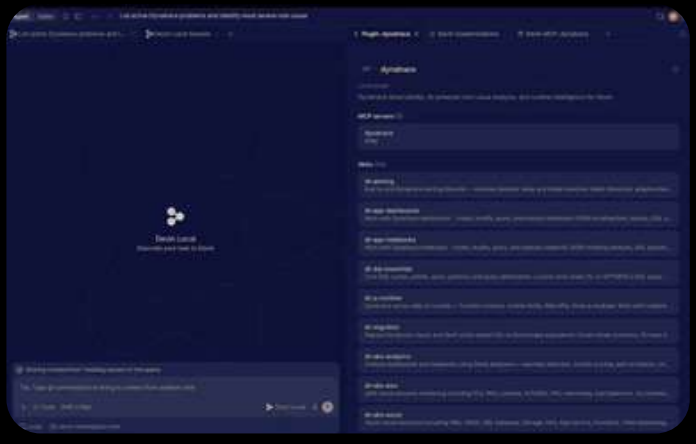
BeyondTrust proporciona información contextual sobre ARMORY CASTLE y el aviso de seguridad BT26-05, incluyendo lo que los equipos de seguridad necesitan saber sobre la vulnerabilidad, los productos afectados, las directrices para su corrección y los últimos hallazgos confirmados.

ver artículo >>

Devin Oncall y Dynatrace: Llevando la inteligencia en tiempo de ejecución a la respuesta autónoma ante incidentes.

Estamos viendo surgir un nuevo desafío a medida que el desarrollo de software asistido por IA se vuelve más común: los agentes autónomos pueden generar código, proponer correcciones e incluso abrir solicitudes de extracción, pero aún necesitan una forma confiable de comprender lo que está sucediendo en producción.

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