BOLETÍN INFORMATIVO

Mainsoft

N°170

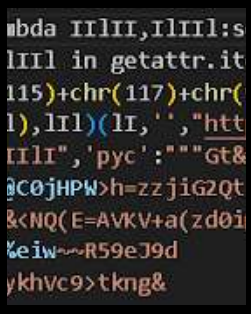
ENERO 2025

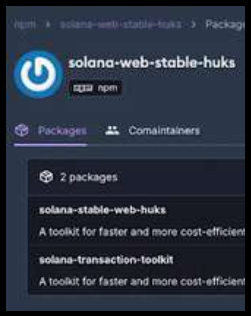
Investigadores encuentran un exploit que permite NTLMv1 a pesar de las restricciones de Active Directory

Los investigadores de ciberseguridad han descubierto que la política de grupo de Microsoft Active Directory, diseñada para deshabilitar NT LAN Manager (NTLM) v1, se puede eludir fácilmente mediante una configuración incorrecta.

Un malware basado en Python permite al ransomware RansomHub explotar fallas de la red

Los investigadores de ciberseguridad han detallado un ataque que involucró a un actor de amenazas que utilizó una puerta trasera basada en Python para mantener un acceso persistente a los puntos finales comprometidos y luego aprovechó este acceso para implementar el ransomware RansomHub en toda la red objetivo.





Los piratas informáticos implementan paquetes npm maliciosos para robar claves de la billetera Solana a través de SMTP de Gmail

Los investigadores de ciberseguridad han identificado tres conjuntos de paquetes maliciosos en el repositorio npm y Python Package Index (PyPI) que vienen con capacidades para robar datos e incluso eliminar datos confidenciales de los sistemas infectados

INCIDENTES DE SISTEMAS

Un investigador descubre fallas críticas en varias versiones de Ivanti Endpoint Manager

Ivanti ha implementado actualizaciones de seguridad para abordar varias fallas de seguridad que afectan a Avalanche, Application Control Engine y Endpoint Manager (EPM), incluidos cuatro errores críticos que podrían provocar la divulgación de información.

Vulnerabilidad de día cero del sistema de archivos de registro común de Windows (CVE-2024-49138) explotada

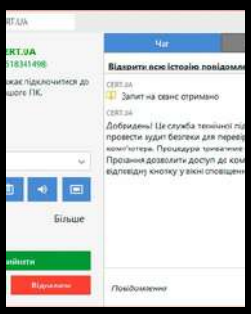
Una vulnerabilidad de día cero en el controlador del Sistema de archivos de registro común de Windows (CLFS), designada como CVE-2024-49138.

Vulnerabilidad de Microsoft Configuration Manager permite ejecución remota de código – PoC publicado

Se ha identificado una vulnerabilidad crítica, CVE-2024-43468, en Microsoft Configuration Manager (ConfigMgr), que representa un grave riesgo de seguridad para las organizaciones que dependen de este software de gestión de sistemas ampliamente utilizado.

CERT-UA advierte contra las solicitudes de "auditoría de seguridad" a través de AnyDesk

Los atacantes se hacen pasar por el Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT-UA) a través de AnyDesk para obtener acceso a las computadoras objetivo.



RECOMENDACIONES

LECTURA DE SEGURIDAD

Se puede acceder a archivos cifrados con BitLocker de Windows 11 sin desmontar la computadora portátil

Los investigadores demostraron cómo los atacantes pueden eludir sus protecciones sin manipular físicamente el dispositivo. El exploit, conocido como “bitpixie” (CVE-2023-21563), fue presentado en el Chaos Communication Congress (38C3) por el investigador de seguridad Thomas Lambertz

Resumen semanal: datos de AWS S3 cifrados sin ransomware, se filtraron datos de 15.000 firewalls de Fortinet

A continuación, se ofrece un resumen de algunas de las noticias, artículos, entrevistas y vídeos más interesantes de la semana pasada

El nuevo kit de phishing 'Sneaky 2FA' ataca las cuentas de Microsoft 365 con el código de evasión de 2FA

Los investigadores de ciberseguridad han detallado un nuevo kit de phishing "adversario-en-el-medio" (AitM) que es capaz de acceder a cuentas de Microsoft 365 con el objetivo de robar credenciales y códigos de autenticación de dos factores (2FA) desde al menos octubre de 2024.

NOTICIAS DE

NUESTROS PARTNERS

Cómo reinventar su SOC: cómo lograr una seguridad de red proactiva

Esta publicación de blog brinda asesoramiento sobre cómo los equipos de seguridad pueden avanzar hacia la detección e investigación autónomas de nuevas amenazas, reduciendo la fatiga de alertas y permitiendo una respuesta a las amenazas personalizada y en tiempo real.

IBM adquirirá Applications Software Technology LLC y reforzará la experiencia de Oracle para ayudar a los clientes a transformar sus operaciones

IBM anunció su intención de adquirir Applications Software Technology LLC 1 , una consultora global de Oracle. Applications Software Technology aporta una profunda experiencia en el impulso de transformaciones empresariales con Oracle Cloud Applications, incluso para clientes del sector público, como el gobierno local y la educación primaria y secundaria.

Ingiera y enriquezca los hallazgos de seguridad entregados por Amazon EventBridge con Dynatrace

Dynatrace se integra con Amazon EventBridge para romper los silos entre los equipos de DevSecOps al unificar los hallazgos de seguridad a lo largo del ciclo de vida del desarrollo de software (SDLC) y enriquecerlos con el contexto de tiempo de ejecución.

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

CYLANCE — Más Información

IBM Gold Partner — Más Información