BOLETÍN INFORMATIVO

Mainsoft

N°162

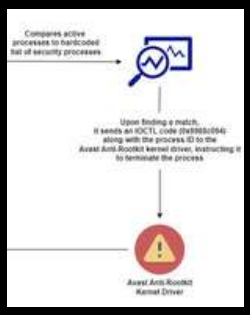
NOVIEMBRE 2024

Los puntos ciegos de ciberseguridad en las herramientas IaC y PaC exponen las plataformas en la nube a nuevos ataques

Los investigadores de ciberseguridad han revelado dos nuevas técnicas de ataque contra herramientas de infraestructura como código (IaC) y política como código (PaC) como Terraform y Open Policy Agent (OPA) de HashiCorp, que aprovechan lenguajes dedicados y específicos del dominio (DSL) para violar las plataformas en la nube y exfiltrar datos.

Investigadores descubren malware que utiliza BYOVD para eludir las protecciones antivirus

Los investigadores de ciberseguridad han descubierto una nueva campaña maliciosa que aprovecha una técnica llamada Bring Your Own Vulnerable Driver (BYOVD) para desactivar las protecciones de seguridad y, en última instancia, obtener acceso al sistema infectado.



Advertencia: Más de 2000 dispositivos de Palo Alto Networks han sido hackeados en una campaña de ataques en curso

Se estima que alrededor de 2.000 dispositivos de Palo Alto Networks han sido comprometidos como parte de una campaña que abusa de las fallas de seguridad recientemente reveladas que han sido objeto de explotación activa.

Ataque PyPI: ChatGPT y suplantadores de identidad de Claude distribuyen JarkaStealer a través de bibliotecas Python

Investigadores de ciberseguridad han descubierto dos paquetes maliciosos cargados en el repositorio Python Package Index (PyPI) que se hacían pasar por modelos de inteligencia artificial (IA) populares como OpenAI ChatGPT y Anthropic Claude para entregar un ladrón de información llamado JarkaStealer.

INCIDENTES DE SISTEMAS

Wireshark 4.4.2: actualizaciones de seguridad, corrección de errores, compatibilidad con protocolos actualizada

Wireshark, el popular analizador de protocolos de red, ha llegado a la versión 4.4.2. Se utiliza para resolución de problemas, análisis, desarrollo y educación.

Google expone GLASSBRIDGE: una red de sitios de noticias falsas con influencia pro-China

Las agencias gubernamentales y organizaciones no gubernamentales de Estados Unidos se han convertido en el objetivo de un naciente actor de amenaza estatal chino conocido como Storm-2077.

Microsoft, Meta y el Departamento de Justicia desbaratan el cibercrimen y las redes fraudulentas a nivel mundial

Meta Platforms, Microsoft y el Departamento de Justicia de EE. UU. (DoJ) han anunciado acciones independientes para abordar el ciberdelito e interrumpir los servicios que posibilitan estafas, fraudes y ataques de phishing.

Resumen semanal: vulnerabilidades de día cero explotadas en los firewalls de Palo Alto Networks y dos puertas traseras de Linux desconocidas identificadas

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

RECOMENDACIONES

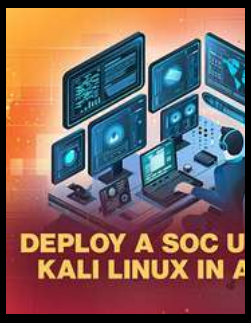
LECTURA DE SEGURIDAD

Volar bajo el radar: técnicas de evasión de seguridad

Profundice en la evolución de las técnicas de evasión de phishing y malware y comprenda cómo los atacantes utilizan métodos cada vez más sofisticados para eludir las medidas de seguridad.

AI Kuru, ciberseguridad y computación cuántica

A medida que continuamos delegando más operaciones de infraestructura a la inteligencia artificial (IA), las computadoras cuánticas están avanzando hacia el día Q (es decir, el día en que las computadoras cuánticas puedan romper los métodos de cifrado actuales). Esto podría comprometer la seguridad de las comunicaciones digitales, así como los sistemas de control autónomos que utilizan IA y ML para tomar decisiones.



Implementar un SOC con Kali Linux en AWS

El proyecto Kali SOC en AWS es una implementación basada en Terraform que permite la implementación de un Centro de operaciones de seguridad (SOC) en AWS, utilizando el conjunto de herramientas Kali Linux para las actividades del equipo púrpura. Este entorno es ideal para perfeccionar las habilidades en operaciones de seguridad, detección de amenazas, respuesta a incidentes y escenarios de capacitación.

Cómo desbloquear la seguridad de Google Workspace: ¿está haciendo lo suficiente para proteger sus datos?

Google Workspace se ha convertido rápidamente en la columna vertebral de la productividad de las empresas de todo el mundo, ya que ofrece una suite integral con herramientas de colaboración, almacenamiento en la nube y correo electrónico. Este enfoque de plataforma única facilita que los equipos se conecten y trabajen de manera eficiente, sin importar dónde se encuentren, lo que permite una transformación digital fluida que es escalable y adaptable.

NOTICIAS DE

NUESTROS PARTNERS

IBM y Pasqal planean expandir la iniciativa de supercomputación centrada en lo cuántico

IBM (NYSE: IBM) y Pasqal anunciaron una actualización de su colaboración prevista para construir nuevos marcos integrados para la supercomputación centrada en lo cuántico con Qiskit, el software cuántico de mayor rendimiento del mundo.

Darktrace lidera el futuro de la detección y respuesta en red con reconocimiento de KuppingerCole

Darktrace acaba de recibir el título de "Líder general" en el informe Leadership Compass 2024 de KuppingerCole para detección y respuesta de redes (NDR). ¿Por qué? Nuestra inteligencia artificial de autoaprendizaje y la automatización inteligente hacen que abordar las amenazas sea más rápido y más fácil, lo que ayuda a los equipos de seguridad a mantenerse a la vanguardia.

Dynatrace se une a la Asociación de Seguridad Inteligente de Microsoft

A medida que las organizaciones adoptan más tecnologías nativas de la nube, el riesgo (y las consecuencias) de los ciberataques también aumentan. Este riesgo creciente amplifica la necesidad de soluciones de seguridad confiables que se integren con los sistemas existentes. Por eso, estamos orgullosos de anunciar que Dynatrace se ha unido a la Asociación de Seguridad Inteligente de Microsoft (MISA).

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