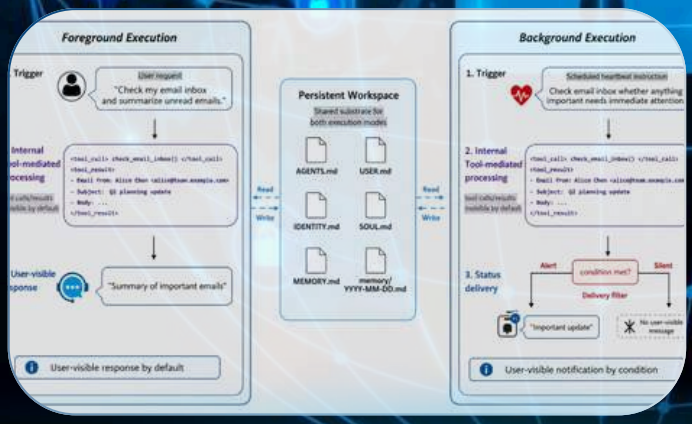
BOLETÍN INFORMATIVO

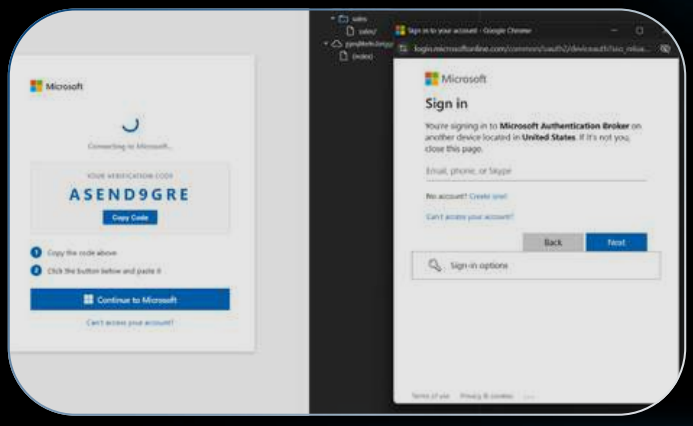
#228 | Julio 2026

El nuevo ataque MemGhost implanta falsos recuerdos persistentes en agentes de IA mediante un solo correo electrónico.

Si le das a un asistente de IA memoria y acceso a tu bandeja de entrada, le estás dando a un atacante la oportunidad de reescribir lo que cree saber sobre ti. Un solo correo electrónico puede engañar a ese agente para que guarde un "dato" falso sobre el usuario, oculte el cambio y manipule discretamente sus respuestas en sesiones posteriores

ver artículo >>





Forg365 PhaaS ataca a Microsoft 365 con robo de código de dispositivo y sesión AitM.

Una nueva operación de phishing como servicio (PhaaS, por sus siglas en inglés) llamada Forg365 está utilizando una combinación de phishing mediante código de dispositivo , tácticas de adversario en el medio (AitM, por sus siglas en inglés), evasión de antibots, creación de señuelos asistida por inteligencia artificial (IA) y operaciones de buzón de correo posteriores al compromiso dirigidas a cuentas de Microsoft 365.

ver artículo >>

El nuevo RAT MODBEACON utiliza transmisión gRPC para el tráfico C2 cifrado.

Se ha atribuido al grupo de ciberdelincuentes vinculado a China conocido como Silver Fox la creación de un nuevo troyano de acceso remoto (RAR) basado en Rust llamado MODBEACON

ver artículo >>

INCIDENTES DE SISTEMAS

URGENTE: Progress advierte a los clientes de ShareFile que apaguen los controladores de zona de almacenamiento debido a una amenaza de seguridad.

Progress Software ha pedido a los clientes de ShareFile que apaguen los servidores Windows que ejecutan sus Storage Zone Controllers, confirmando a The Hacker News que está respondiendo a una "amenaza de seguridad externa creíble".

ver artículo >>

Los instaladores falsos de 7-Zip convierten los dispositivos en nodos proxy residenciales.

Investigadores de ciberseguridad han revelado detalles de un nuevo actor de amenazas denominado Lurking Lizard, que ha estado operando un negocio de proxies residenciales maliciosos de extremo a extremo utilizando una infraestructura que comprende más de 230 dominios similares.

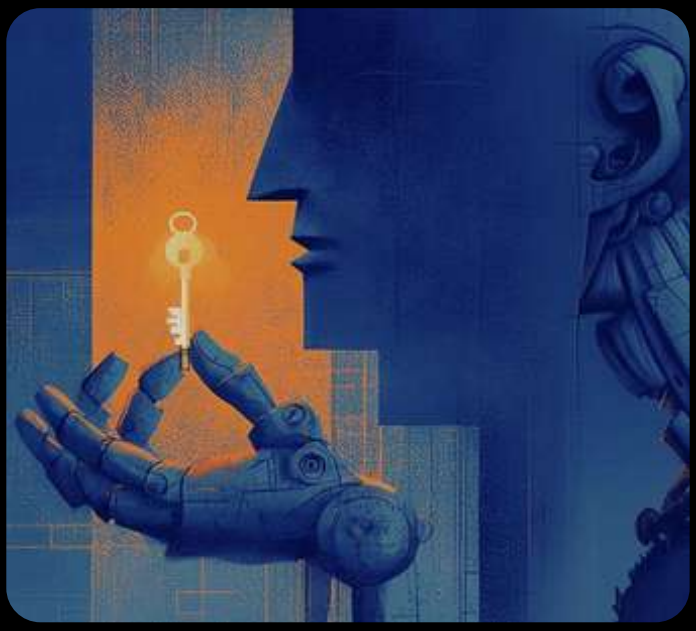
ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

Negociador de ransomware que traicionó a sus clientes fue condenado a 70 meses de prisión.

Un antiguo negociador de ransomware de la empresa de respuesta a incidentes DigitalMint ha sido condenado a 70 meses de prisión tras admitir que compartió información confidencial de clientes con el grupo de ransomware BlackCat y que posteriormente ayudó a llevar a cabo ataques de ransomware.

ver artículo >>



Los identificadores de cliente OAuth falsos están ayudando a los atacantes a eludir los registros de inicio de sesión.

Los atacantes que realizan enumeraciones de cuentas contra inquilinos de la nube de Microsoft han añadido un paso que les permite evitar que sus sondeos queden registrados en la telemetría habitual. Suplantan el ID de cliente de OAuth, el identificador único global asignado a una aplicación y que se transmite client_iden una solicitud de autenticación.

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

Seguridad después de las firmas: Operando en un mundo de explotación de la divulgación previa a la CVE, límites de confianza colapsados y sistemas autónomos

A medida que la IA transforma el panorama de amenazas, los atacantes explotan vulnerabilidades con mayor rapidez, abusan de identidades de confianza y utilizan herramientas e integraciones basadas en IA para operar a gran escala.

ver artículo >>

Dynatrace planea cumplir con la norma FedRAMP Clase D (Alta): Por qué es importante para la planificación estratégica de la agencia.

Dynatrace tiene previsto obtener la certificación FedRAMP Clase D (Alta), basándose en su certificación FedRAMP Moderada ya existente, establecida en 2020.

ver artículo >>

IBM y Red Hat amplían Lightwell con nuevas ofertas para construir la infraestructura de confianza para el código abierto en la era de la IA.

IBM (NYSE: IBM) y Red Hat anunciaron hoy el lanzamiento comercial de Lightwell, que ofrece remediación automatizada de vulnerabilidades a gran escala mediante dos ofertas: Lightwell Network y Lightwell Clearinghouse Premier.

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