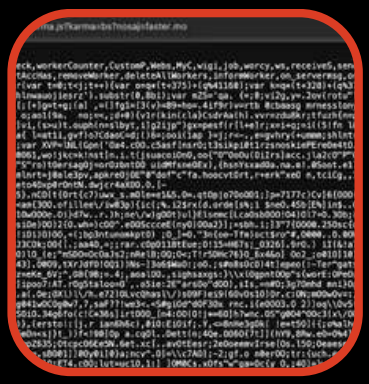
BOLETÍN INFORMATIVO N°191

JULIO 2025

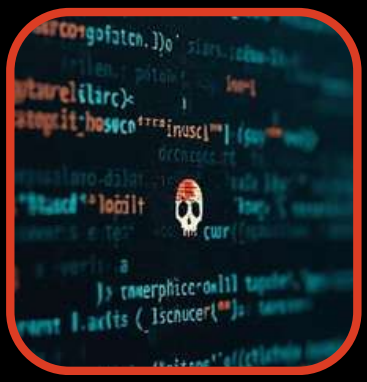


3.500 sitios web pirateados para minar criptomonedas en secreto mediante JavaScript oculto y tácticas WebSocket

Una nueva campaña de ataque ha comprometido más de 3.500 sitios web en todo el mundo con mineros de criptomonedas JavaScript, lo que marca el regreso de los ataques de cryptojacking basados en navegador que alguna vez se popularizaron por empresas como CoinHive .

CERT-UA descubre malware LAMEHUG vinculado a APT28 y utiliza LLM para una campaña de phishing

El Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT-UA) ha revelado detalles de una campaña de phishing diseñada para distribuir un malware con nombre en código LAMEHUG .



Los piratas informáticos utilizan repositorios de GitHub para alojar malware Amadey y ladrones de datos, eludiendo los filtros.

Los actores de amenazas están aprovechando los repositorios públicos de GitHub para alojar cargas maliciosas y distribuirlas a través de Amadey como parte de una campaña observada en abril de 2025.