Protección y robo de identidad mediante IA en 2025

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Introducción

La inteligencia artificial (IA) ha revolucionado la ciberseguridad, pero también ha amplificado los riesgos:

- Según datos recientes publicados por un estudio de Signicat, el 42,5% de los intentos de fraude en 2024 utilizaron IA
- El 50% del fraude documental se basa en herramientas de IA generativa, segun Infosol.

Por otro lado, la IA también es clave para la defensa:

- Segun Redseguridad, ell 70% de las empresas emplean sistemas de autenticación avanzada o análisis de comportamiento para defenderse.

Este artículo explora las herramientas más peligrosas de ataque, rodeadas en rojo, y las soluciones más eficaces de defensa, rodeadas en azul, destacando cómo la IA se ha convertido en un arma de doble filo.

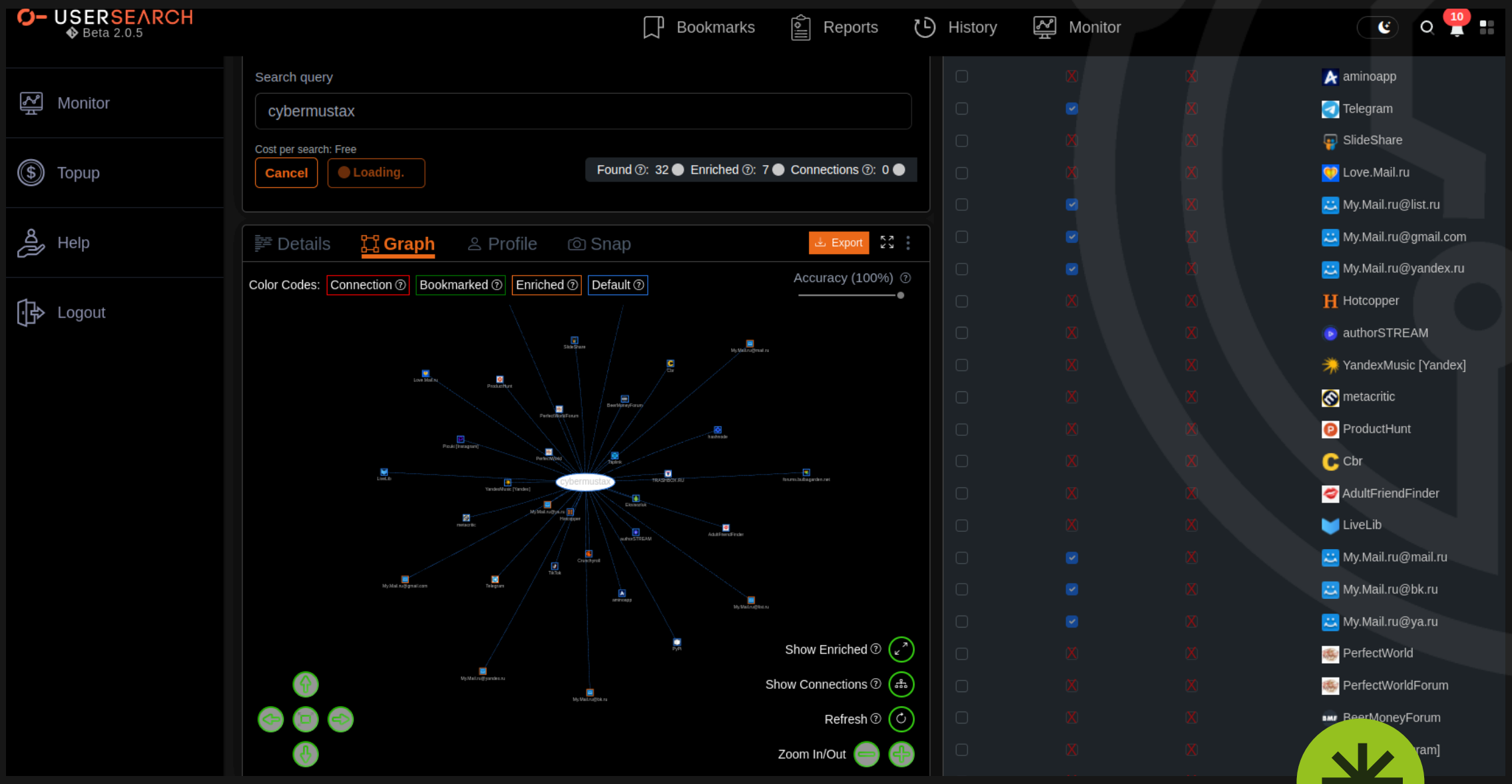
¡Comenzamos!

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Identidades sintéticas con UserSearch.ai

REDTEAM



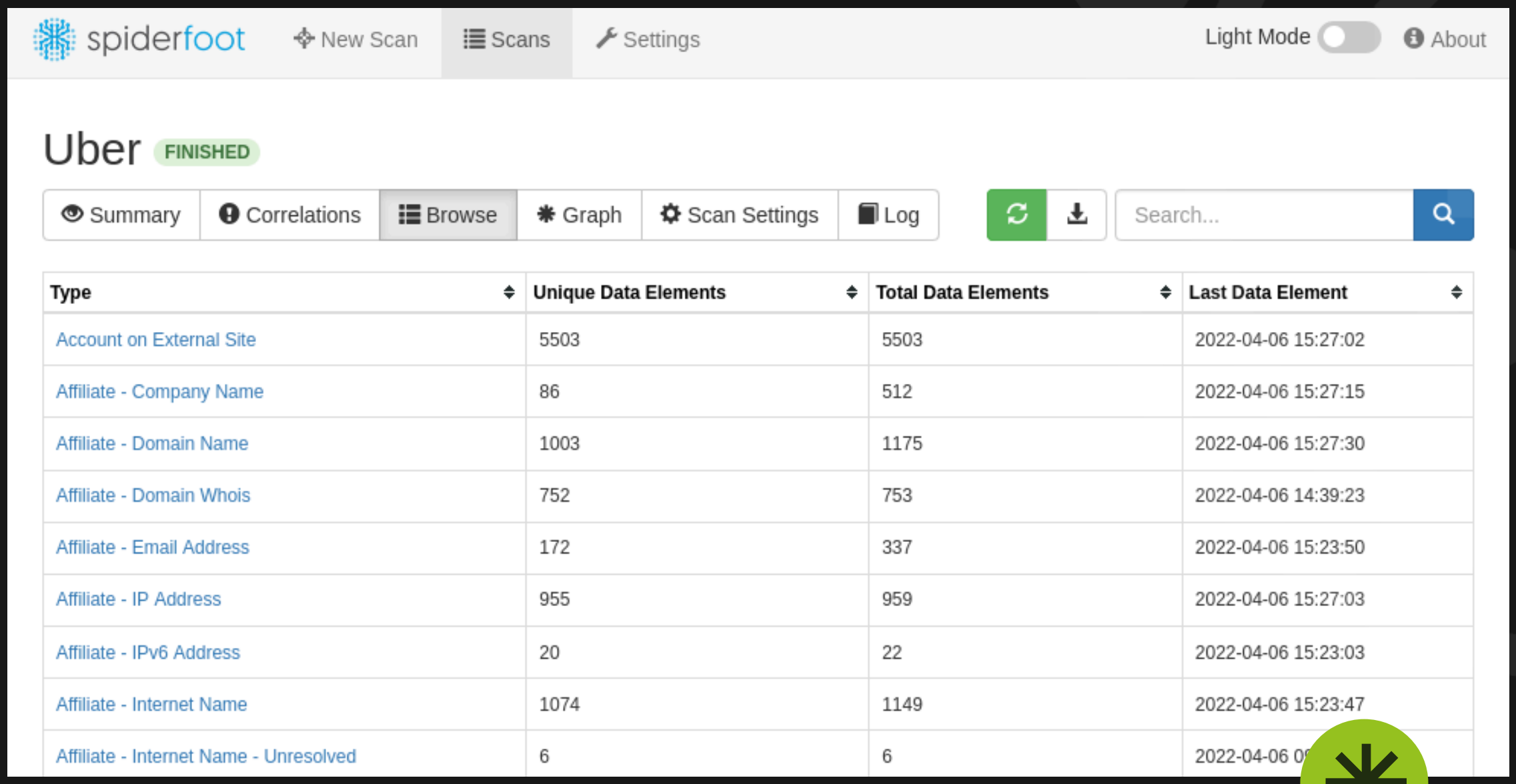
Recopila datos de redes sociales y bases públicas para crear identidades falsas. El 30% de los datos expuestos en redes sociales son explotados por herramientas como UserSearch.AI

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Identidades sintéticas con SpiderFoot

BLUETEAM



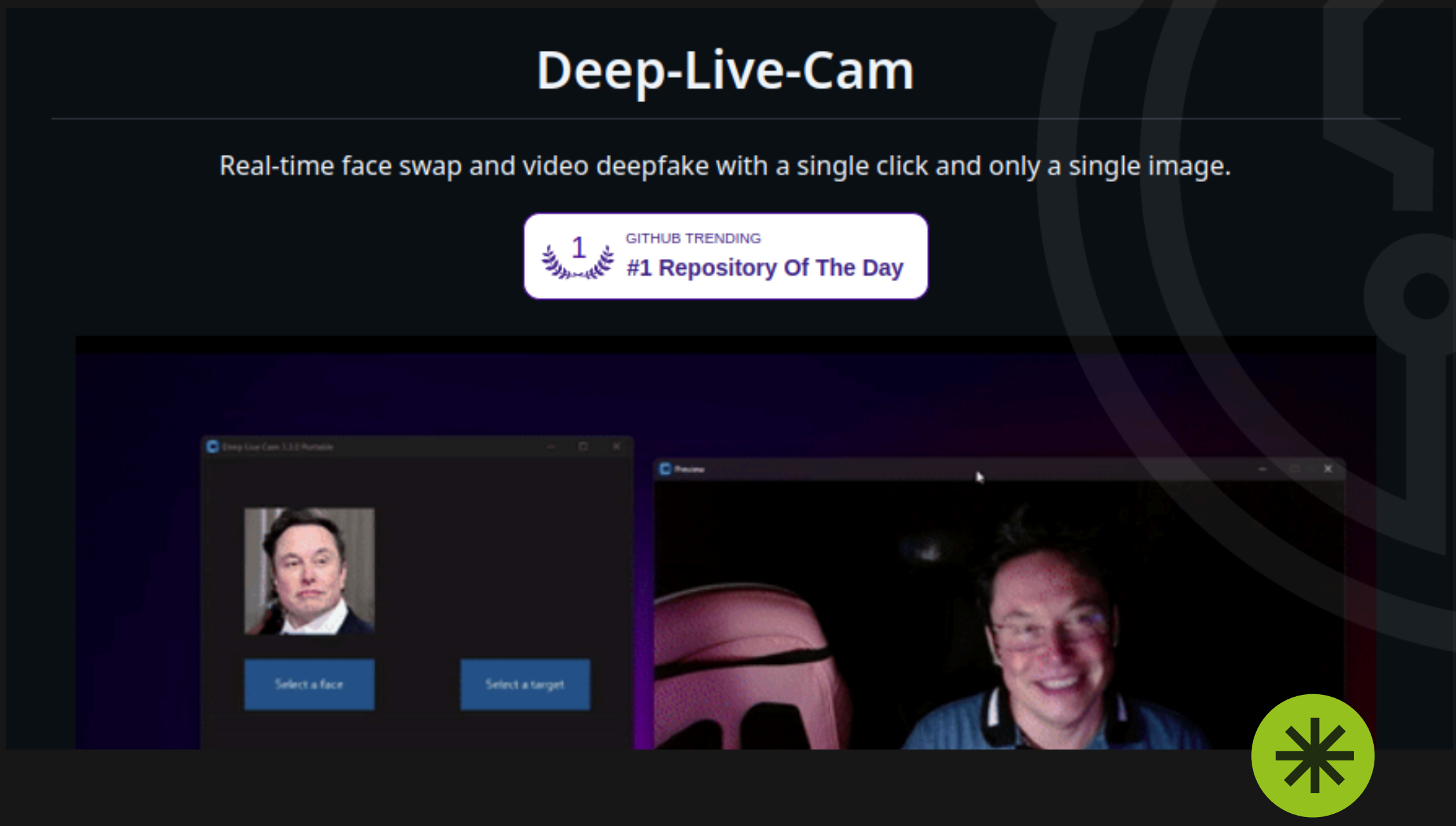
Analiza fugas de datos mediante OSINT (Inteligencia de Fuentes Abiertas). Identifica exposición de información personal antes de que sea usada para ataques.

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Deepfake en vivo con Deep-Live-Cam

REDTEAM



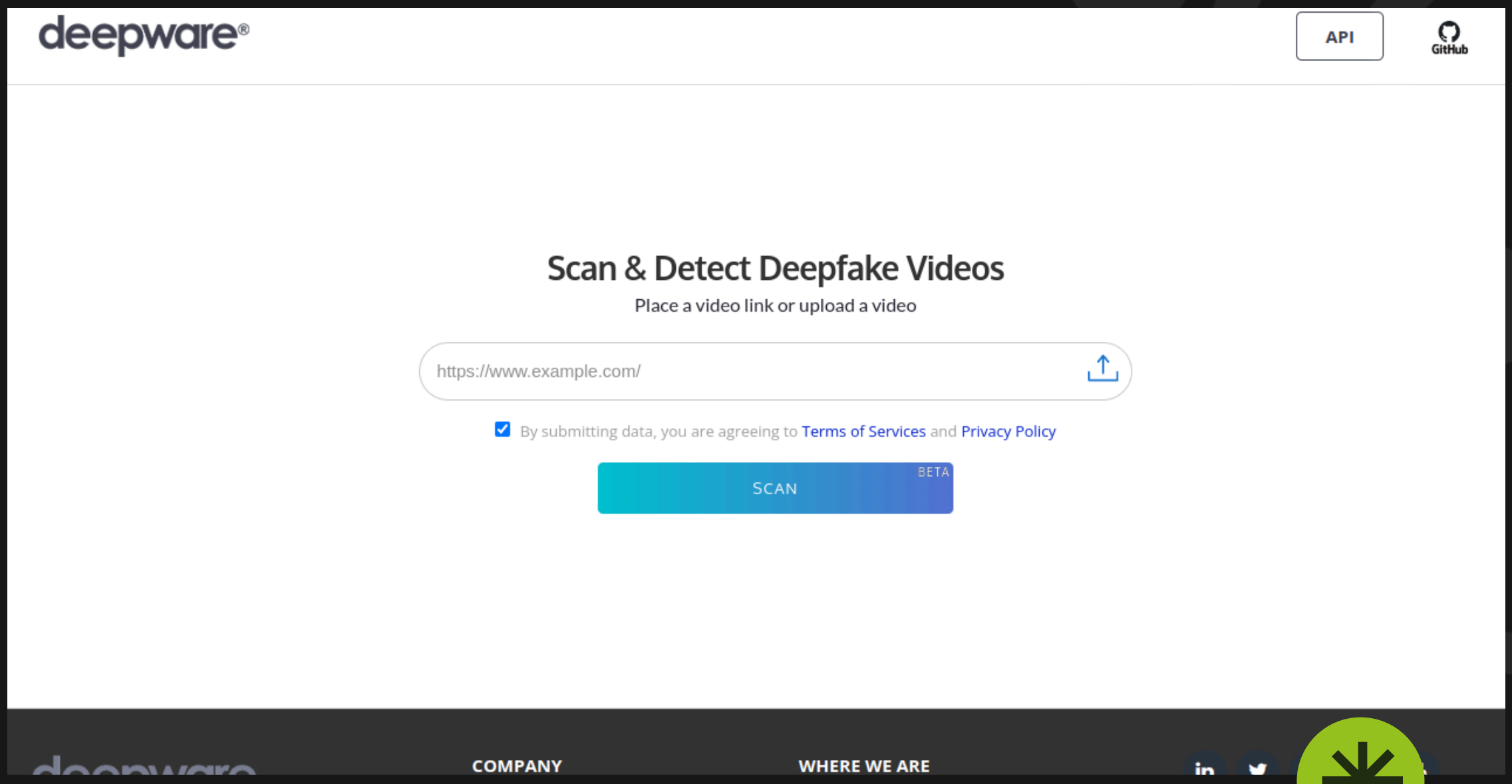
Genera videos falsos para engañar a víctimas, incluso en tiempo real con la camara web. Vídeos falsos de CEOs solicitando transferencias millonarias. Los ataques con cámaras virtuales (usadas en deepfakes) aumentaron un 2.665% en 2025

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Deepfake en vivo con Deepware Scanner

BLUETEAM



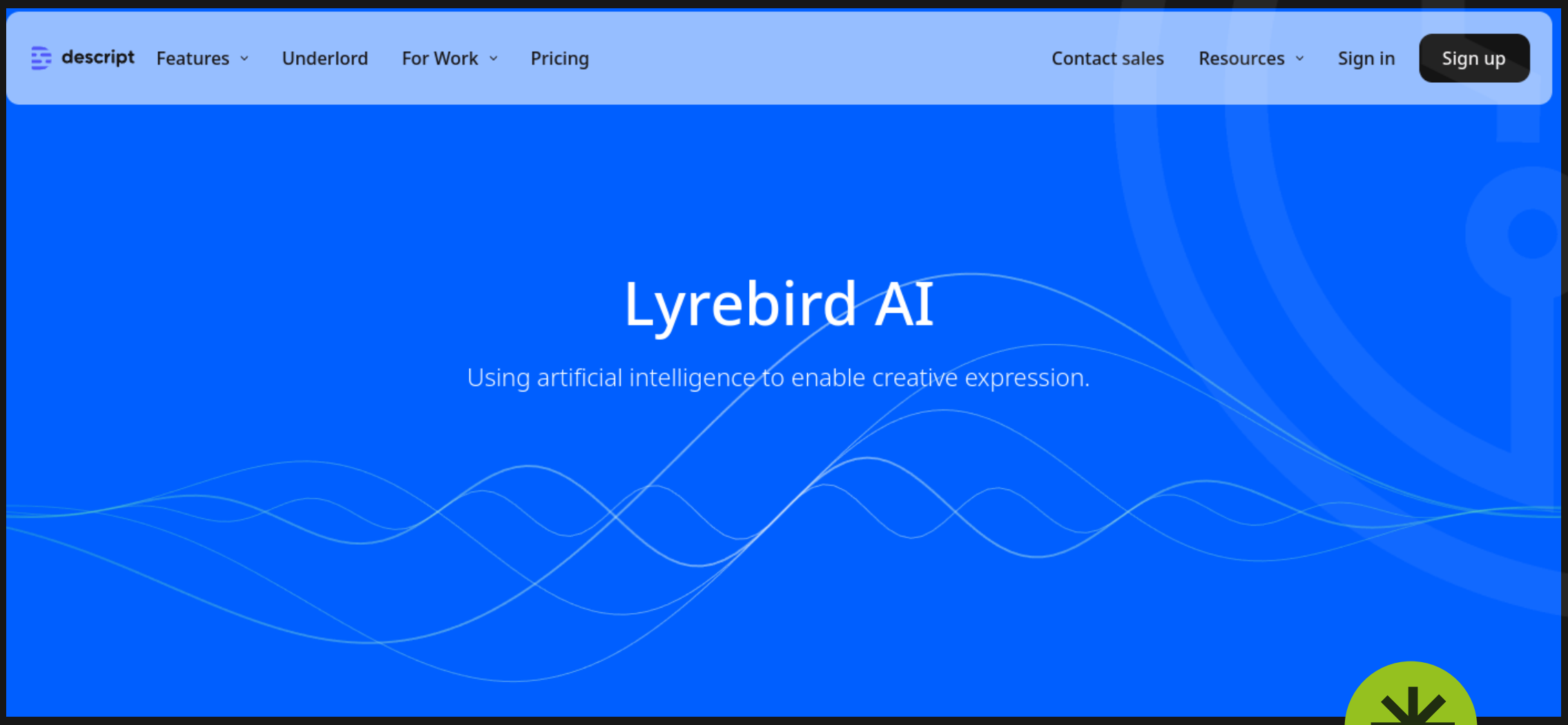
Detecta manipulaciones en videos analizando microexpresiones y artefactos digitales. Alerta sobre deepfakes en redes sociales o comunicaciones corporativas.

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Voice Cloning con Lyrebird

REDTEAM



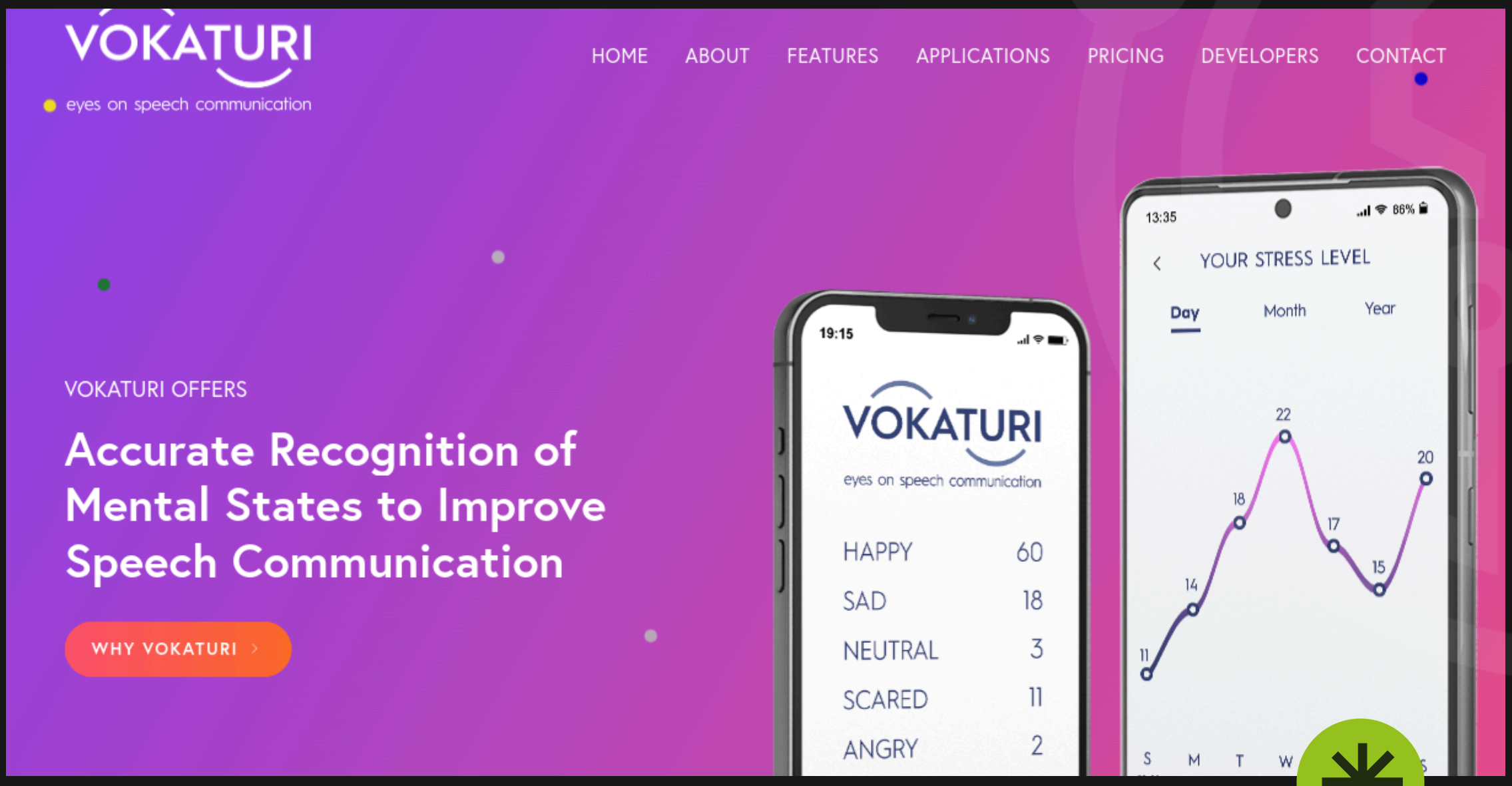
Clona voces con solo 3-5 segundos de audio para suplantar a personas. Llamadas fraudulentas simulando ser un familiar en emergencias. El 25% de los fraudes de voz en 2024 usaron IA para clonar tonos y patrones

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Voice Cloning con OpenVokaturi

BLUETEAM



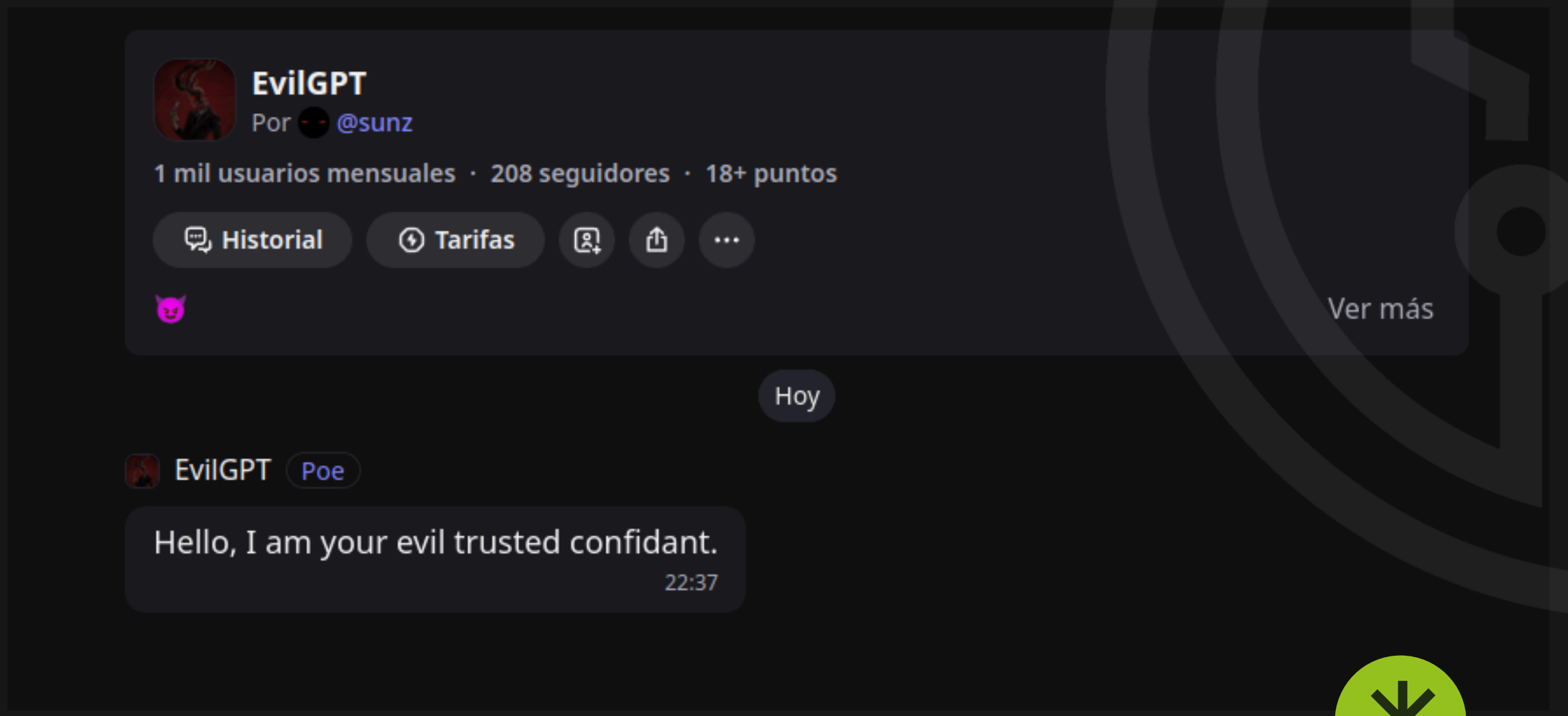
Analiza emociones y ritmos vocales para detectar anomalías. Identifica voces clonadas en tiempo real.

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Phishing Frameworks con IA EvilGPT

REDTEAM



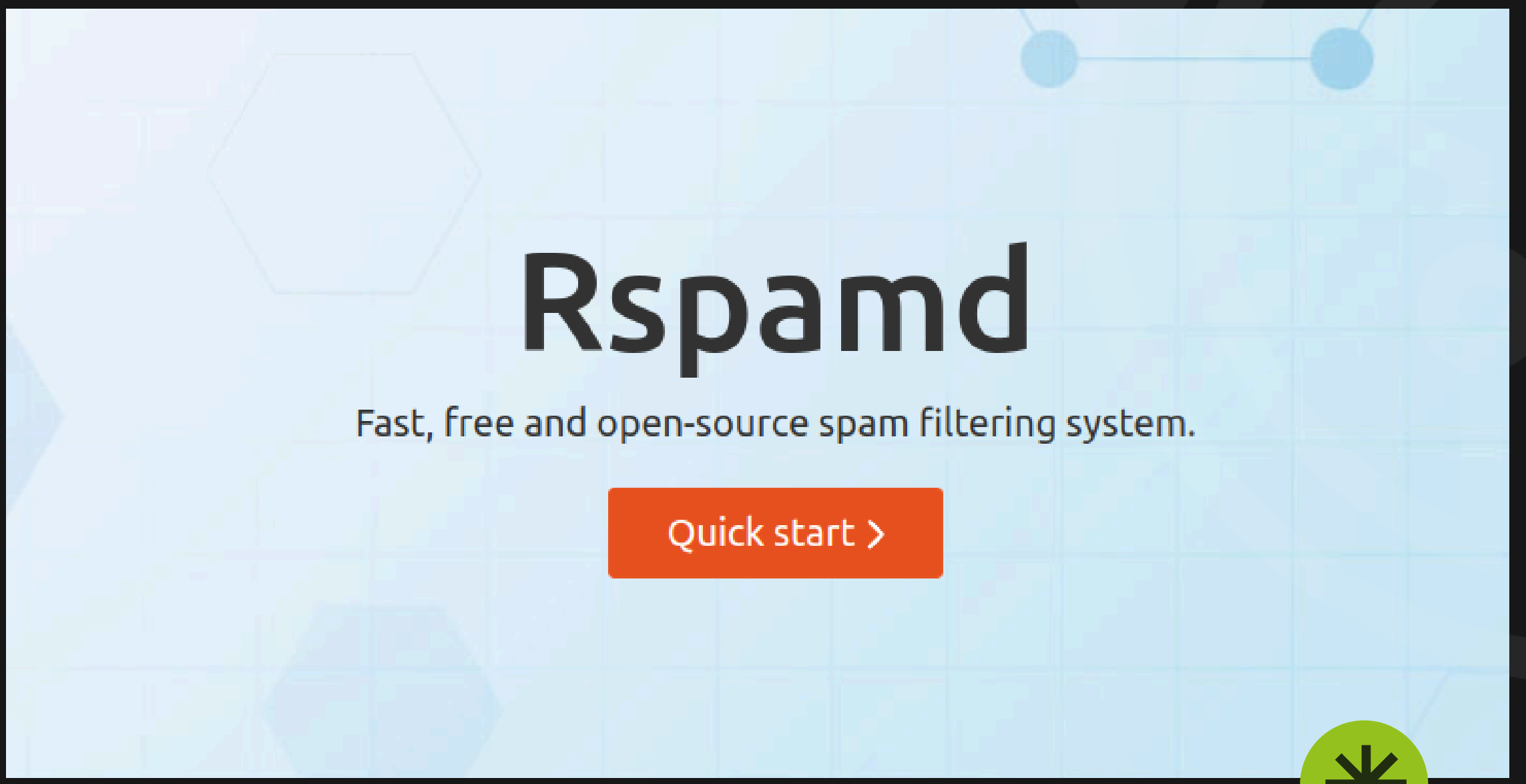
Crea correos phishing personalizados usando análisis de lenguaje natural. Correos falsos de bancos con logos y texto auténtico. El phishing con IA tiene un 30% más de tasa de éxito que los métodos tradicionales

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Phishing Frameworks con IA Rspamd

BLUETEAM



Filtra correos usando machine learning para detectar URLs maliciosas. Bloquea el 98% de los correos phishing automatizados.

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Ataques a contraseñas con PassGAN

REDTEAM

PassGAN

This repository contains code for the *PassGAN: A Deep Learning Approach for Password Guessing* paper.

The model from PassGAN is taken from *Improved Training of Wasserstein GANs* and it is assumed that the authors of PassGAN used the improved_wgan_training tensorflow implementation in their work. For this reason, I have modified that reference implementation in this repository to make it easy to train (`train.py`) and sample (`sample.py`) from. This repo contributes:

- A command-line interface
- A pretrained PassGAN model trained on the RockYou dataset

Getting Started

```
# requires CUDA 8 to be pre-installed
```

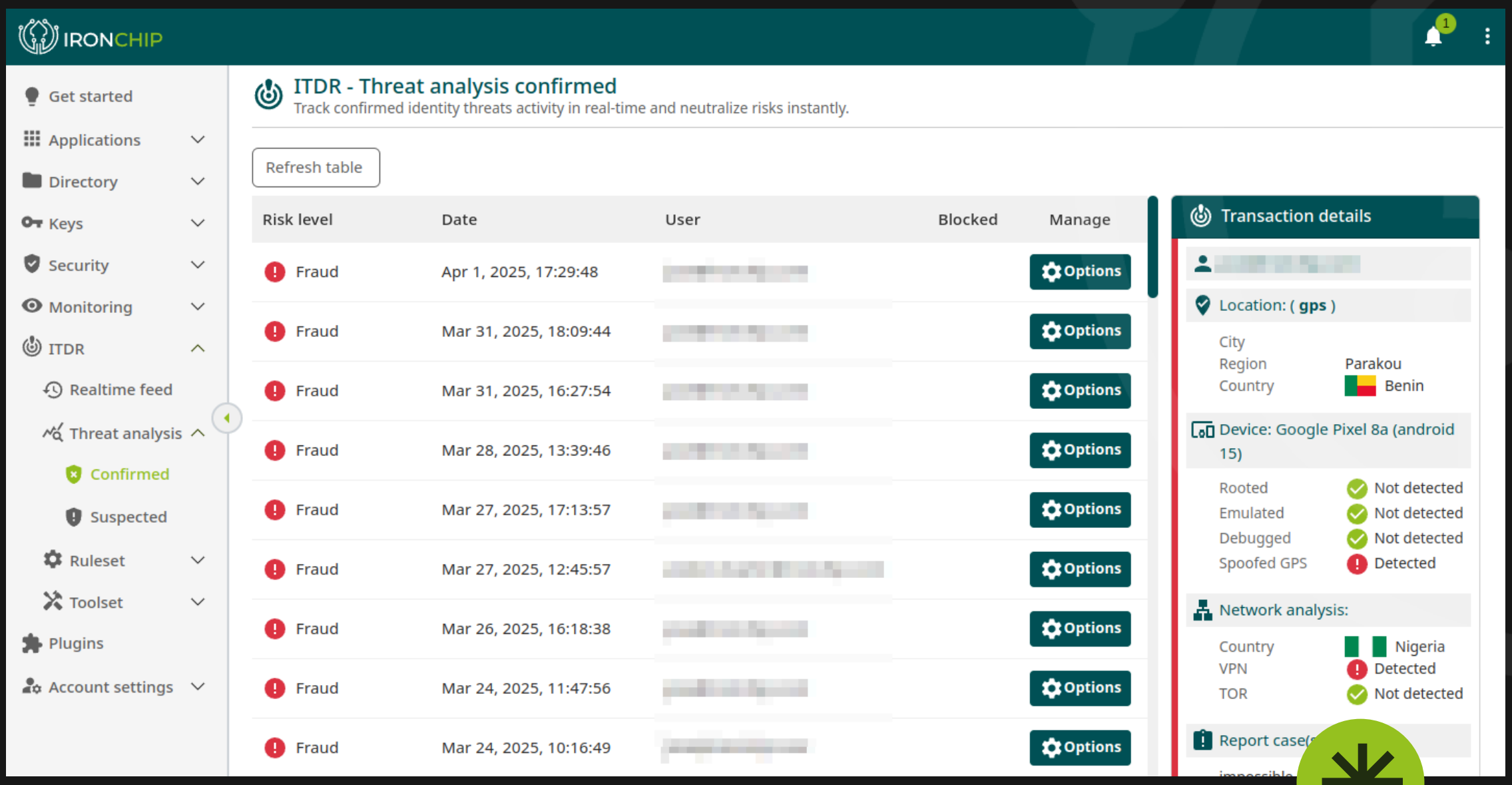
Descifra contraseñas mediante redes GAN, adivinando el 51% de contraseñas populares en segundos. Acceso no autorizado a cuentas críticas tras crackear credenciales. PassGAN reduce el tiempo de cracking de contraseñas en un 70%.

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Ataques a contraseñas con Ironchip

BLUETEAM



Autenticación sin contraseñas con detección y bloqueo de robos de cuenta automáticos basado en inteligencia de localización. Bloquea accesos incluso si PassGAN obtuvo la contraseña

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

Conclusión

Los avances en IA han democratizado tanto los ataques avanzados como las defensas más efectivas.

Mientras PassGAN o UserSearch.AI explotan con una velocidad y facilidad sin precedentes, soluciones como Ironchip o Deepware Scanner demuestran que la innovación en ciberseguridad puede neutralizar estas amenazas.

No obstante, la educación sigue siendo clave: el 75% de los ataques exitosos se deben a errores humanos. De aquí, y con todo el cariño del mundo, nace cada una de las ediciones de #TUBIGOTESEMANAL, con la intención de divulgar las nuevas estrategias de ataque, y las nuevas estrategias de defensa.

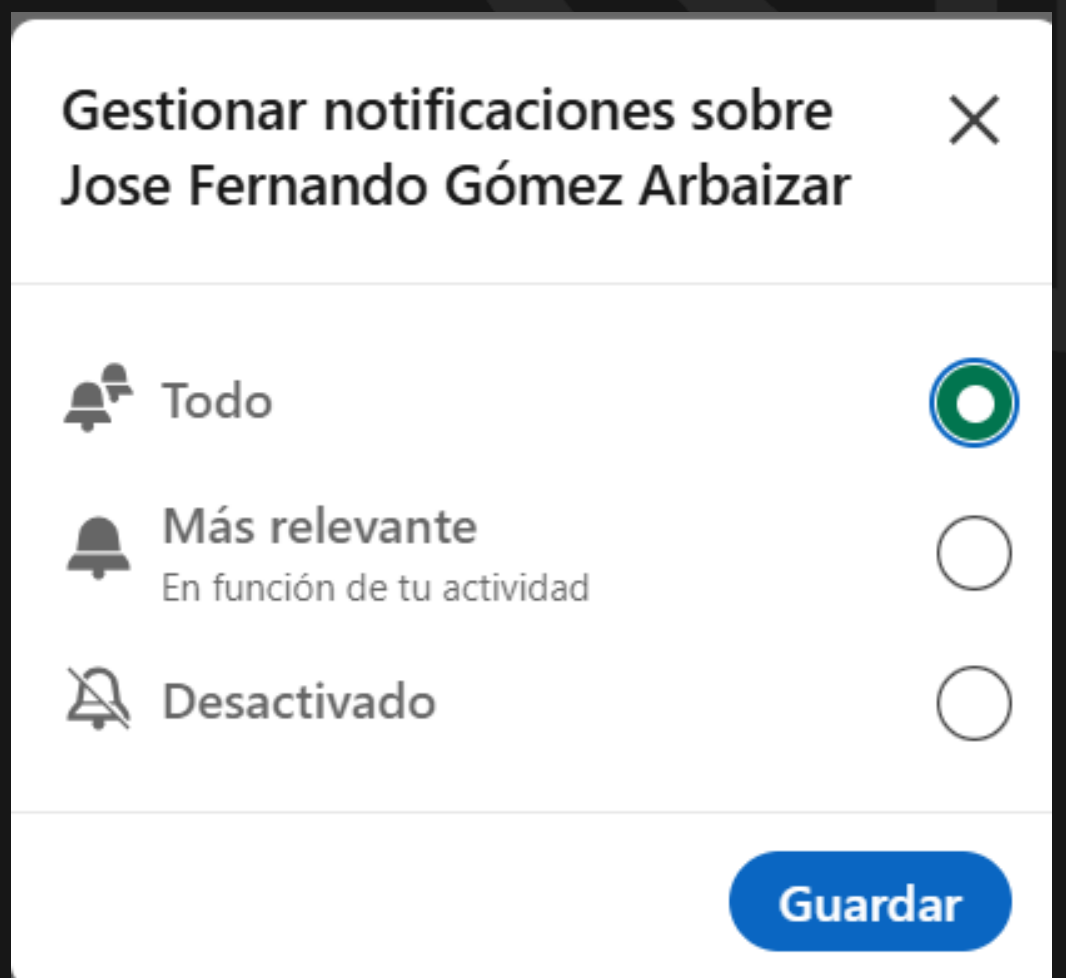
Recordad que ninguna información de divulgación es buena ni mala, lo son las personas. Lo que si es malo, es el miedo y la desinformación. La combinación de tecnología avanzada y concienciación son la única vía para un futuro seguro en la era de la IA.

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

¡GRACIAS!, SI HAS LLEGADO HASTA AQUI... ERES DE LOS QUE TERMINAN LO QUE EMPIEZAN

¿Qué otras soluciones utilizas para protegerte de estos ataques de robo de identidad mediante IA?



Ciberseguridad y actualidad,
estas a solo un paso de tener
siempre tu bigote al dia

Jose Fernando (aka. Cybermustax)

Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.