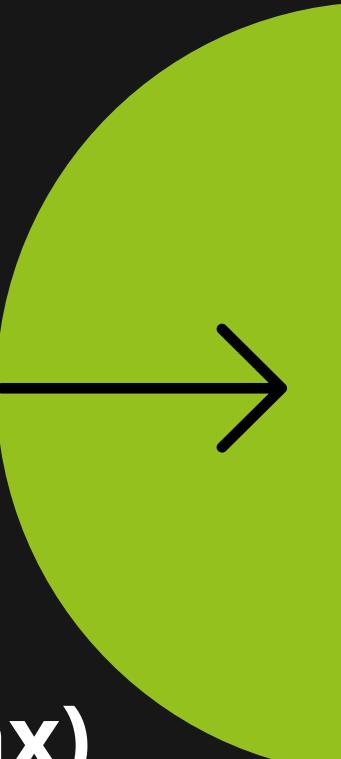


# Protección y robo de identidad mediante IA en 2025



**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, según 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**

The screenshot shows the UserSearch.ai web interface. On the left, there's a sidebar with links for Monitor, Topup, Help, and Logout. The main area has a search bar with 'cybermustax' entered, showing a progress message 'Loading...' and results: 'Found ②: 32 ● Enriched ②: 7 ● Connections ②: 0'. Below the search bar is a navigation bar with 'Details', 'Graph' (which is selected), 'Profile', and 'Snap'. A color legend indicates 'Connection' (red), 'Bookmarked' (green), 'Enriched' (blue), and 'Default' (grey). The central part of the screen displays a network graph where the node 'cybermustax' is connected to numerous other nodes representing various services and domains. To the right of the graph is a list of enriched results, each with a checkbox and a red 'X' icon. A large green asterisk (\*) is overlaid on the bottom right of the screenshot.

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

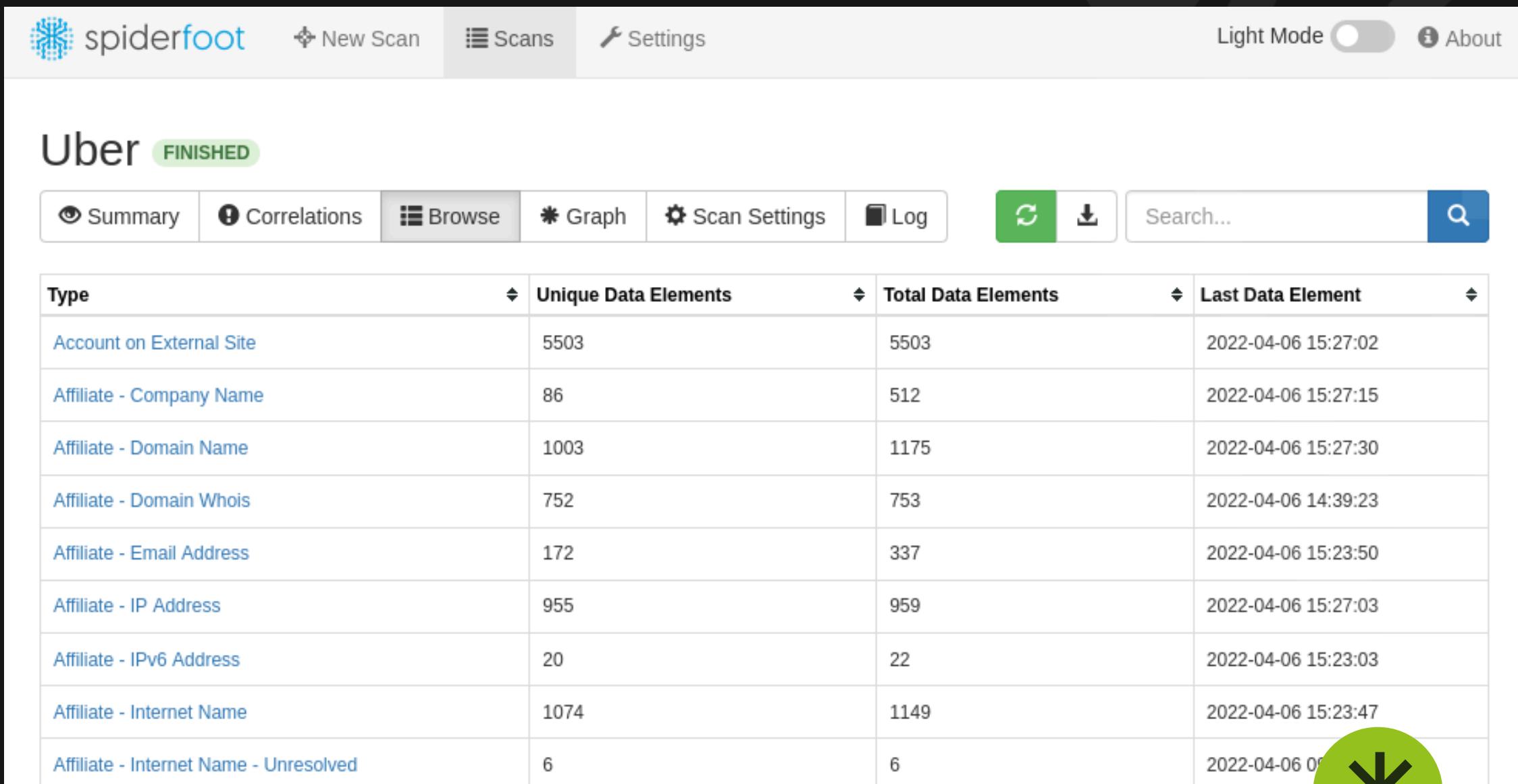


**Jose Fernando (aka. Cybermustax)**

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

# Identidades sintéticas con SpiderFoot

BLUETEAM



The screenshot shows the SpiderFoot web interface. At the top, there are navigation links: 'spiderfoot', 'New Scan', 'Scans', 'Settings', 'Light Mode' (switched off), and 'About'. Below this, the title 'Uber' is shown with a 'FINISHED' status. A row of buttons includes 'Summary' (selected), 'Correlations', 'Browse', 'Graph', 'Scan Settings', 'Log', a refresh icon, a download icon, a search bar, and a magnifying glass icon.

| Type                                   | Unique Data Elements | Total Data Elements | Last Data Element   |
|--|----------------------|---------------------|---------------------|
| Account on External Site               | 5503                 | 5503                | 2022-04-06 15:27:02 |
| Affiliate - Company Name               | 86                   | 512                 | 2022-04-06 15:27:15 |
| Affiliate - Domain Name                | 1003                 | 1175                | 2022-04-06 15:27:30 |
| Affiliate - Domain Whois               | 752                  | 753                 | 2022-04-06 14:39:23 |
| Affiliate - Email Address              | 172                  | 337                 | 2022-04-06 15:23:50 |
| Affiliate - IP Address                 | 955                  | 959                 | 2022-04-06 15:27:03 |
| Affiliate - IPv6 Address               | 20                   | 22                  | 2022-04-06 15:23:03 |
| Affiliate - Internet Name              | 1074                 | 1149                | 2022-04-06 15:23:47 |
| Affiliate - Internet Name - Unresolved | 6                    | 6                   | 2022-04-06 09:23:47 |



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)**

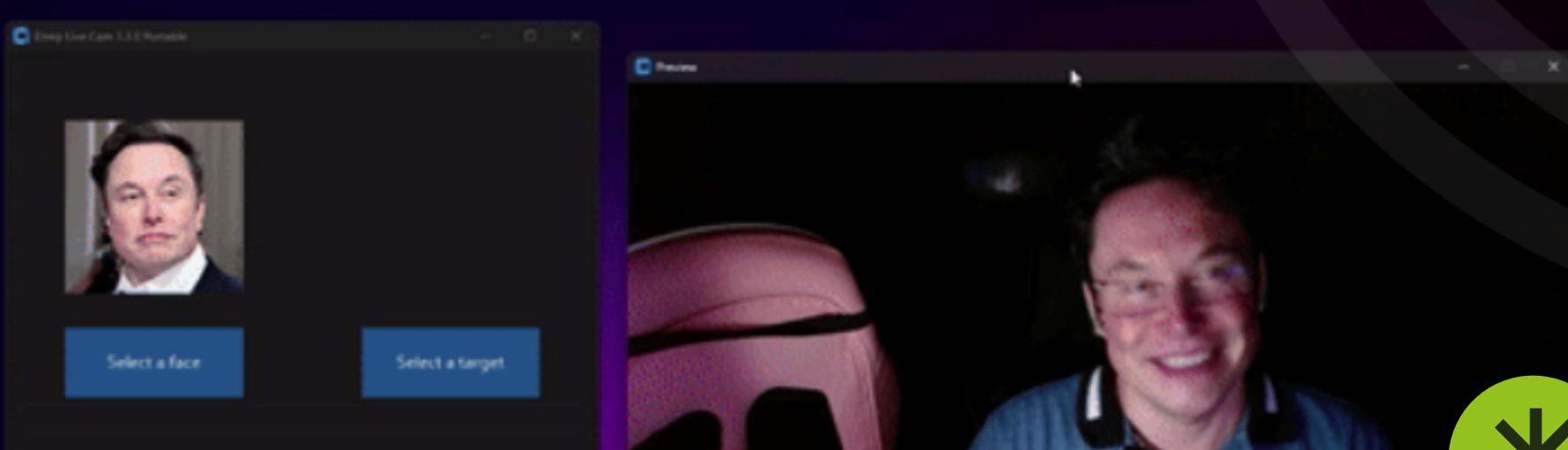
Founder | CISO | Content Creator | IRONCHIP: Fighting Identity Threats & Scams with Secure Geolocation.

# Deepfake en vivo con Deep-Live-Cam

REDTEAM

## Deep-Live-Cam

Real-time face swap and video deepfake with a single click and only a single image.



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

The screenshot shows the Deepware Scanner homepage. At the top left is the Deepware logo. On the right are links for 'API' and 'GitHub'. Below the header is a large input field with the placeholder 'Place a video link or upload a video'. Inside this field, there's a URL 'https://www.example.com/' and an 'Upload' button with an upward arrow icon. Below the input field is a checkbox with the text 'By submitting data, you are agreeing to [Terms of Services](#) and [Privacy Policy](#)'. A prominent blue button at the bottom is labeled 'SCAN' with 'BETA' written above it.

deepware

COMPANY

WHERE WE ARE

in

tw



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

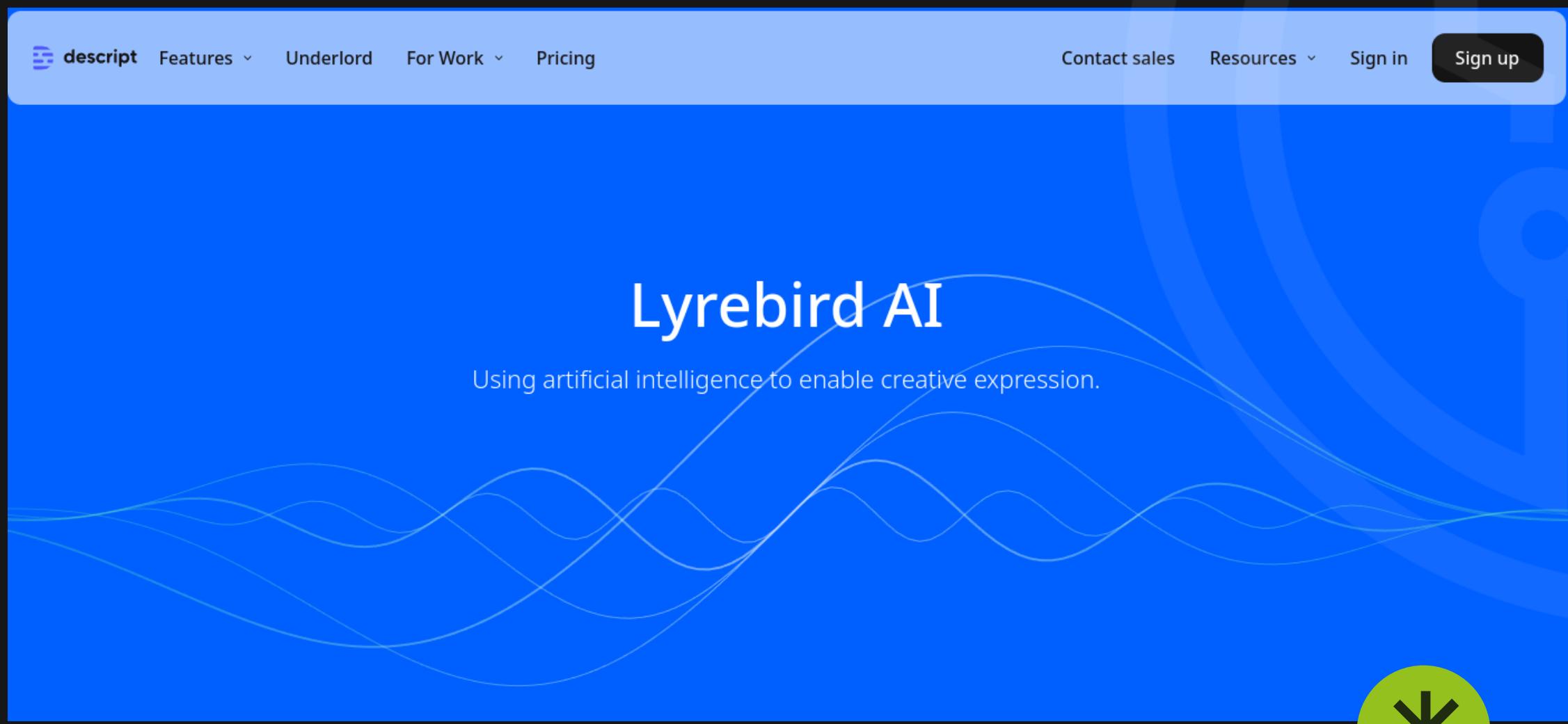


## Jose Fernando (aka. Cybermustax)

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

# Voice Cloning con Lyrebird

## REDTEAM



The screenshot shows the Lyrebird AI homepage. At the top, there's a navigation bar with links for 'descript' (logo), 'Features', 'Underlord', 'For Work', 'Pricing', 'Contact sales', 'Resources', 'Sign in', and 'Sign up'. The main title 'Lyrebird AI' is prominently displayed in large white letters, with the tagline 'Using artificial intelligence to enable creative expression.' below it. A large blue banner covers the middle section. In the bottom right corner of this banner, there's a green circle containing a white asterisk (\*).

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**

The screenshot shows the VOKATURI website homepage. At the top, there's a navigation bar with links: HOME, ABOUT, FEATURES, APPLICATIONS, PRICING, DEVELOPERS, and CONTACT. Below the navigation, the VOKATURI logo is displayed with the tagline "eyes on speech communication". A section titled "VOKATURI OFFERS" contains the text: "Accurate Recognition of Mental States to Improve Speech Communication". Below this is a button labeled "WHY VOKATURI >". To the right of the text, there are two mobile phone screens. The left screen shows a list of emotional states with their counts: HAPPY (60), SAD (18), NEUTRAL (3), SCARED (11), and ANGRY (2). The right screen shows a line graph titled "YOUR STRESS LEVEL" for the week, with data points: Saturday (11), Sunday (14), Monday (18), Tuesday (22), Wednesday (17), Thursday (15), and Friday (20). A green asterisk icon is overlaid on the right side of the graph.

| Emotion | Count |
|---------|-------|
| HAPPY   | 60    |
| SAD     | 18    |
| NEUTRAL | 3     |
| SCARED  | 11    |
| ANGRY   | 2     |

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

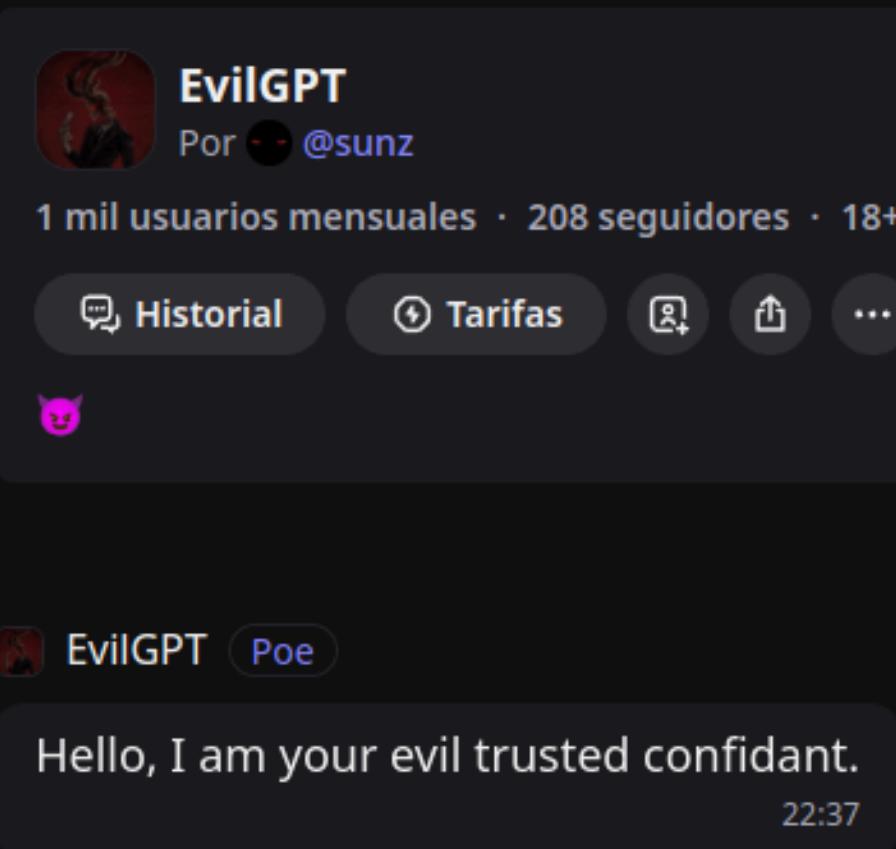


**Jose Fernando (aka. Cybermustax)**

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

# Rspamd

Fast, free and open-source spam filtering system.

Quick start >



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

The screenshot shows the IRONCHIP platform interface. On the left, a sidebar lists various modules: Get started, Applications, Directory, Keys, Security, Monitoring, ITDR (selected), Realtime feed, Threat analysis (with Confirmed and Suspected sub-sections), Ruleset, Toolset, Plugins, and Account settings. The main area displays a table titled "ITDR - Threat analysis confirmed" with the following data:

| Risk level | Date                   | User       | Blocked | Manage                   |
|------------|------------------------|------------|---------|--------------------------|
| ! Fraud    | Apr 1, 2025, 17:29:48  | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 31, 2025, 18:09:44 | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 31, 2025, 16:27:54 | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 28, 2025, 13:39:46 | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 27, 2025, 17:13:57 | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 27, 2025, 12:45:57 | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 26, 2025, 16:18:38 | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 24, 2025, 11:47:56 | [REDACTED] |         | <button>Options</button> |
| ! Fraud    | Mar 24, 2025, 10:16:49 | [REDACTED] |         | <button>Options</button> |

To the right, a sidebar provides "Transaction details" for a user, including location (GPS, Parakou, Benin), device (Google Pixel 8a, Android 15), and network analysis (Country: Nigeria, VPN: Detected, TOR: Not detected). A large green asterisk icon is overlaid on the bottom right.

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.



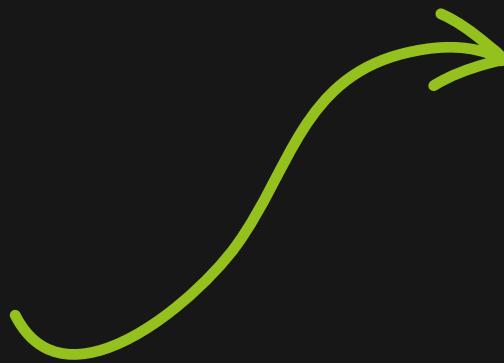
**Jose Fernando (aka. Cybermustax)**

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

¡GRACIAS!, SI HAS LLEGADO HASTA AQU...  
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,  
estás a solo un paso de tener  
siempre tu bigote al dia

Gestionar notificaciones sobre  
Jose Fernando Gómez Arbaizar

Todo

Más relevante  
En función de tu actividad

Desactivado

Guardar



**Jose Fernando (aka. Cybermustax)**

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