DNSCheck

Framework para Administradores de Redes Contra Ameaças Baseadas em DNS

GTER • 16 DE DEZEMBRO DE 2025

GABRIELE ZANCHETA SCAVAZINI

THE BOSS

Kim Morgan De O. I. Porto

Matheus B. Moriel

Guilherme R. Bofo

GABRIELE Z. SCAVAZINI

ACME!

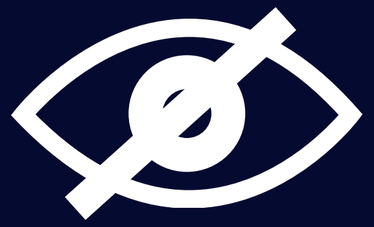
Cybersecurity Research

- Localizado em São José do Rio Preto
- UNESP - IBILCE

Por Que DNSCheck?

Sistema dividido em 3 partes:

Blocklists



Dashboards

Classificadores

Aliado ao SysAdmin Brasileiro

Aliado poderoso para administradores de sistemas

Sistemas similares podem custar milhares de reais por mês

Solução brasileira focada nas necessidades locais

Análise rápida e eficaz de domínios desconhecidos

100% Open Source

O DNSCheck será totalmente de código aberto, permitindo:

- Contribuição da comunidade de segurança brasileira
- Transparência completa da implementação
- Colaboração em melhorias e novas features
- Uso livre para fins educacionais e profissionais

Stack Tecnológico

Django - Framework Python para segurança e escalabilidade

Django REST Framework - APIs acessíveis para classificadores

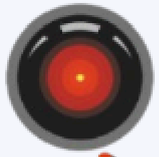
HTML, CSS, JavaScript - Interface web

Stack Modular

DNSCHECK
POWERED BY ACME! CYBERSECURITY

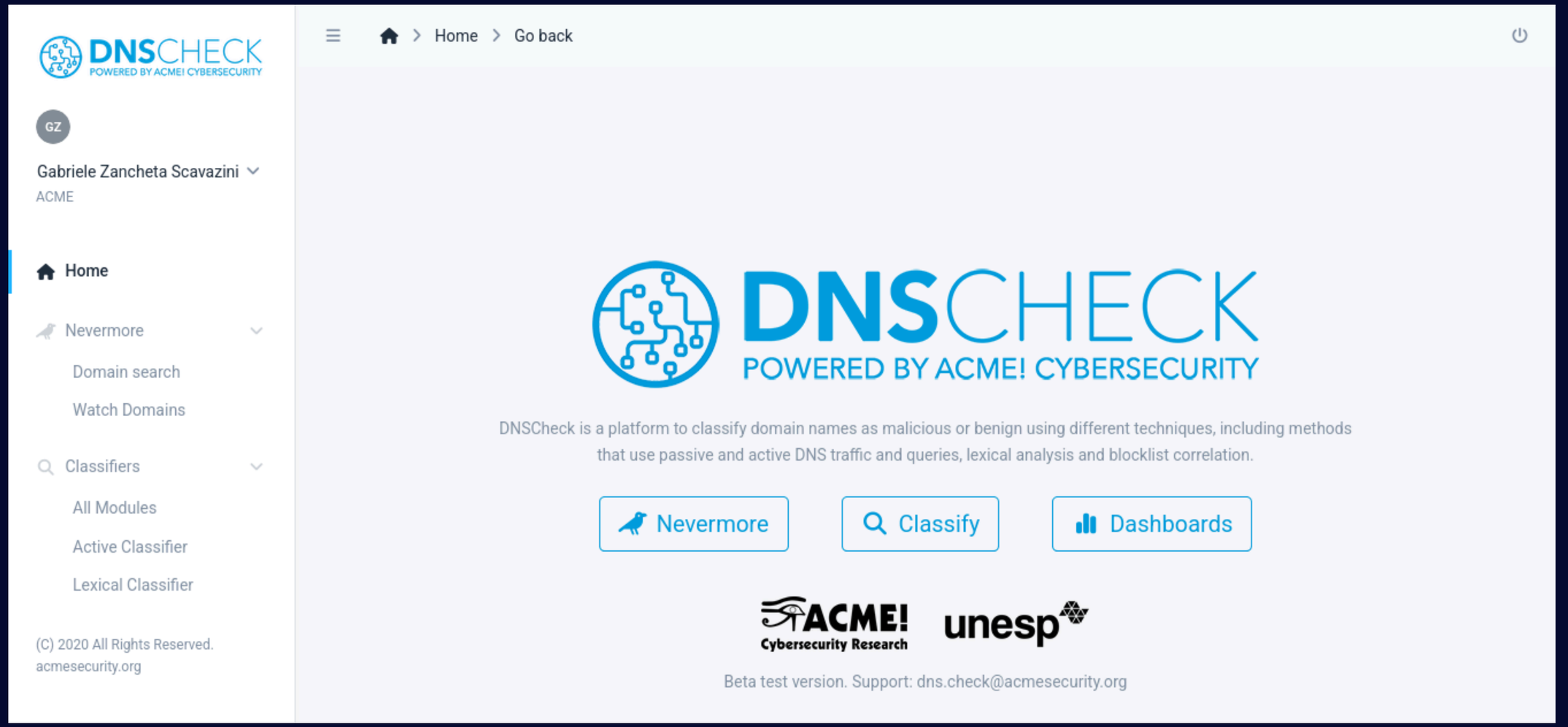
pDNS Monitor
POWERED BY ACME! CYBERSECURITY

Nevermore
POWERED BY ACME! CYBERSECURITY



Sentinel
POWERED BY ACME! CYBERSECURITY

Interface Principal

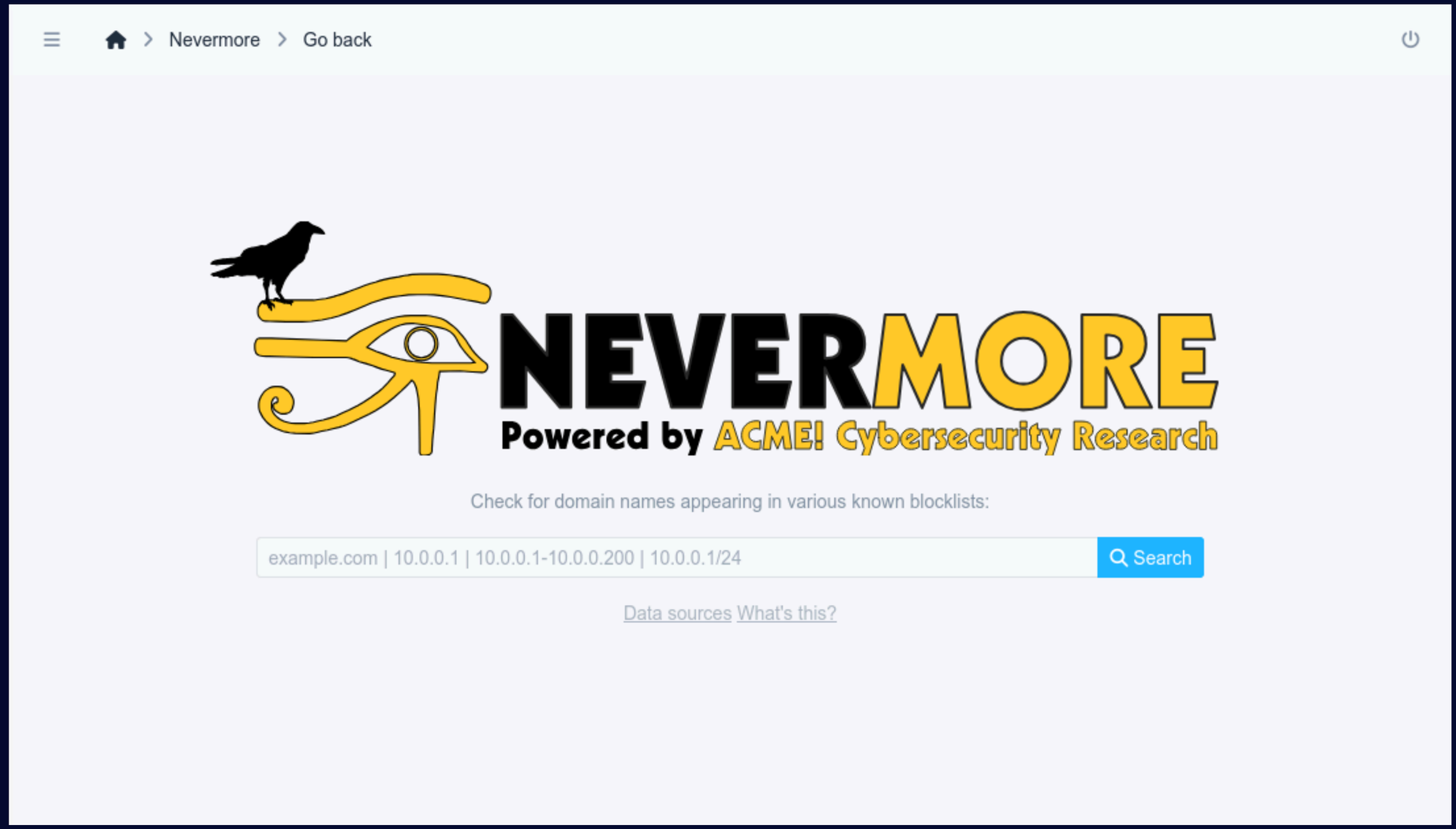


Nevermore: Blocklists

Corvinho que consulta e enriquece blocklists

- Consulta diária da lista Hagezi's TIF
- ~2 milhões de domínios enriquecidos com DNS
- IPs, ASs, MXs e outras informações DNS extraídas
- Dataset gigantesco para pesquisa e treinamento de IA

Interface Nevermore



Interface Nevermore

Interface Nevermore

Blocklist detection	
Source blocklist	tif
First detection	2025-11-17

DNS Records

Data obtained by querying DNS servers for this specific domain.

IP	ASN	TTL
54.156.158.84	14618	N/A

MX: N/A

TXT: N/A

NS: N/A

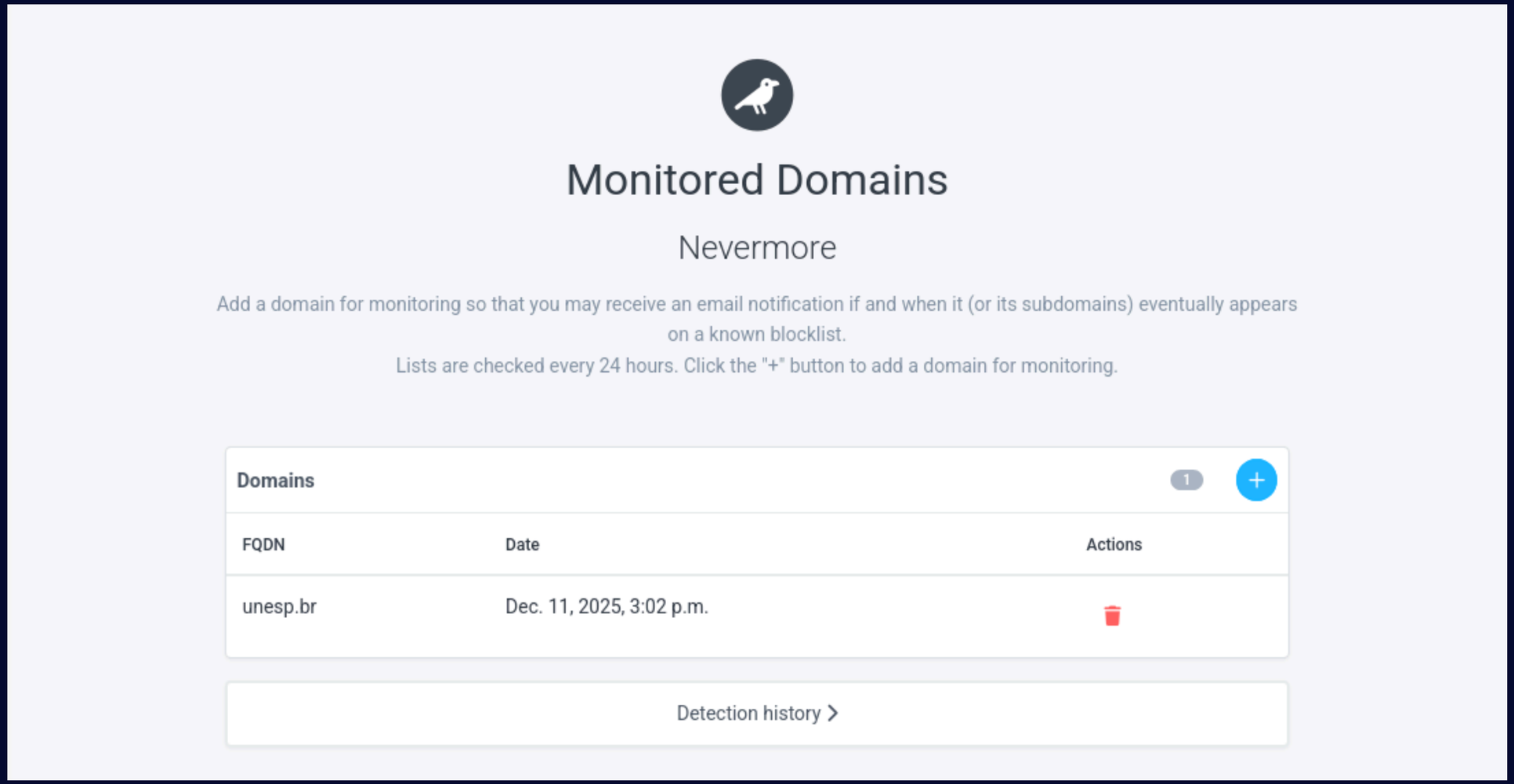
CNAME: N/A

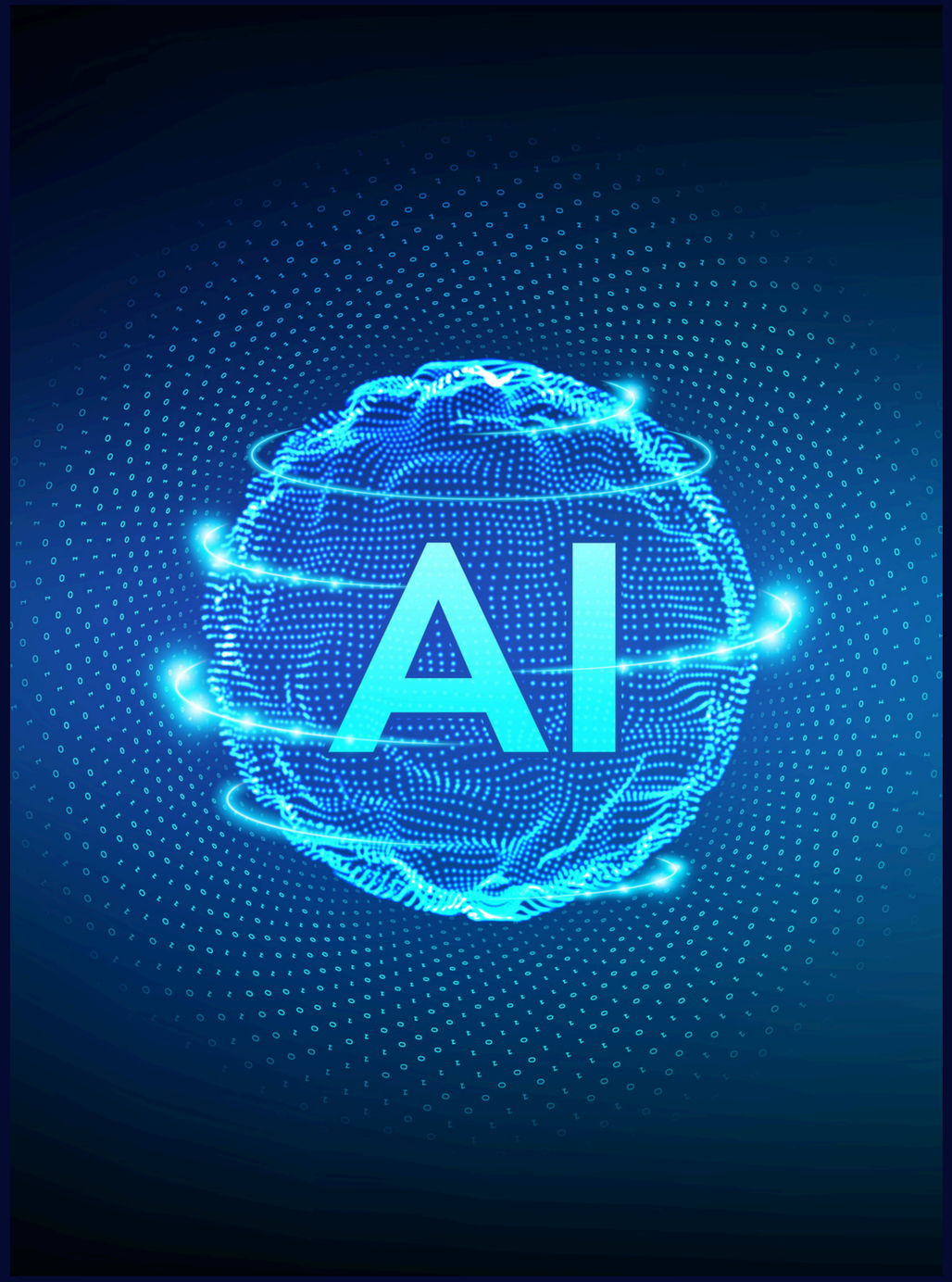
SOA: N/A

ASNs: 16509

Data sources What's this?

Interface Watch Domains



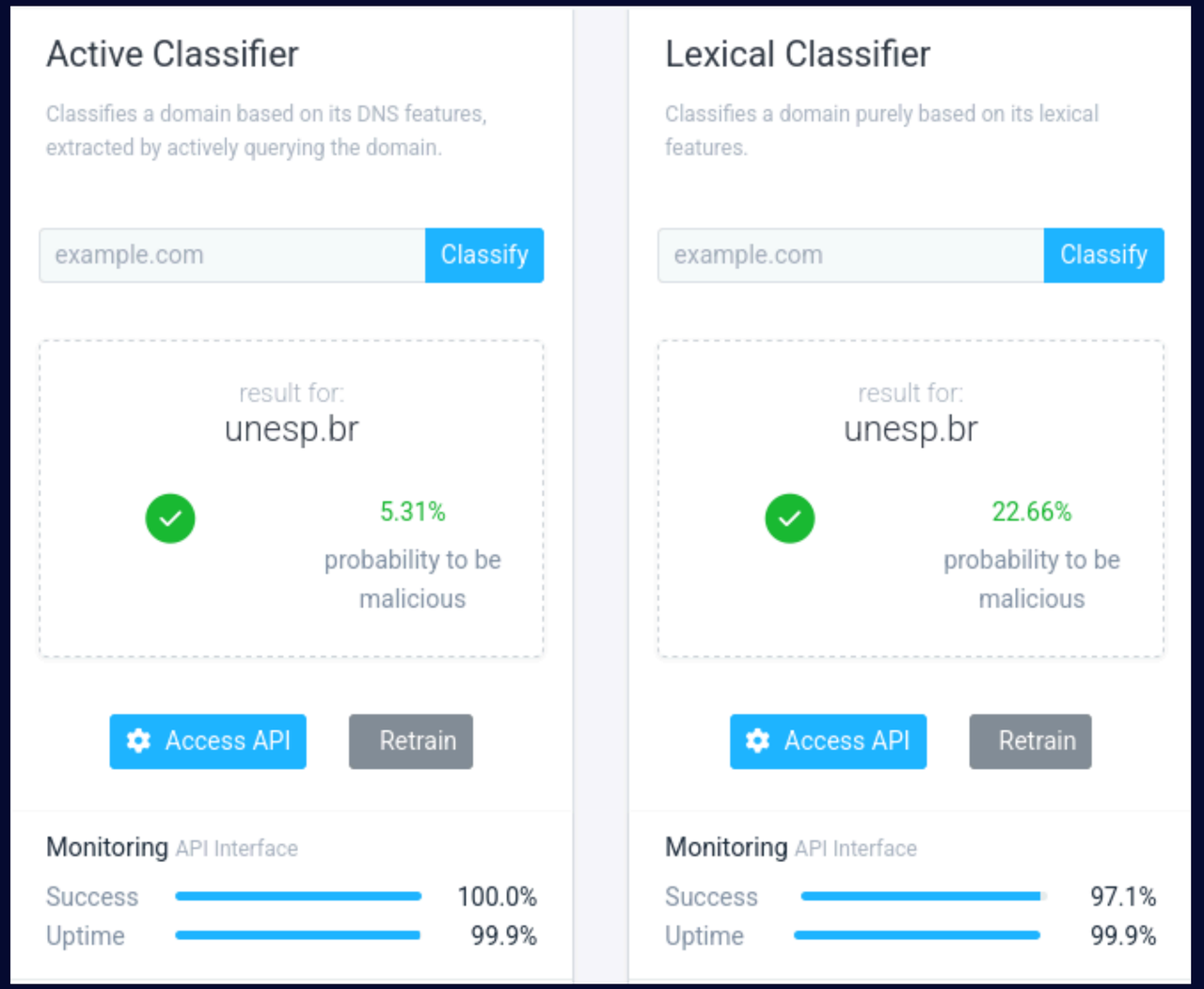


Classificadores IA

Léxico - Análise de características do domínio

Ativo - Dados de DNS ativo (IPs, TTL, etc)

Interface Classificadores

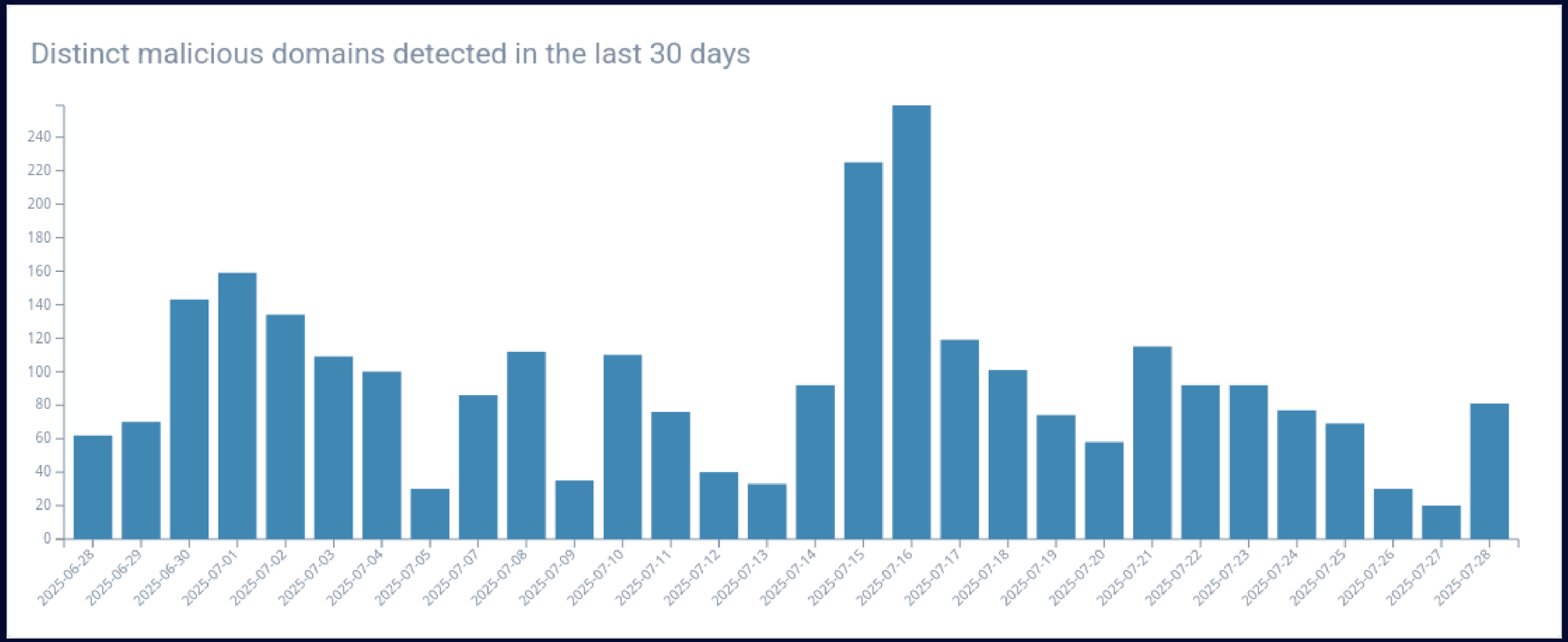


Dashboards

Dados de terceiro via acordo com UNESP:

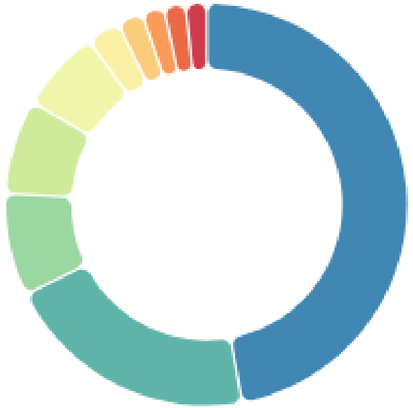
- Base de dados ENTRADA2 (projeto open-source)
- Análise de IPs acessando domínios maliciosos
- ASs com maior atividade suspeita
- Distribuição geográfica de acessos
- Informações acionáveis

Interface Dashboards



Interface Dashboards

Most accessed malicious domains



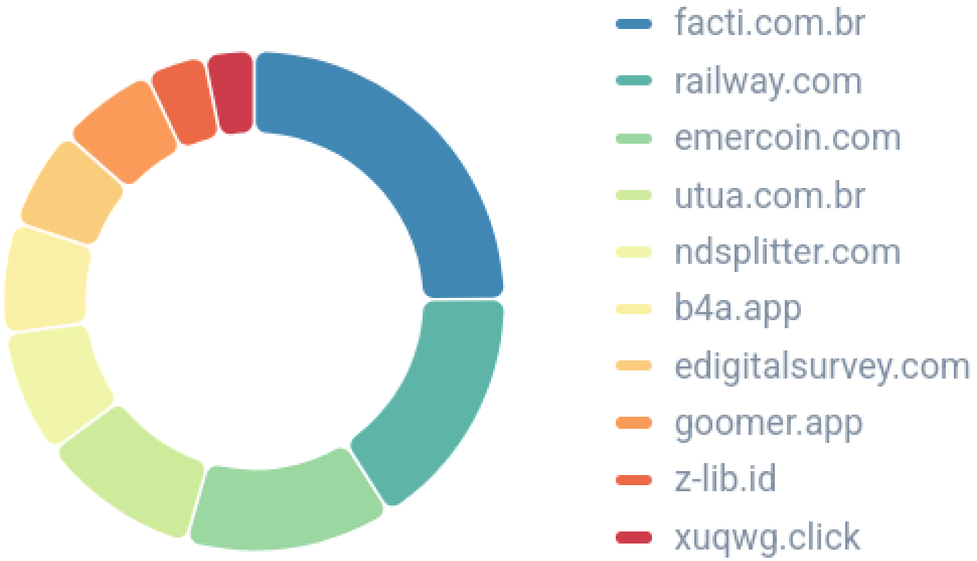
- o789thktrk.com
- secu100.net
- rtmark.net
- polyfill.io
- remodelingcontractorassociation.com
- ammails.ru
- outbyte.com
- peacemail.com
- vegemail.com
- pancingqueen.com

Autonomous Systems with the most malicious domain detections

- CLOUDFLARENET
- SERVERS-COM
- DataWeb Global Group B.V.
- AMAZON-02
- RETN Limited
- Trellian Pty. Limited
- GOOGLE-CLOUD-PLATFORM
- ZEN-ECN
- AMAZON-AES
- FORTINET

Interface Dashboards

Most accessed malicious domains from CLOUDFLARENET

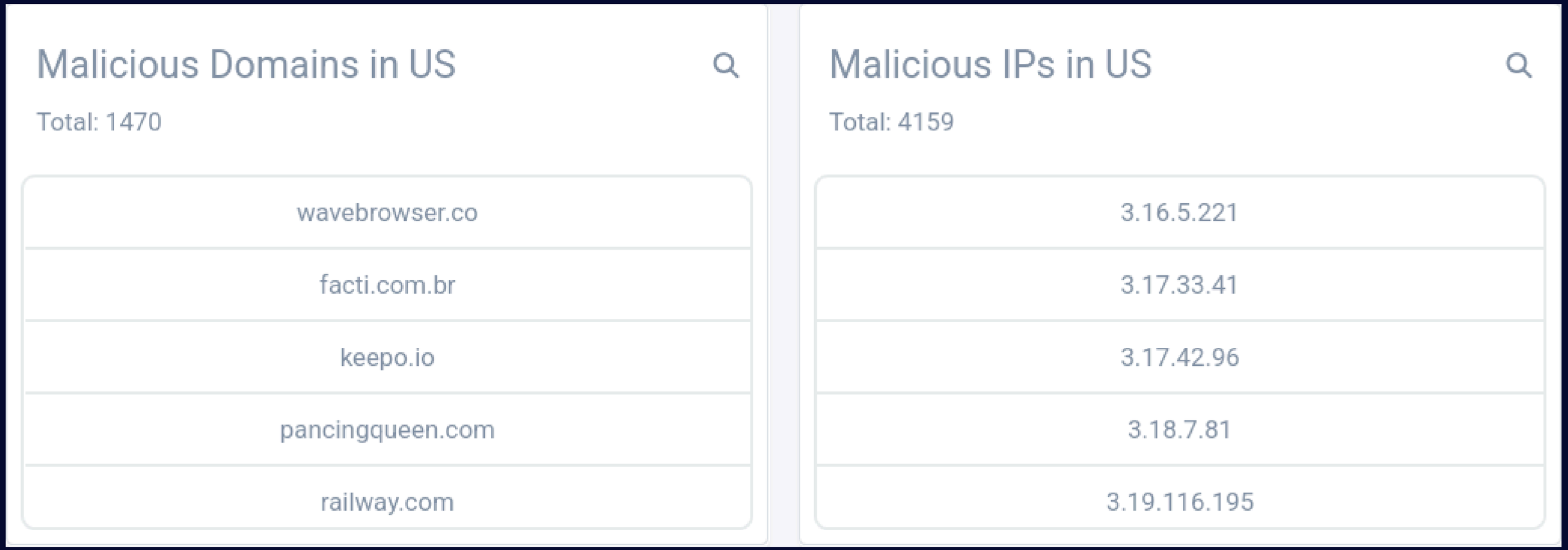


Malicious domains from CLOUDFLARENET

Total: 376

facti.com.br
Total accesses: 34936
emercoin.com
utua.com.br

Interface Dashboards



Trabalhos Futuros

Em termos de novos estudos:

- AMAZONAS
- DGA Classifier
- Clustering Classifier

OBRIGADA!

DNSCheck: Framework para Administradores de Redes Contra Ameaças Baseadas em DNS

dnscheck.acmesecurity.org

Quer participar?

gabriele.scavazini@acmesecurity.org

Perguntas?