

DNSCheck

Framework para Administradores de Redes Contra Ameaças Baseadas em DNS



THE BOSS



Kim Morgan De O. I.
Porto



Matheus B. Moriel



Guilherme R. Bofo



GABRIELE Z. SCAVAZINI

 **TACME!**
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



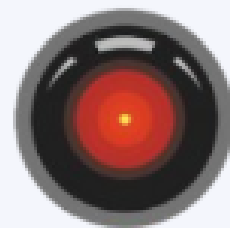
pDNS Monitor

POWERED BY ACME! CYBERSECURITY



Nevermore

POWERED BY ACME! CYBERSECURITY



Sentinel

POWERED BY ACME! CYBERSECURITY

Interface Principal

The screenshot displays the main interface of the DNSCHECK application. On the left is a vertical sidebar with the DNSCHECK logo (POWERED BY ACME! CYBERSECURITY) at the top, followed by a user profile for Gabriele Zancheta Scavazini (ACME). The sidebar contains a 'Home' link and two expandable sections: 'Nevermore' (with 'Domain search' and 'Watch Domains') and 'Classifiers' (with 'All Modules', 'Active Classifier', and 'Lexical Classifier'). At the bottom of the sidebar is a copyright notice: '(C) 2020 All Rights Reserved. acmesecurity.org'.

The main content area features a breadcrumb trail: 'Home > Go back'. The central part of the page displays the DNSCHECK logo and a description: 'DNSCheck is a platform to classify domain names as malicious or benign using different techniques, including methods that use passive and active DNS traffic and queries, lexical analysis and blocklist correlation.' Below this text are three buttons: 'Nevermore' (with a bird icon), 'Classify' (with a magnifying glass icon), and 'Dashboards' (with a bar chart icon).

At the bottom of the page, there are logos for 'ACME! Cybersecurity Research' and 'unesp', followed by the text 'Beta test version. Support: dns.check@acmesecurity.org'.

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

  > Nevermore > [Go back](#) 



NEVERMORE

Powered by **ACME!** Cybersecurity Research

Check for domain names appearing in various known blocklists:

Q Search

[Data sources](#) [What's this?](#)

Interface Nevermore



Check for domain names appearing in various known blocklists:

Search

Malicious domains matching "americanas" found in blocklists. Click an item for more info.

Updated every 48 hours.

americanasbrasil.online

IPs: 54.156.158.84

ASNs: 14618

ddd.americanassc.org

IPs: 43.155.128.171, 2001:cdba::3257:9652

ASNs: 132203

ofertasamericanas.online

IPs: 13.248.213.45, 76.223.67.189

ASNs: 16509

[Data sources](#) [What's this?](#)

Interface Nevermore

Blocklist detection	
Source blocklist	<u>tif</u>
First detection	2025-11-17

DNS Records ▾

Data obtained by querying DNS servers for this specific domain.

IP	ASN	TTL
54.156.158.84	<u>14618</u>	<u>N/A</u>

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



Monitored Domains

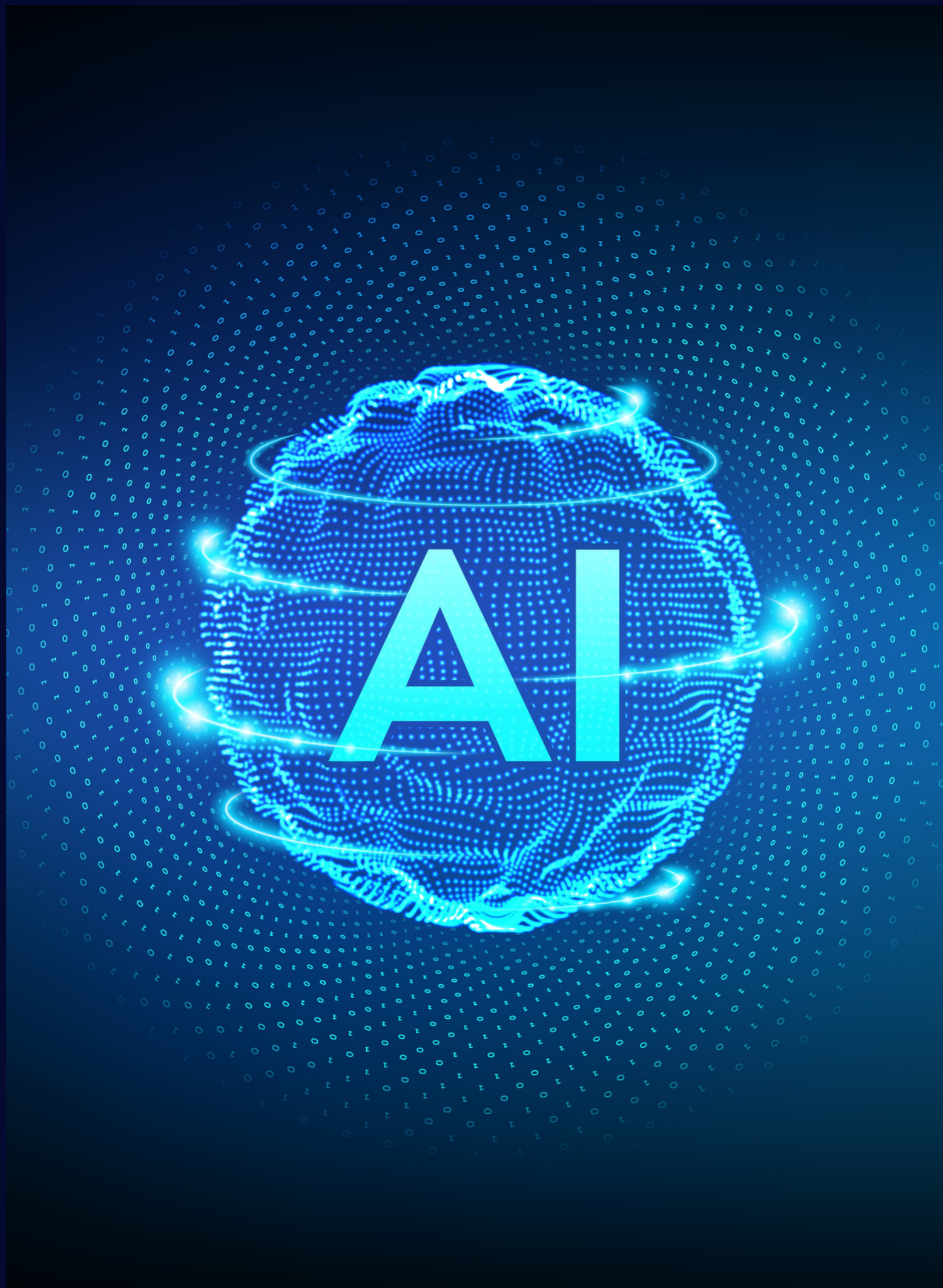
Nevermore

Add a domain for monitoring so that you may receive an email notification if and when it (or its subdomains) eventually appears on a known blocklist.

Lists are checked every 24 hours. Click the "+" button to add a domain for monitoring.

Domains 1 +		
FQDN	Date	Actions
unesp.br	Dec. 11, 2025, 3:02 p.m.	

Detection history >



Classificadores IA

Léxico - Análise de
características do domínio

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

Interface Classificadores

Active Classifier

Classifies a domain based on its DNS features, extracted by actively querying the domain.

Classify

result for:
unesp.br



5.31%
probability to be
malicious

 Access APIRetrain

Monitoring API Interface

Success		100.0%
Uptime		99.9%

Lexical Classifier

Classifies a domain purely based on its lexical features.

Classify

result for:
unesp.br



22.66%
probability to be
malicious

 Access APIRetrain

Monitoring API Interface

Success		97.1%
Uptime		99.9%

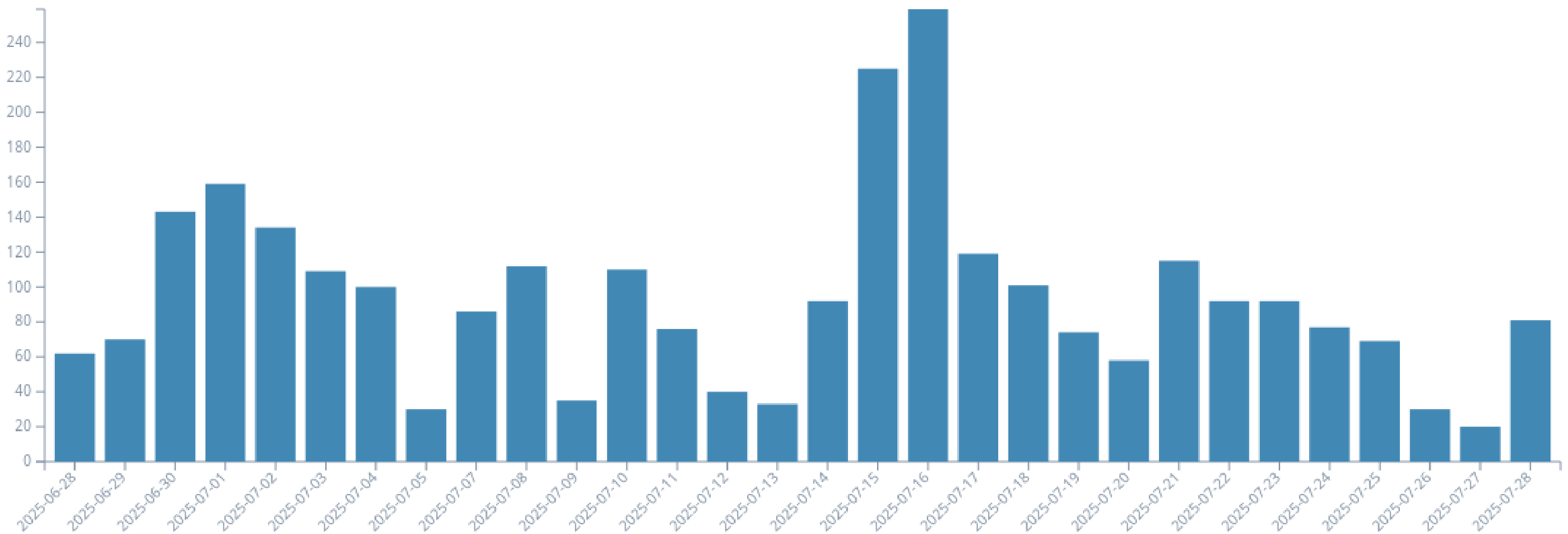
Dashboards

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
-

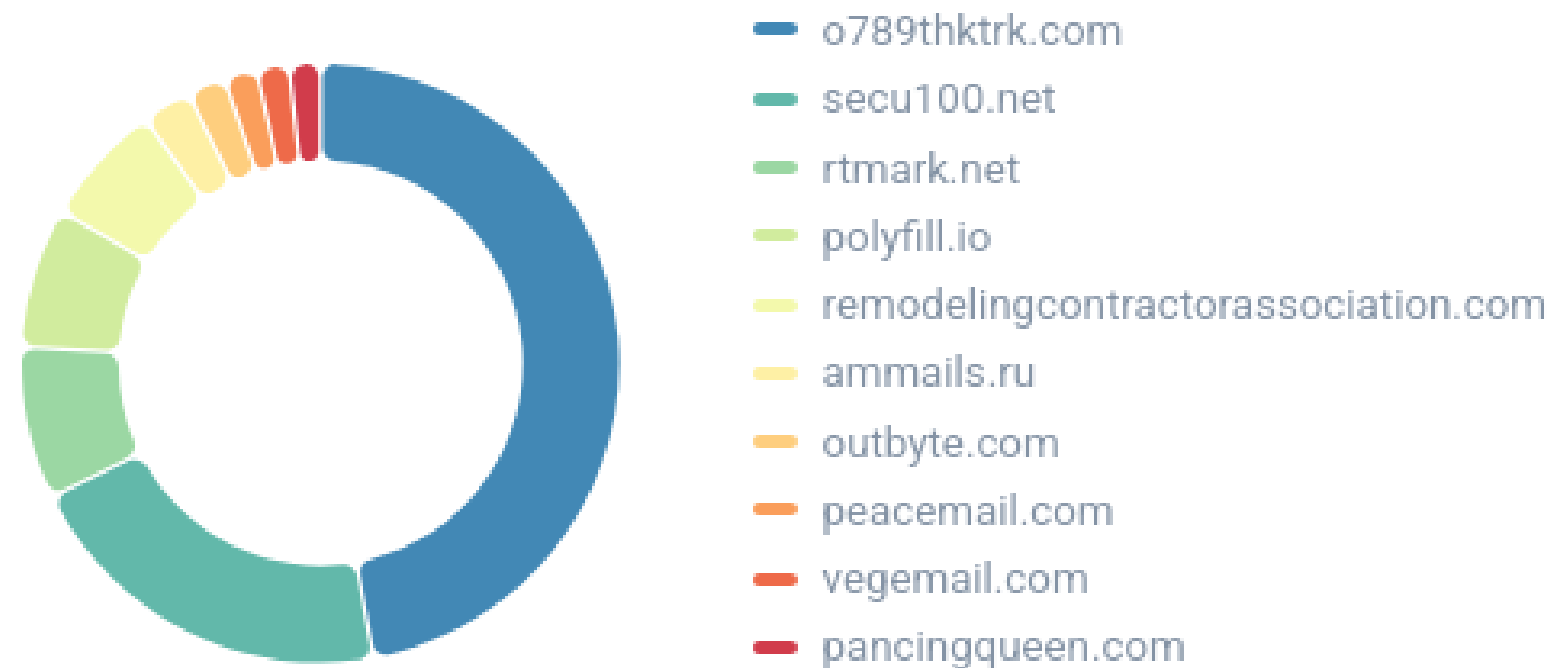
Interface Dashboards

Distinct malicious domains detected in the last 30 days

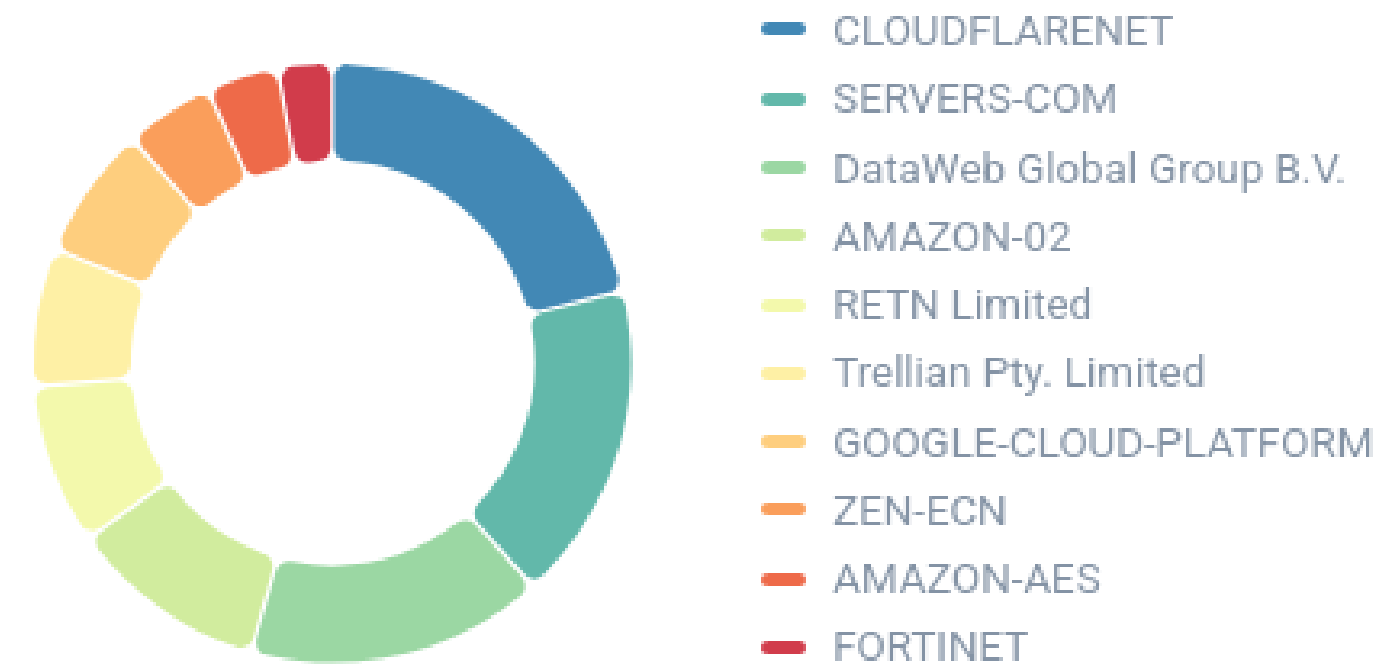


Interface Dashboards

Most accessed malicious domains



Autonomous Systems with the most malicious domain detections



Interface Dashboards

Most accessed malicious domains from CLOUDFLARENET



- facti.com.br
- railway.com
- emercoin.com
- utua.com.br
- ndsplitter.com
- b4a.app
- edigitalsurvey.com
- goomer.app
- z-lib.id
- xuqwg.click

Malicious domains from
CLOUDFLARENET



Total: 376

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

Interface Dashboards

Malicious Domains in US



Total: 1470

wavebrowser.co
facti.com.br
keepo.io
pancingqueen.com
railway.com

Malicious IPs in US



Total: 4159

3.16.5.221
3.17.33.41
3.17.42.96
3.18.7.81
3.19.116.195

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?