INFORMATION AND
COMMUNICATION
TECHNOLOGIES
AUTHORITY

.TRABİS
.tr AĞ BİLGİ SİSTEMİ

ICANN 81 ANNUAL GENERAL MEETING

.TR ccTLD

ABUSE MITIGATION MECHANISM

12.11.2024

Mahmut Esat Yıldırım
mesat.yildirim@btk.gov.tr

The Relationship Between CERT and ccTLD

- TR-CERT (Turkish Computer Emergency Response Team) is the national cybersecurity incident response center of Türkiye. Its primary role is to **detect, analyze, and mitigate** cybersecurity threats and incidents across the country.

- Within our institution, TR-CERT, which operates within the same department as TRABIS, utilizes artificial intelligence technologies in its R&D activities to detect malicious activities, anticipate threats, and enhance capabilities to combat them.

National Cyber Security Strategies and Action Plans

2013-2014

2016-2019

2020-2023

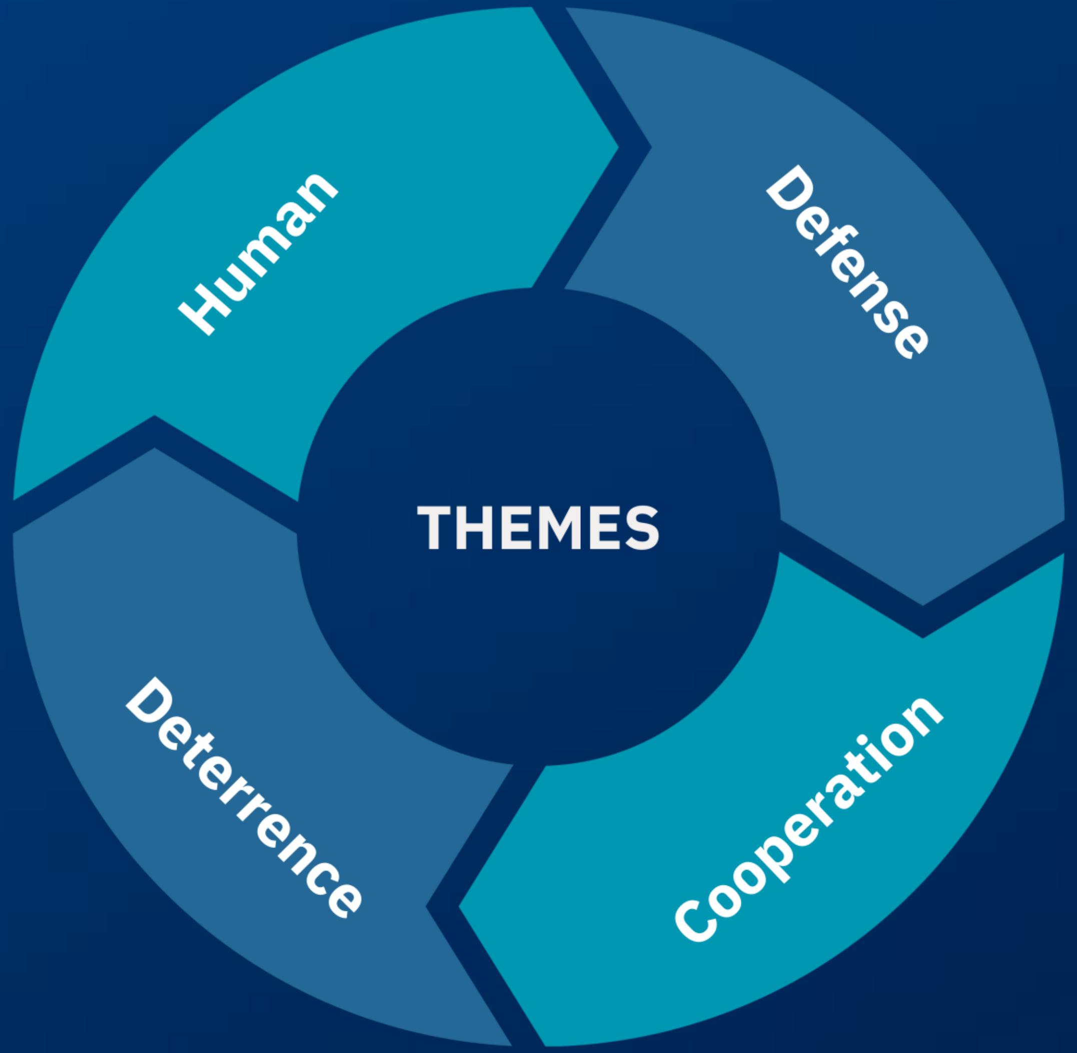
2024-2028

National Cyber Security Strategy and Action Plan 2024-2028

ULUSAL
SİBER GÜVENLİK
STRATEJİSİ VE EYLEM PLANI
2024-2028

- ✓ 4 THEMES
- ✓ 6 STRATEGIC OBJECTIVES
- ✓ 18 TARGETS
- ✓ 61 ACTION ITEMS

Themes and Strategic Objectives



- Human-Centered Cyber Security Approach
- Safe Use of Technology and Its Contribution to Cyber Security
- Cyber Resilience

- Proactive Cyber Defense and Deterrence
- Domestic and National Technologies in Combating Cyber Threats
- Türkiye Brand in the International Arena

Legal Basis

- Abuse mitigation measures are implemented in accordance with the provisions outlined in the articles of Turkiye's Electronic Communications Law No. 5809

- Article 60, paragraph 11: The organization (ICTA / BTK) takes or have someone take **all kinds of necessary measures** to protect and deter against cyber attacks to government organizations, private and real entities.

Legal Basis

- Article 60, paragraph 12: The organization (ICTA / BTK) can receive and evaluate information, documents, data and records from relevant places within the scope of its duty; can benefit from archives, electronic data processing centers and communication infrastructure, contact them and can take or have someone take other necessary measures within this scope. In this context, all kinds of information and document requests requested by the Authority is carried out by the relevant ministry, institutions and organizations without delay.

Legal Basis

- Within the framework of legal regulations, the ".tr" ccTLD supports law enforcement in combating cyber-crime by implementing necessary technical and organizational measures to provide information and documents requested by authorities such as courts for the prevention, detection, and investigation of abuse-related offenses.

What Types of ABUSIVE Activities?

- Phishing
- Malware Distribution
- Spam
- Domain Hijacking
- Botnet Command and Control (C2)
- Child Exploitation Materials
- Fraud and Scams
- DNS Abuse (e.g., DNS Hijacking, DNS Spoofing)
- Privacy Violations

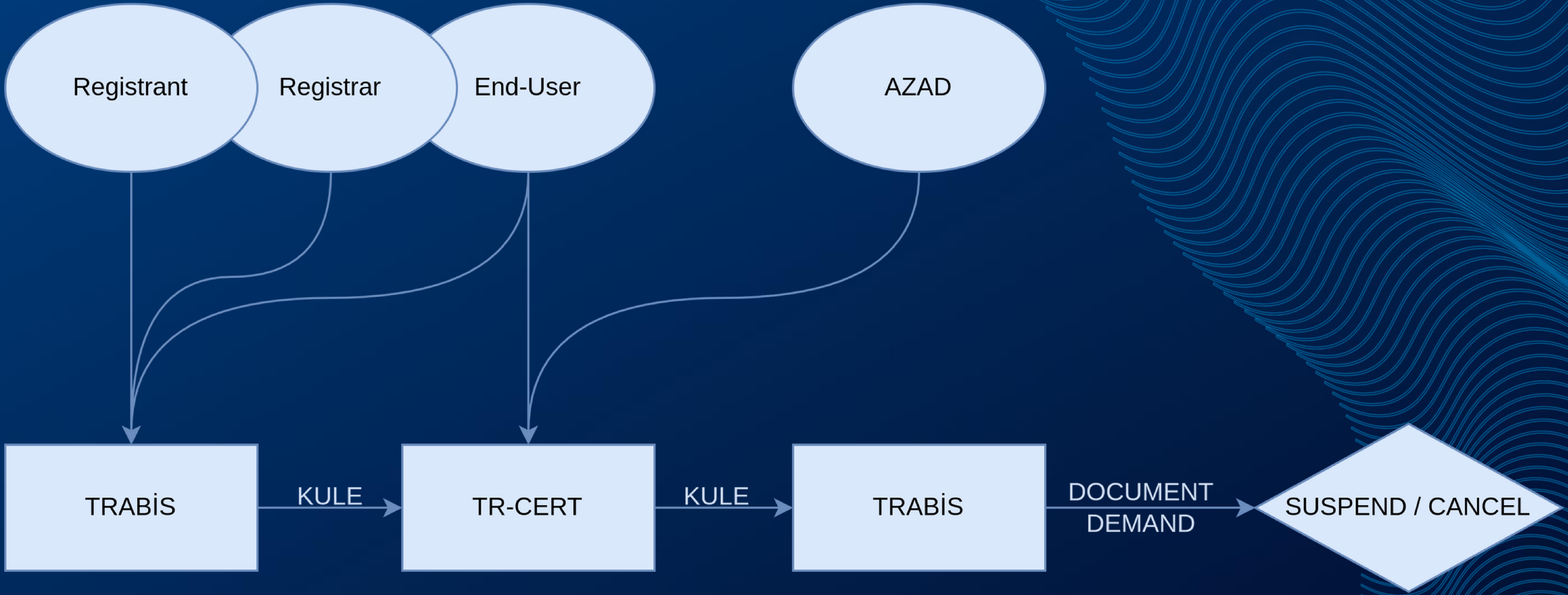
AZAD

The AZAD project optimizes the use of artificial intelligence technologies, enhancing the ability to detect malicious activities, identify threats in advance.

In this way, phishing addresses targeting users in Türkiye are detected and blocked before or as soon as they become active.

To quickly and effectively manage domain name Abuse complaints, information flow and incident management between TRABIS and TR-CERT are conducted through the KULE application.

DNS Abuse Flow in TRABİS



Kule Incident Statistics

Complaints: 13K

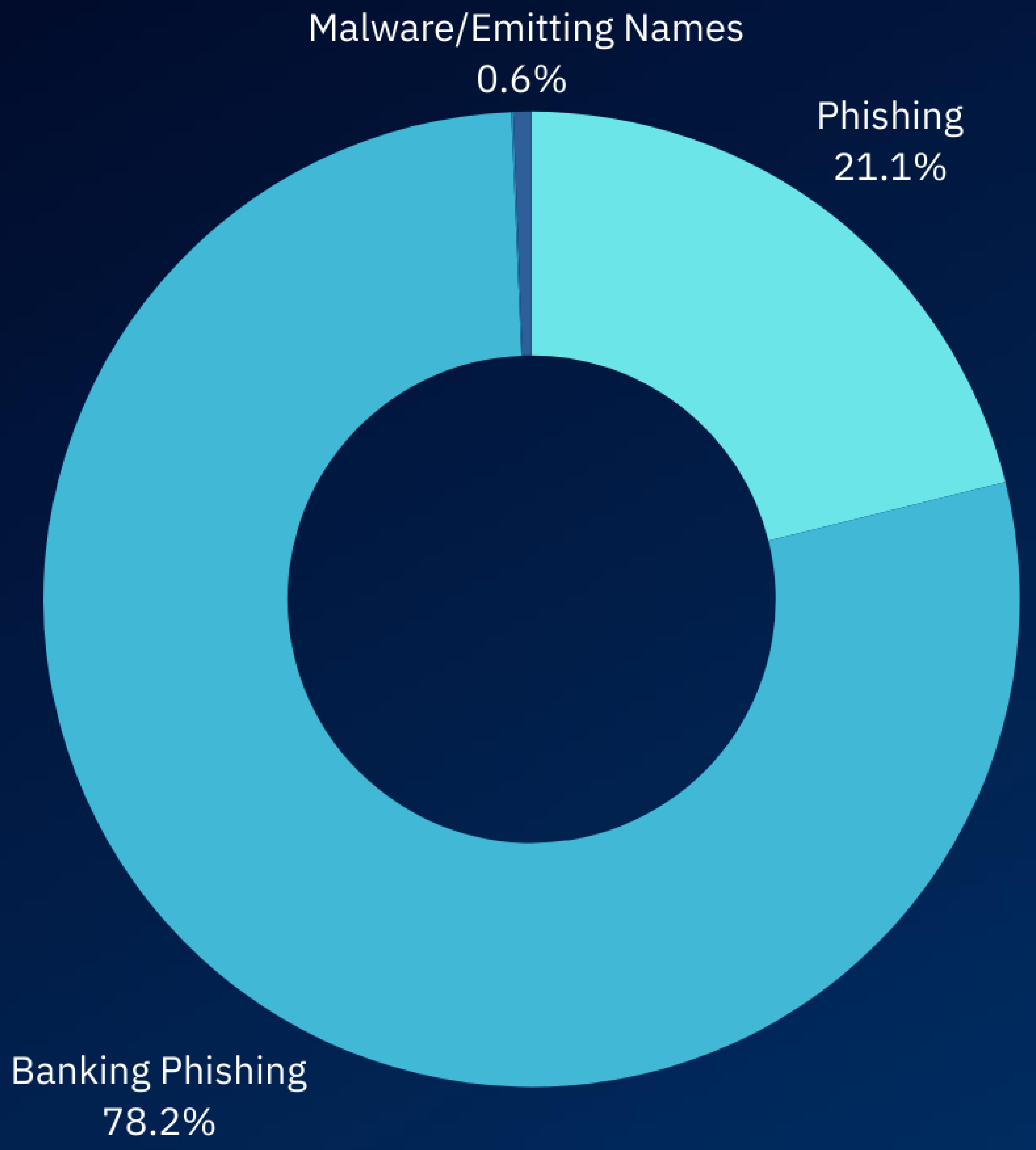
Abuse: 5K

Re-activate: 5

INCIDENTS: 8K

AZAD: 62

Abuse Statistics



TYPE	NUMBER
Phishing	**932**
Banking Phishing	**3414**
Malware /Command Control	**3**
Malware/Emitting Names	**26**

Some Common Patterns & Restricted Names List

- Words such as complaint, application, dues, cancellation, loan used for **identity theft are** around 60 out of a total of 1300 sites opened for abuse purposes.

- The number of words containing banking does not exceed 20 because of the **restricted domain names list**.

- The list of restricted domain names includes terms like bank, finance, and ministry to prevent the allocation of fake domain names that could be used to deceive internet users by impersonating financial and government institutions.

- Domain names containing such words are subject to a secondary review and are only allocated to those who can provide valid documentation.

Mostly Used Abusive Words

Words used for abuse purposes primarily involve **shopping scams** and **credit card fraud**. Some mostly used WORDS:

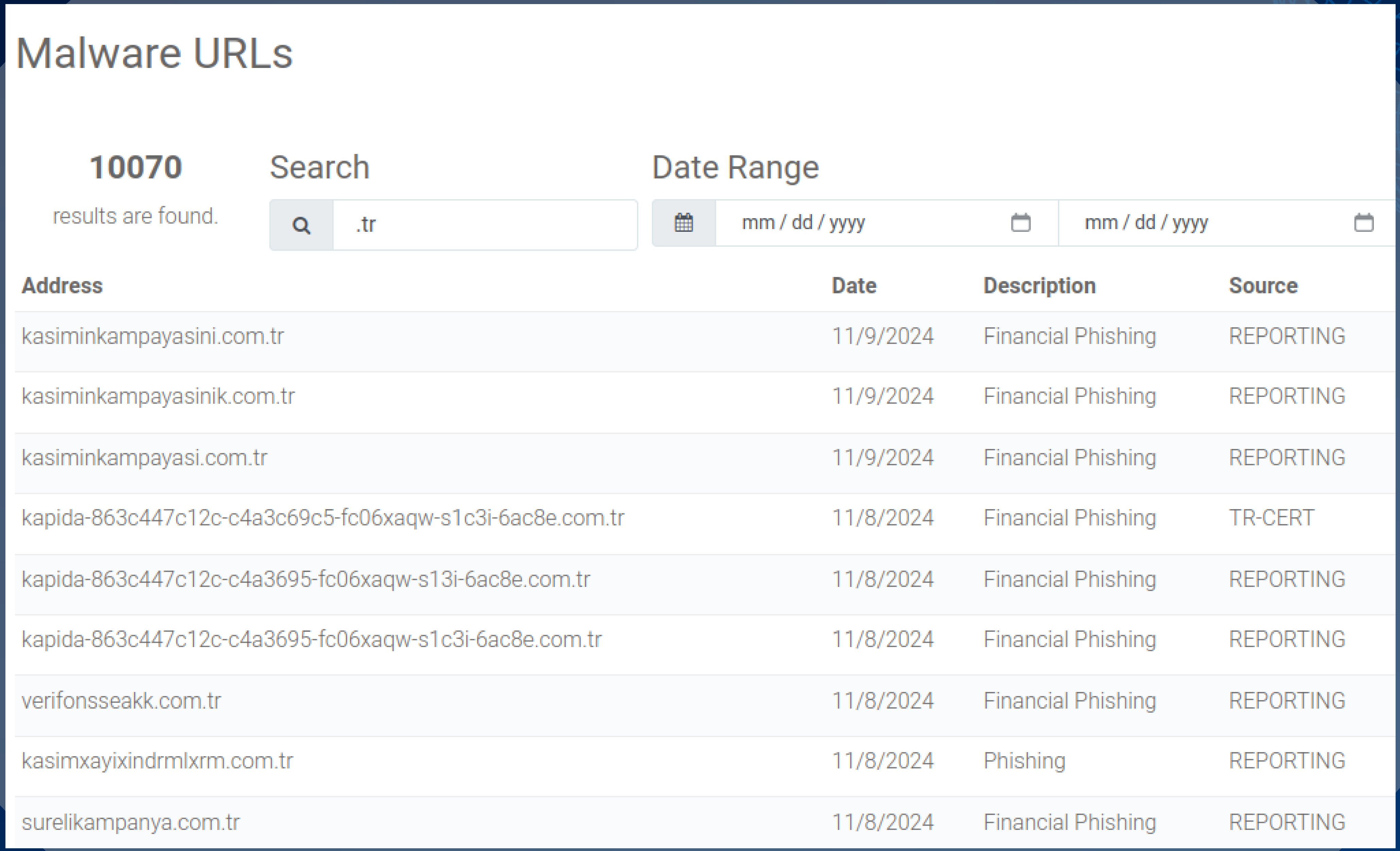
- **Fırsat: Opportunity**
- **İndirim: Discount**
- **Güven: Trust**
- **Çevrimiçi: Online**
- **Kampanya: Campaign**
- **Sepet: Basket**
- **Kapında: Atyourdoor**

Some Turning Points

Before TRABIS	2022	2023	2025
Document-based registration model for com.tr, net.tr, org.tr	Documentless allocation of com.tr, net.tr, org.tr with the opening of TRABİS	TRABİS abuse mitigation mechanism with the support of TR-CERT and IA App	Enhancing the capabilities of abuse mitigation mechanism

Complaints Methods

- ihbar@usom.gov.tr
- Malware URLs Page
- usom.gov.tr



Malware URLs

10070
results are found.

Search
.tr

Date Range
mm / dd / yyyy
mm / dd / yyyy

Address	Date	Description	Source
kasiminkampayasini.com.tr	11/9/2024	Financial Phishing	REPORTING
kasiminkampayasinik.com.tr	11/9/2024	Financial Phishing	REPORTING
kasiminkampayasi.com.tr	11/9/2024	Financial Phishing	REPORTING
kapida-863c447c12c-c4a3c69c5-fc06xaqw-s1c3i-6ac8e.com.tr	11/8/2024	Financial Phishing	TR-CERT
kapida-863c447c12c-c4a3695-fc06xaqw-s13i-6ac8e.com.tr	11/8/2024	Financial Phishing	REPORTING
kapida-863c447c12c-c4a3695-fc06xaqw-s1c3i-6ac8e.com.tr	11/8/2024	Financial Phishing	REPORTING
verifonsseakk.com.tr	11/8/2024	Financial Phishing	REPORTING
kasimxayixindrmlxrm.com.tr	11/8/2024	Phishing	REPORTING
surelikampanya.com.tr	11/8/2024	Financial Phishing	REPORTING

Approach and Collaboration

- We are open to collaborating with GAC members to find the most effective policies for mitigating DNS abuse.
- We are curious about the abuse policies of ccTLDs of other countries.
- We would like to contribute our experiences to the community

Q & A / Contact

mesat.yildirim@btk.gov.tr

info@trabis.gov.tr