Fraudulent e-shops .es Case Study

54th TF-CSIRT meeting Warsaw, Poland

Javier Berciano

What is **INCIBE**?

Leading company in **cybersecurity and digital trust development** for:

The public

Companies, especially those in **strategic sectors**

The academic research network in Spain (RedIRIS)

It leads different cybersecurity **interventions at a national and international level**

CERTSI (Security and Industry CERT)

certsi_
SECURITY AND INDUSTRY CERT

A benchmark for the **technical resolution of cybersecurity incidents** that affect essential services

Awareness & Prevention

Detection & Mitigation

Response

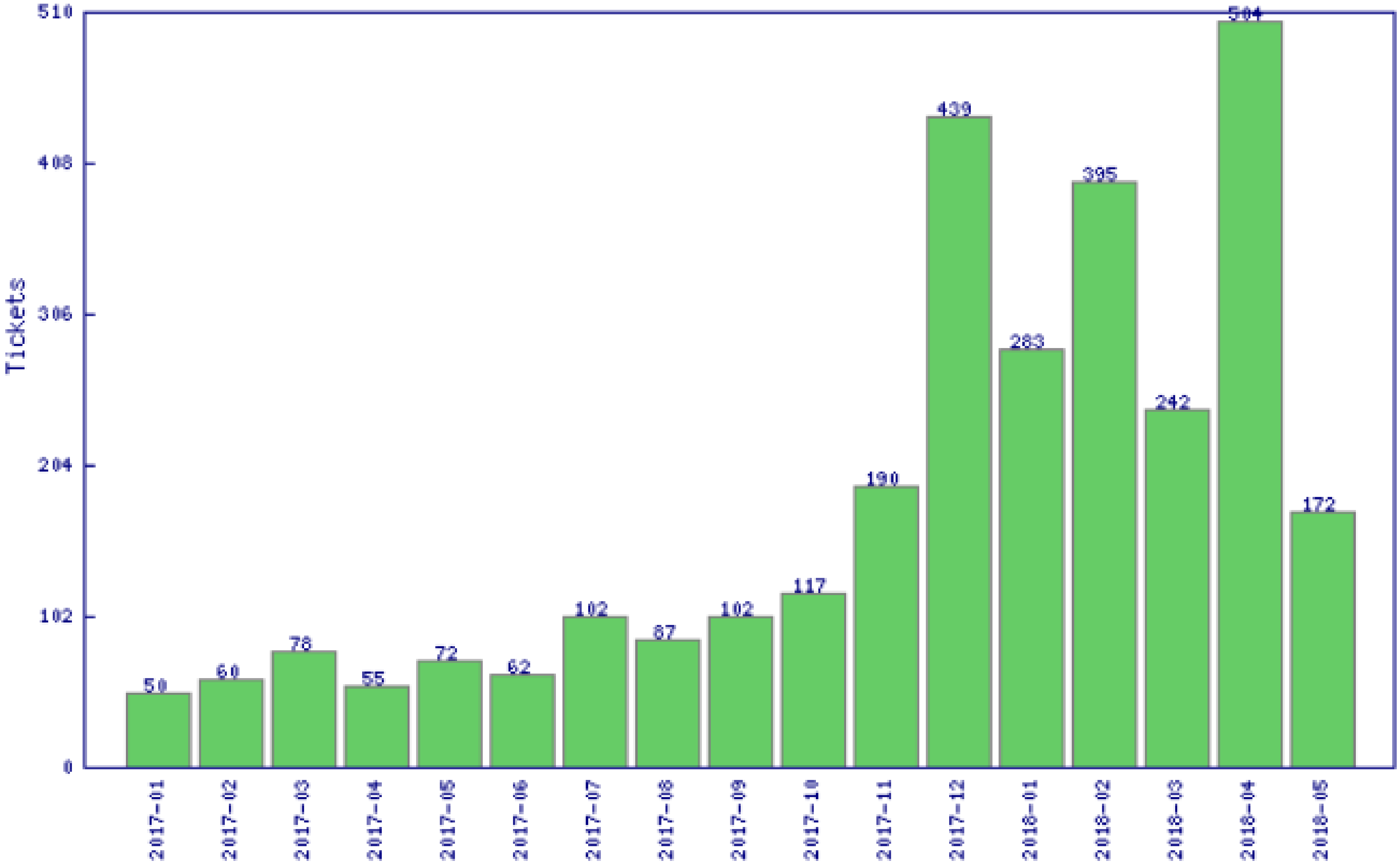
individuals

companies

critical infrastructure operators

academic and research network

Fraud Scam evolution

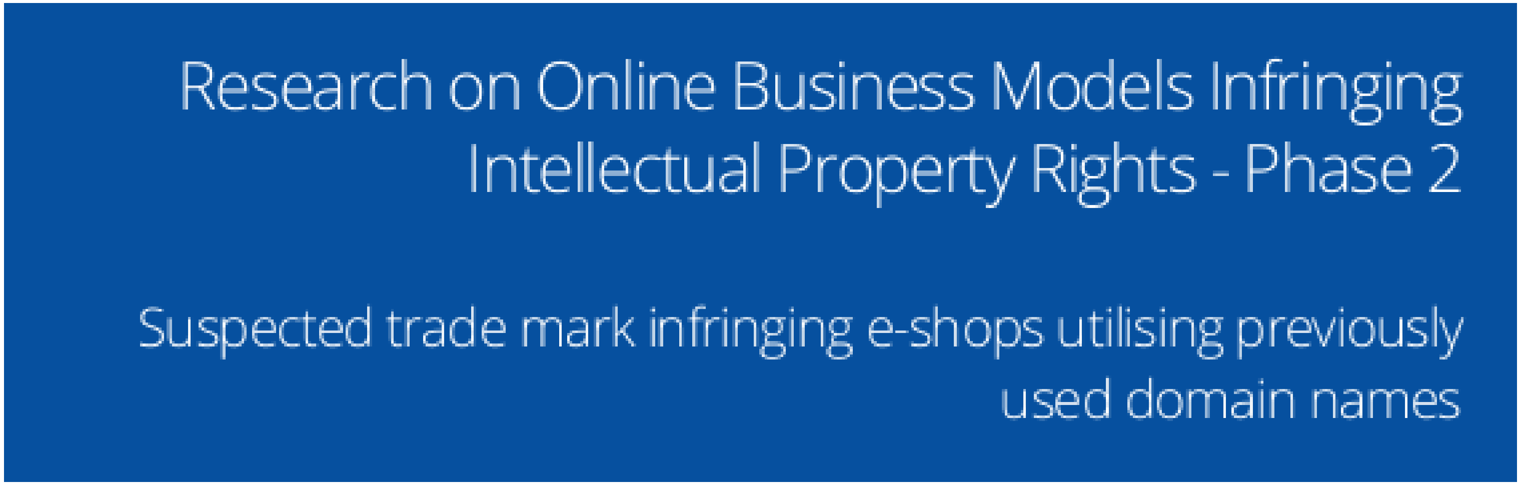


Main indicators

- Web content (trade marks)
- Domain contacts (email address and email provider)
- Re-activated domains (prior use of the domain names was completely unrelated to e-shop)

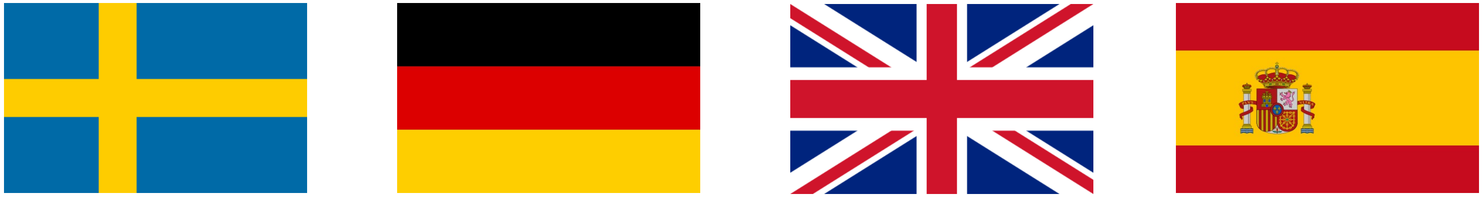
EUIPO research

EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE



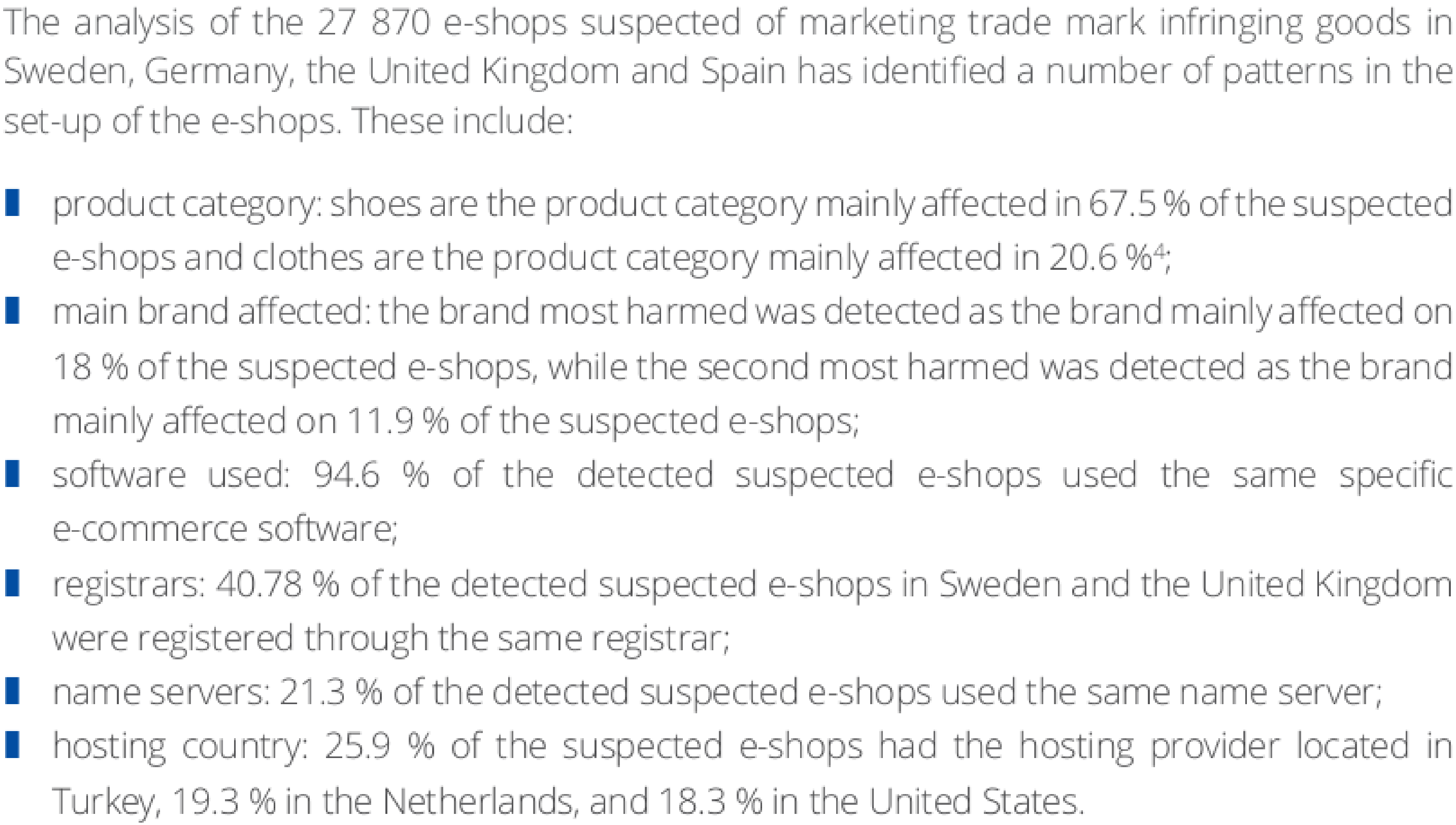
Research on Online Business Models Infringing Intellectual Property Rights - Phase 2

Suspected trade mark infringing e-shops utilising previously used domain names



Source: https://euipo.europa.eu/

EUIPO research



The analysis of the 27 870 e-shops suspected of marketing trade mark infringing goods in Sweden, Germany, the United Kingdom and Spain has identified a number of patterns in the set-up of the e-shops. These include:

- product category: shoes are the product category mainly affected in 67.5 % of the suspected e-shops and clothes are the product category mainly affected in 20.6 %[4];
- main brand affected: the brand most harmed was detected as the brand mainly affected on 18 % of the suspected e-shops, while the second most harmed was detected as the brand mainly affected on 11.9 % of the suspected e-shops;
- software used: 94.6 % of the detected suspected e-shops used the same specific e-commerce software;
- registrars: 40.78 % of the detected suspected e-shops in Sweden and the United Kingdom were registered through the same registrar;
- name servers: 21.3 % of the detected suspected e-shops used the same name server;
- hosting country: 25.9 % of the suspected e-shops had the hosting provider located in Turkey, 19.3 % in the Netherlands, and 18.3 % in the United States.

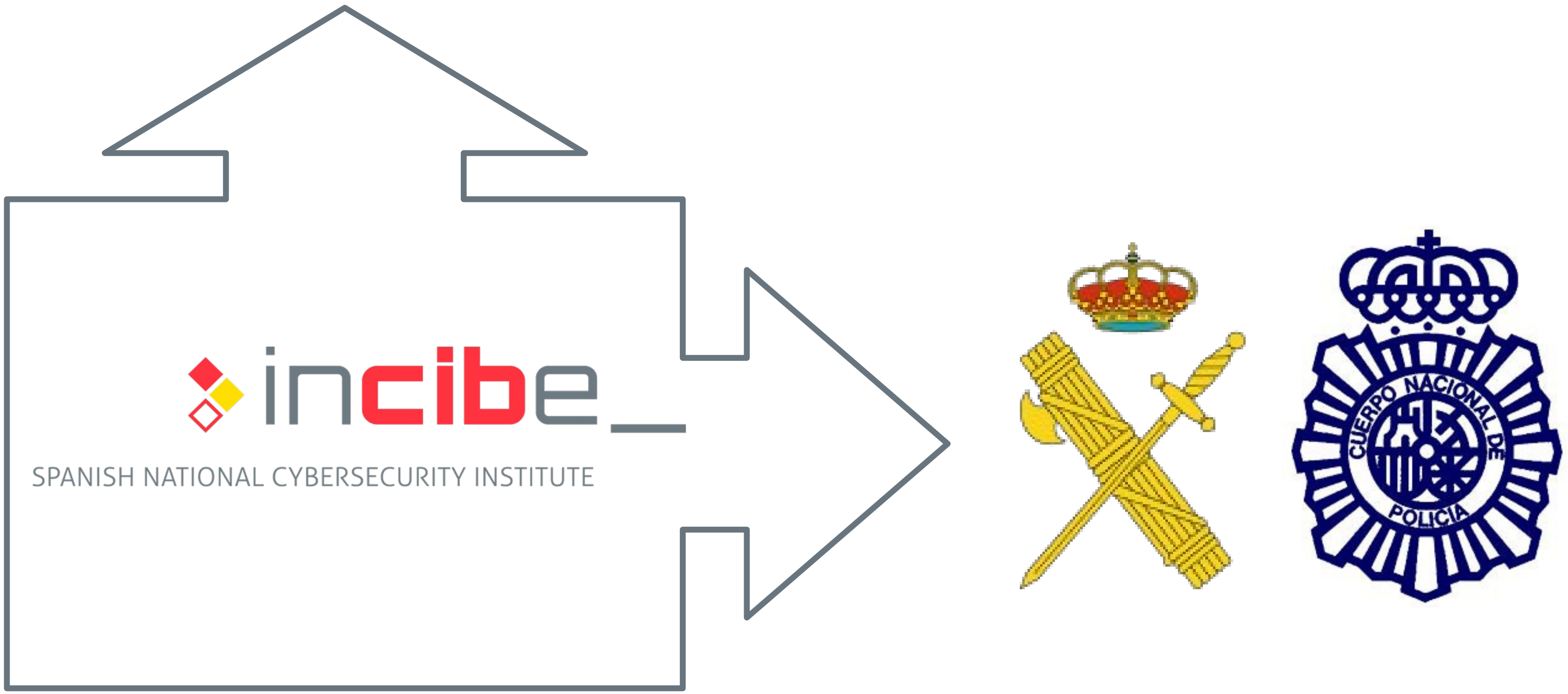
Source: https://euipo.europa.eu/

Collaboration

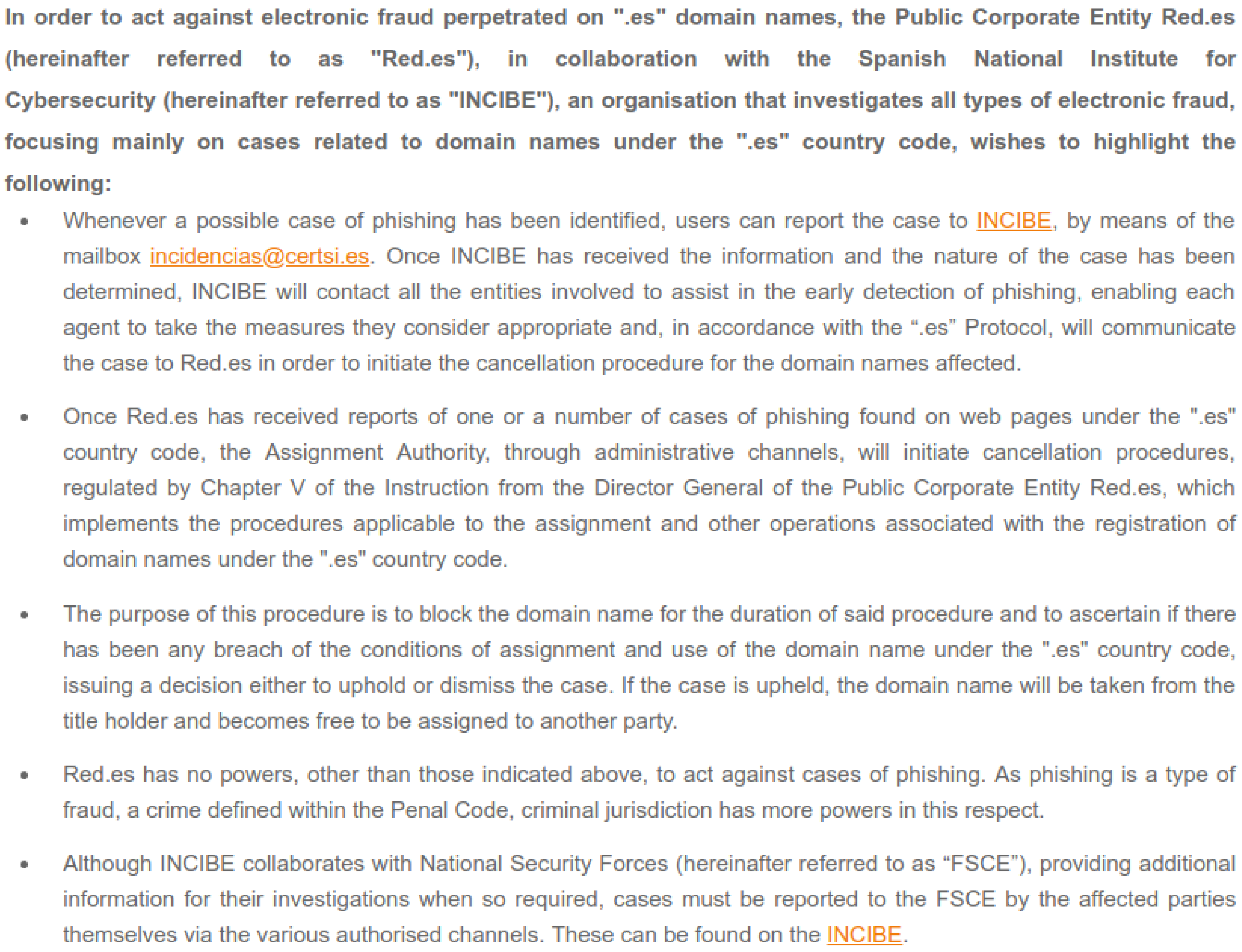
red.es

dominios es

& Internet Domain Registrars


incibe_
SPANISH NATIONAL CYBERSECURITY INSTITUTE
CUERPO NACIONAL DE POLICIA

.es ccTLD antiphishing



In order to act against electronic fraud perpetrated on ".es" domain names, the Public Corporate Entity Red.es (hereinafter referred to as "Red.es"), in collaboration with the Spanish National Institute for Cybersecurity (hereinafter referred to as "INCIBE"), an organisation that investigates all types of electronic fraud, focusing mainly on cases related to domain names under the ".es" country code, wishes to highlight the following:

- Whenever a possible case of phishing has been identified, users can report the case to INCIBE, by means of the mailbox incidencias@certsi.es. Once INCIBE has received the information and the nature of the case has been determined, INCIBE will contact all the entities involved to assist in the early detection of phishing, enabling each agent to take the measures they consider appropriate and, in accordance with the “.es” Protocol, will communicate the case to Red.es in order to initiate the cancellation procedure for the domain names affected.

- Once Red.es has received reports of one or a number of cases of phishing found on web pages under the ".es" country code, the Assignment Authority, through administrative channels, will initiate cancellation procedures, regulated by Chapter V of the Instruction from the Director General of the Public Corporate Entity Red.es, which implements the procedures applicable to the assignment and other operations associated with the registration of domain names under the ".es" country code.

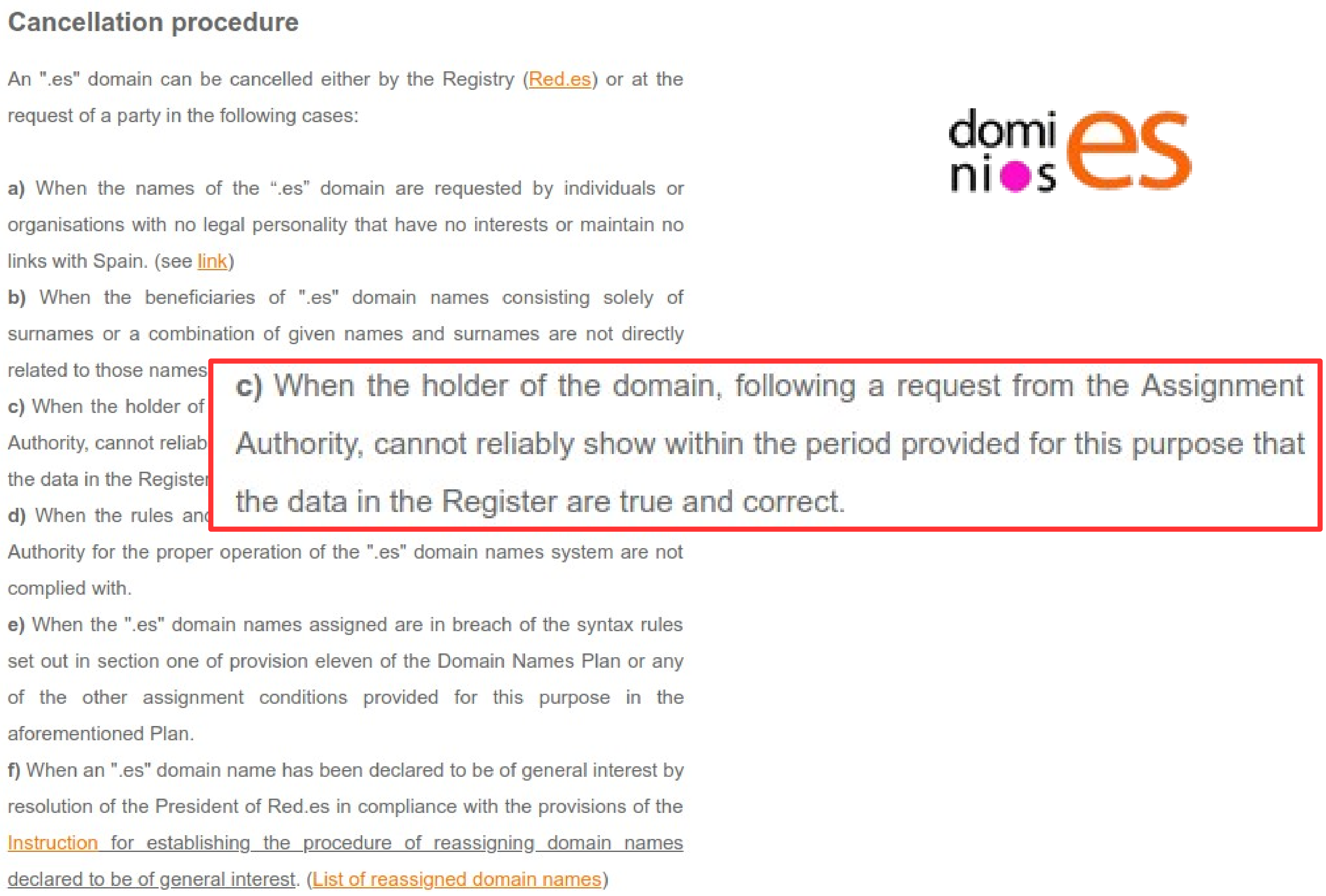
- The purpose of this procedure is to block the domain name for the duration of said procedure and to ascertain if there has been any breach of the conditions of assignment and use of the domain name under the ".es" country code, issuing a decision either to uphold or dismiss the case. If the case is upheld, the domain name will be taken from the title holder and becomes free to be assigned to another party.

- Red.es has no powers, other than those indicated above, to act against cases of phishing. As phishing is a type of fraud, a crime defined within the Penal Code, criminal jurisdiction has more powers in this respect.

- Although INCIBE collaborates with National Security Forces (hereinafter referred to as “FSCE”), providing additional information for their investigations when so required, cases must be reported to the FSCE by the affected parties themselves via the various authorised channels. These can be found on the INCIBE.

http://www.dominios.es/dominios/en/todo-lo-que-necesitas-saber/valores-anadidos/antiphising

.es ccTLD cancellation procedure



Cancellation procedure

An ".es" domain can be cancelled either by the Registry (Red.es) or at the request of a party in the following cases:

a) When the names of the “.es” domain are requested by individuals or organisations with no legal personality that have no interests or maintain no links with Spain. (see link)

b) When the beneficiaries of ".es" domain names consisting solely of surnames or a combination of given names and surnames are not directly related to those names

c) When the holder of the domain, following a request from the Assignment Authority, cannot reliably show within the period provided for this purpose that the data in the Register are true and correct.

d) When the rules and

Authority for the proper operation of the ".es" domain names system are not complied with.

e) When the ".es" domain names assigned are in breach of the syntax rules set out in section one of provision eleven of the Domain Names Plan or any of the other assignment conditions provided for this purpose in the aforementioned Plan.

f) When an ".es" domain name has been declared to be of general interest by resolution of the President of Red.es in compliance with the provisions of the Instruction for establishing the procedure of reassigning domain names declared to be of general interest. (List of reassigned domain names)

http://www.dominios.es/dominios/en/todo-lo-que-necesitas-saber/sobre-registros-de-dominios/cancelacion

Detection process

Automated

Risk index based on:
- whois data (contact information)
- web content analysis
- domain history

Semi - automated

Review of medium risk domains:
- suspicious email providers in contacts
- domain history

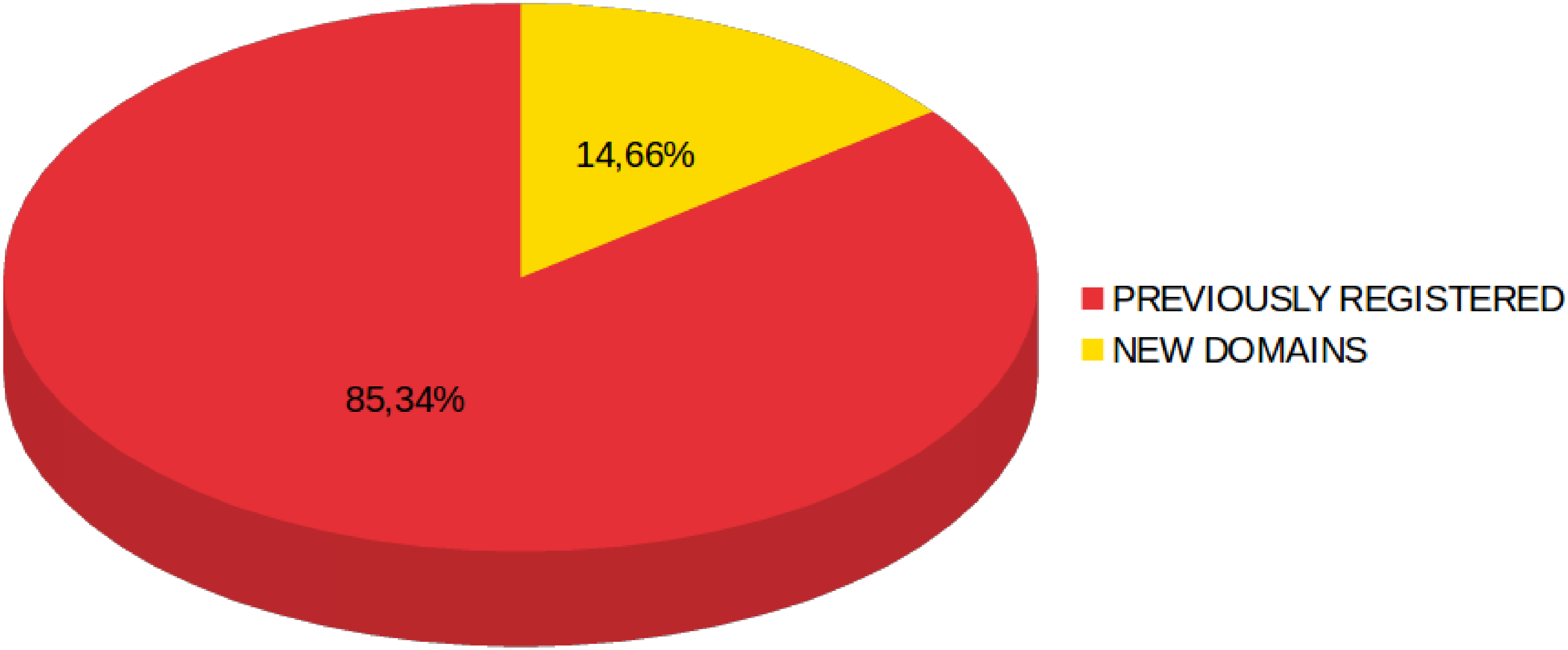
Improve detection rules

Statistics

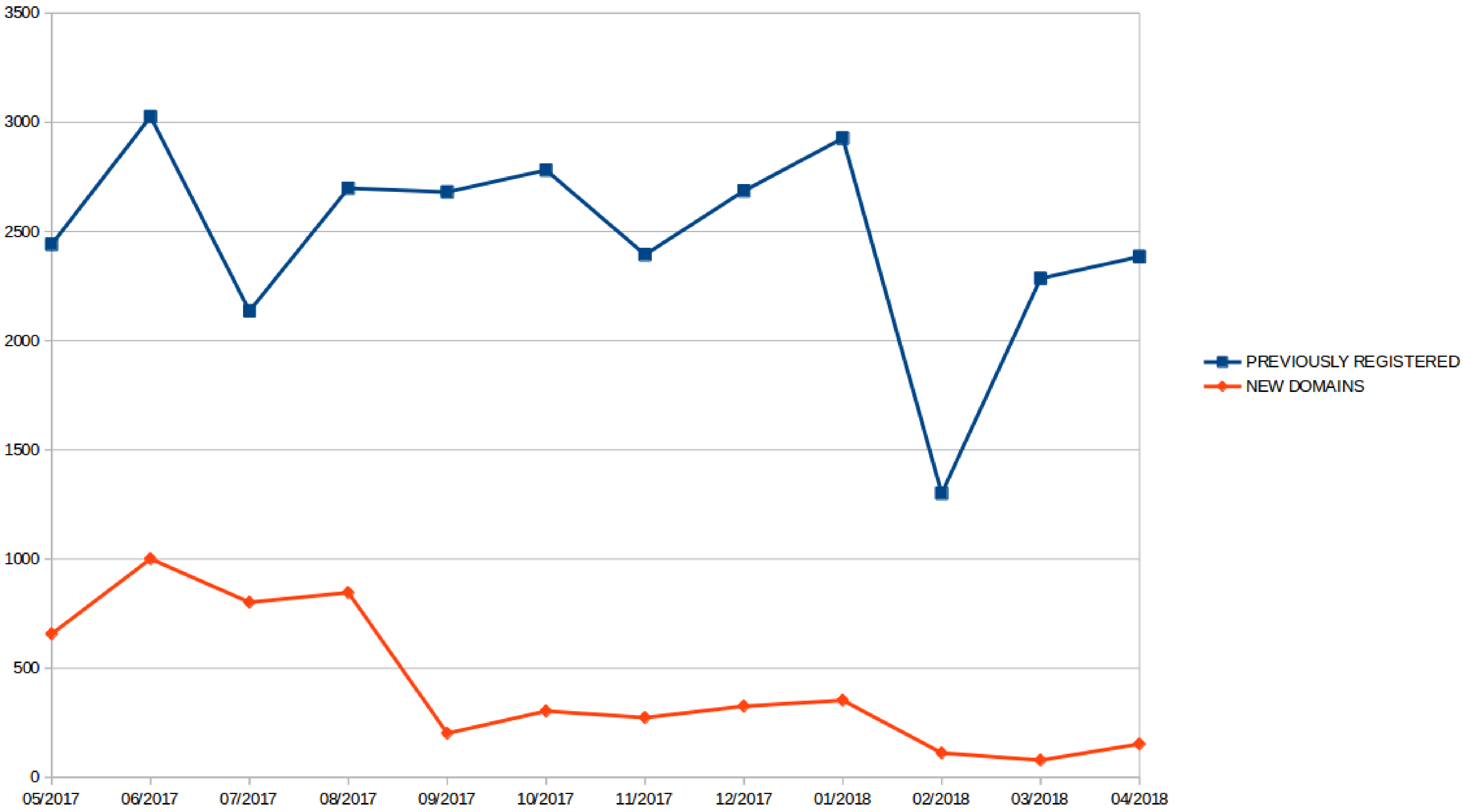
Fraudulent e-shops detected in 1 year

34.850

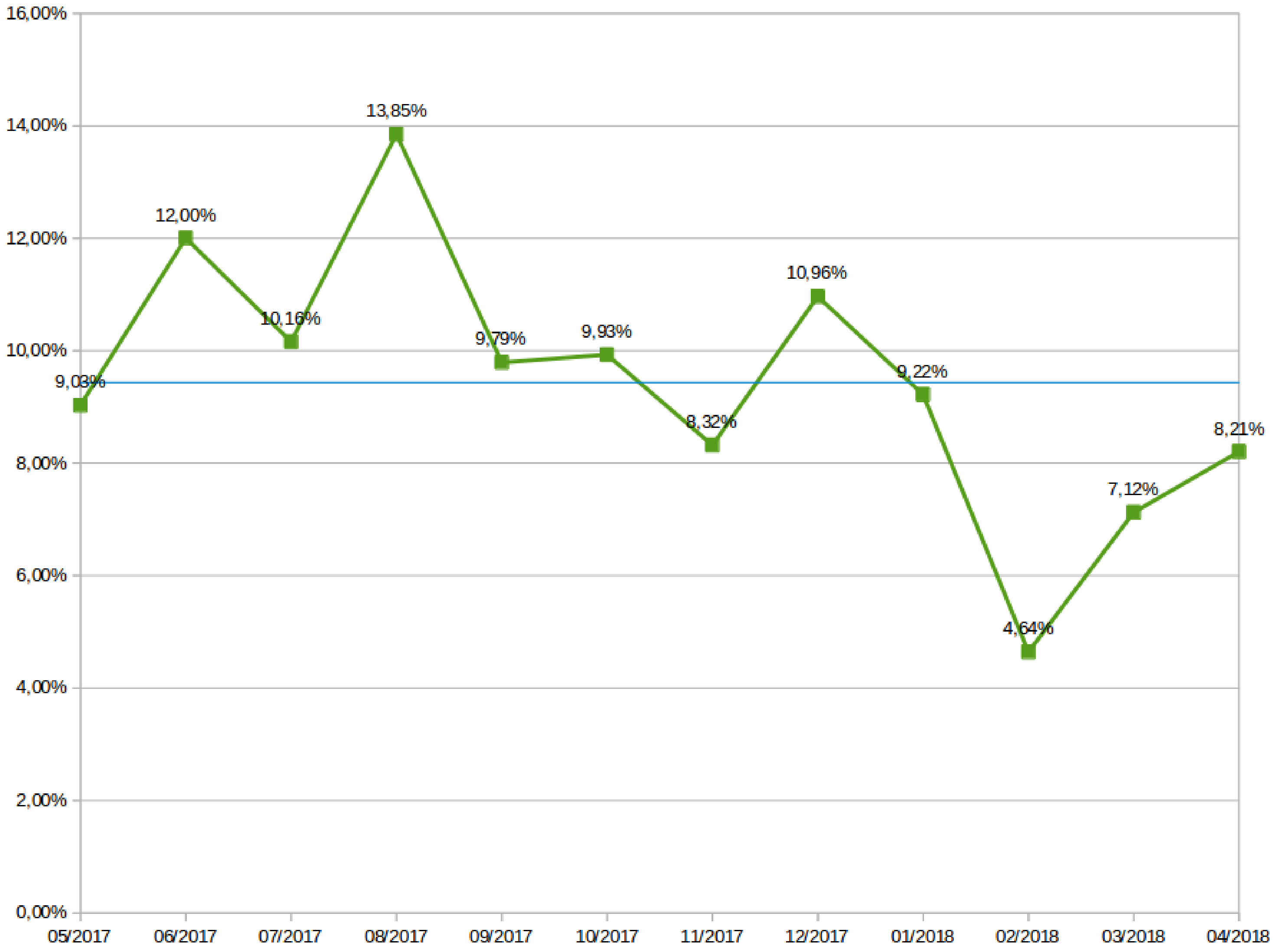
Previously registered?



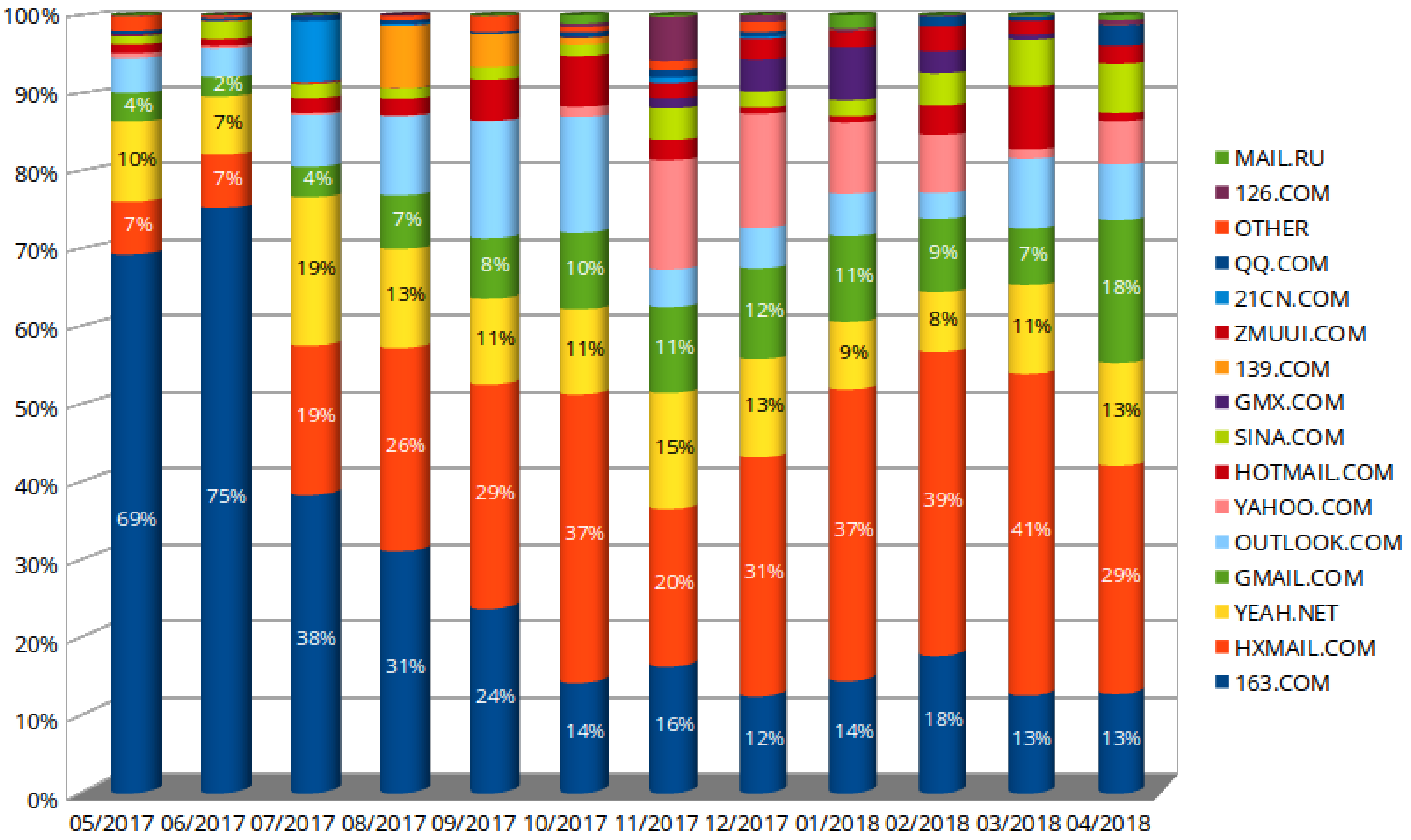
Fraudulent domains monthly evolution



Evolution fraudulent e-shops registered monthly

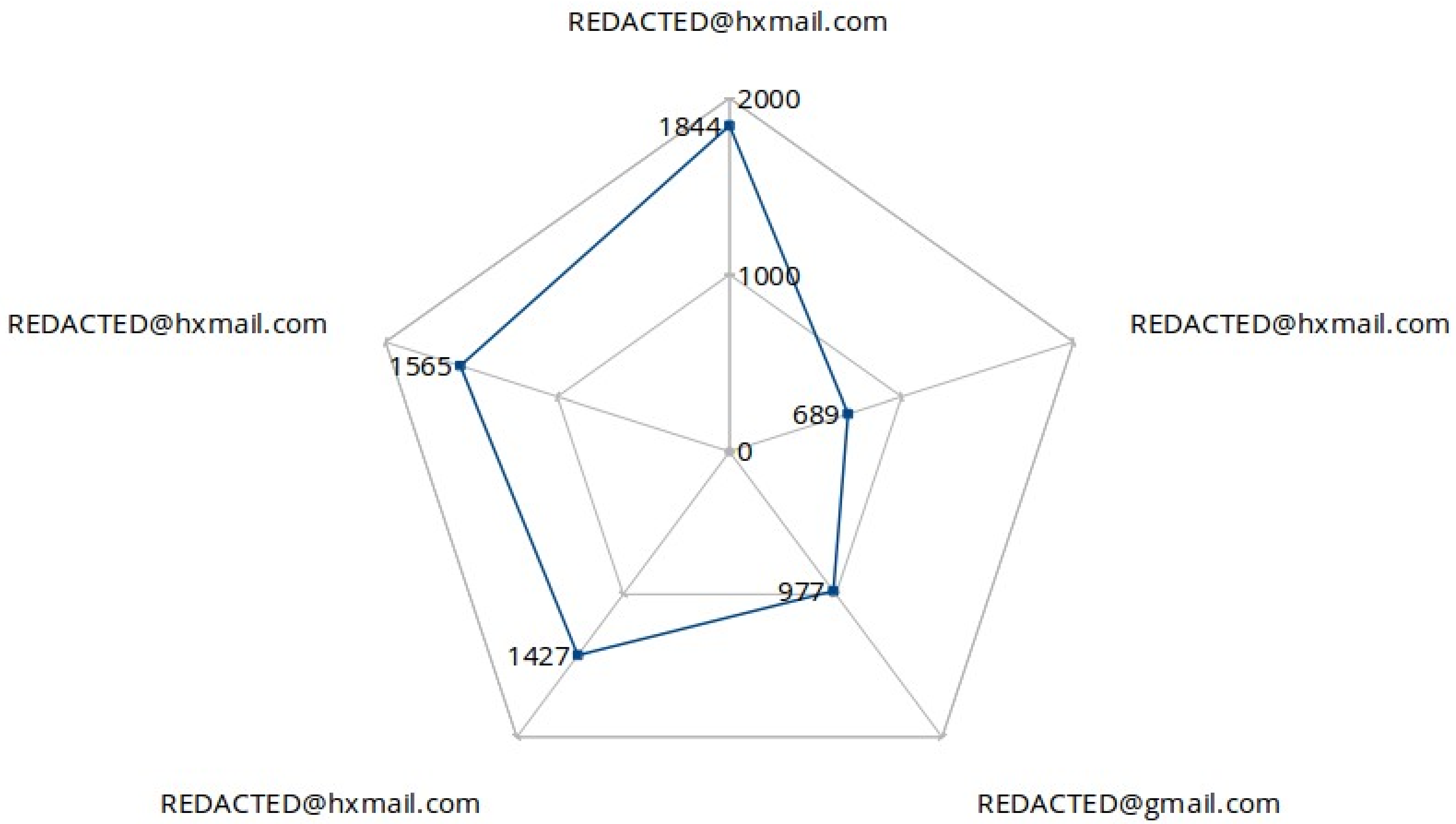


Contacts by domain / email provider

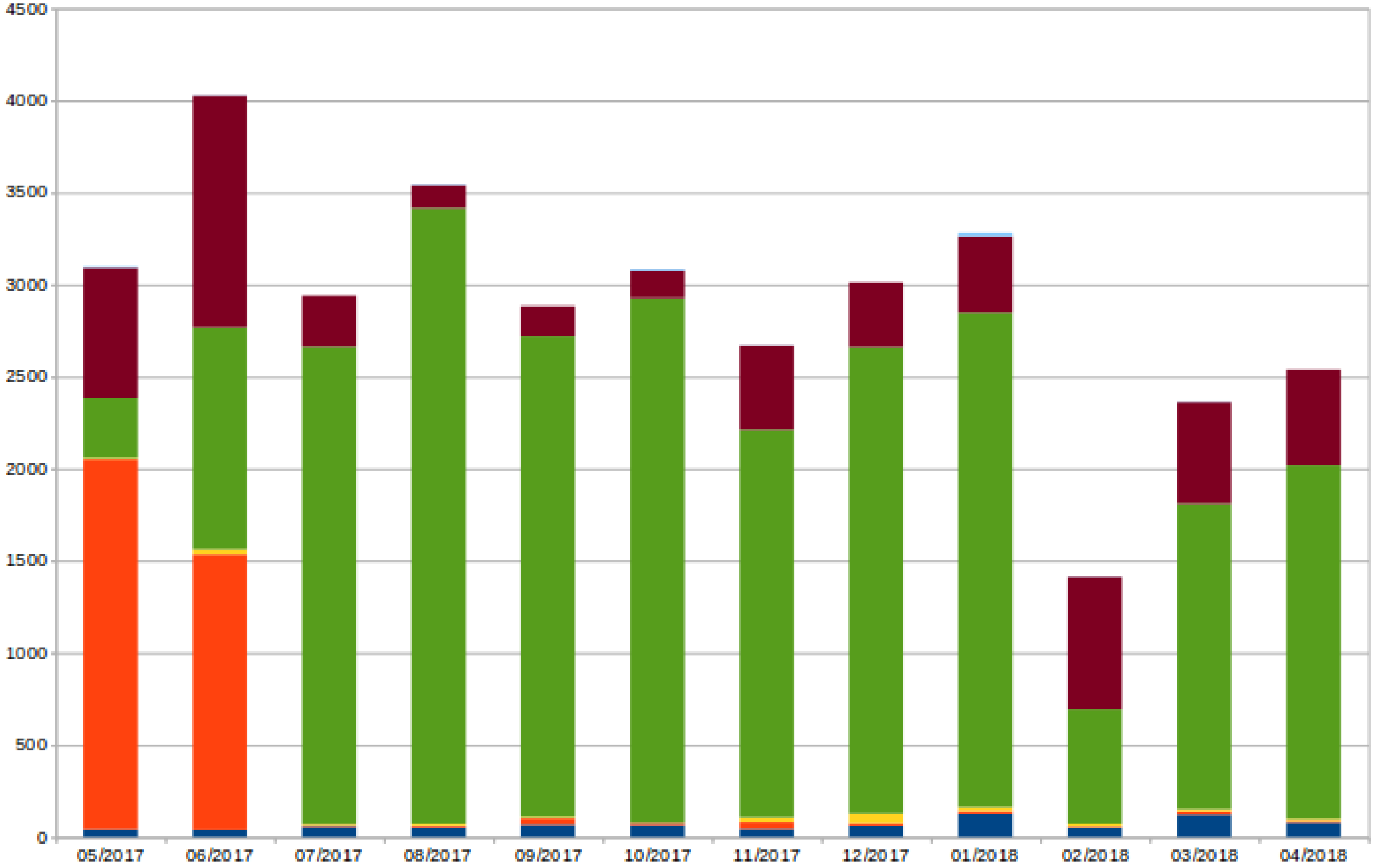


Top 5 actors

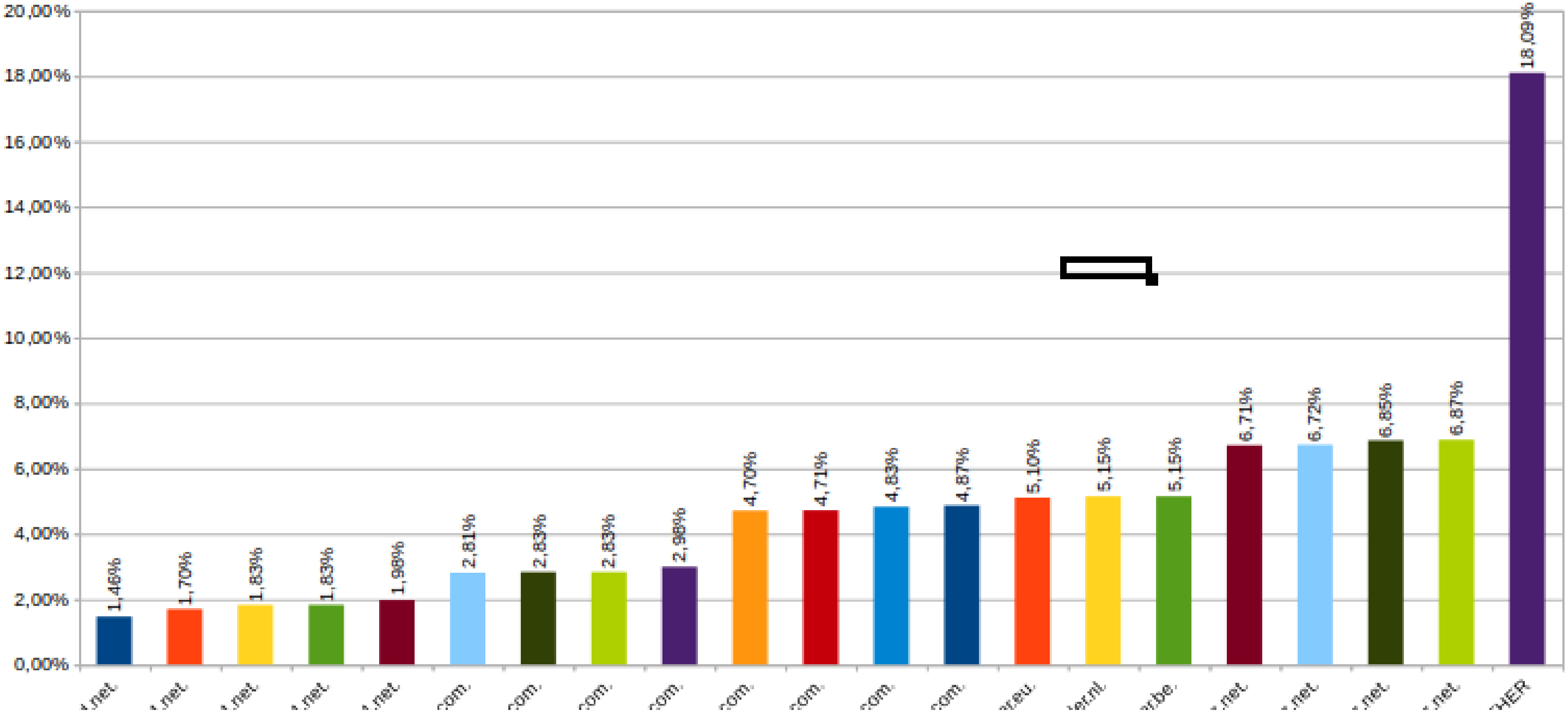
18,65% suspicious domains were registered using **5 email addresses**
Those 5 email addresses have **6.502** domains registered



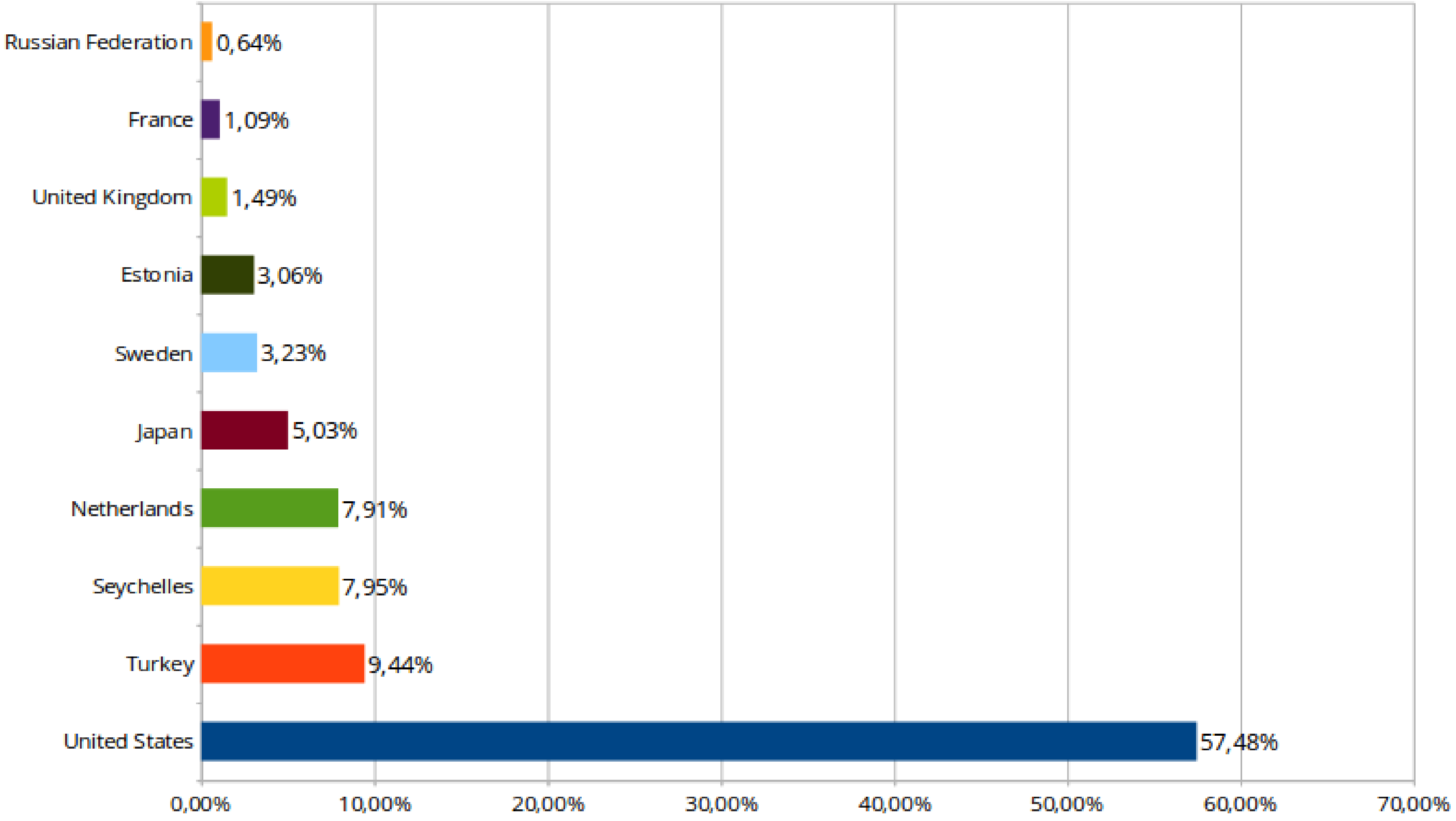
Domain Name Registrar distribution



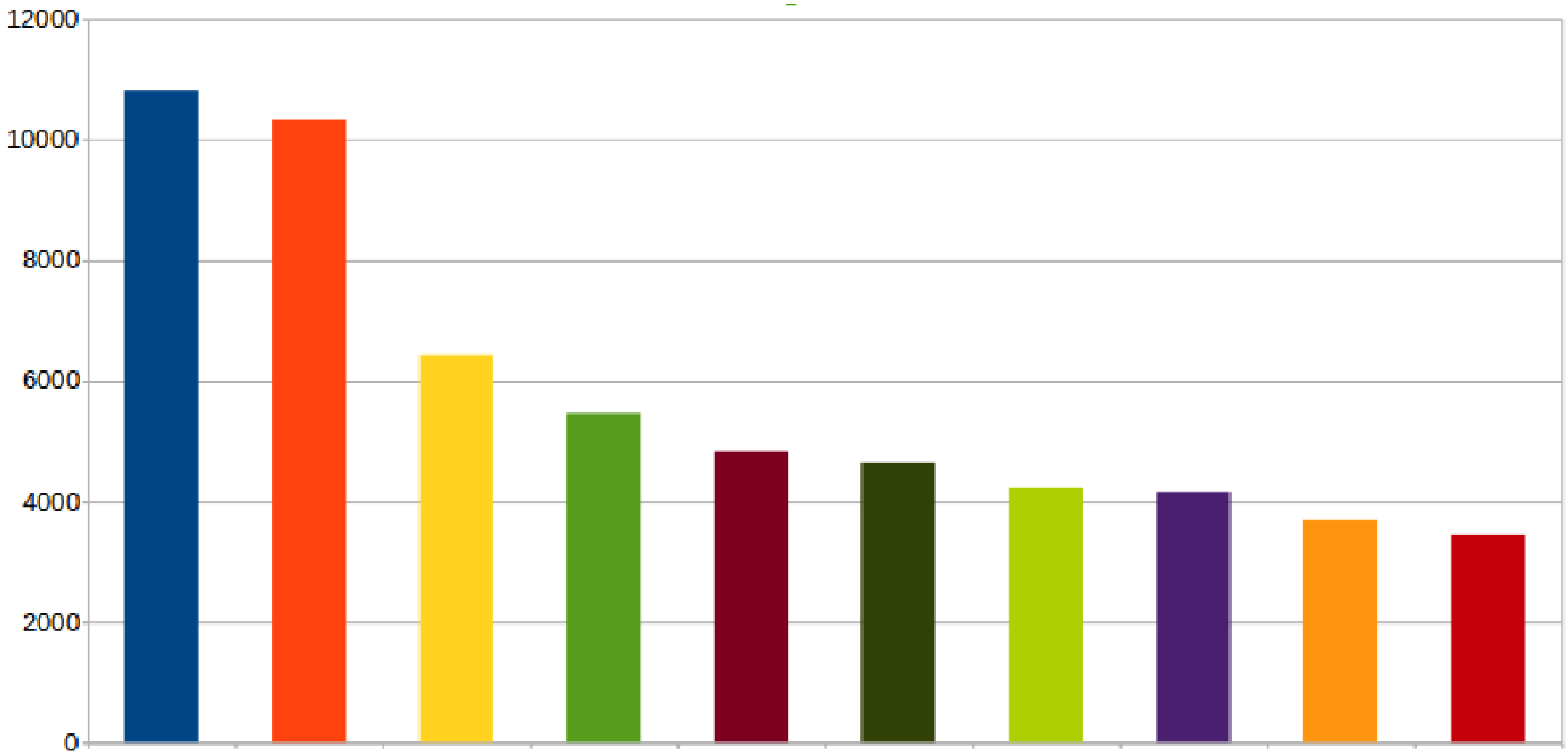
Nameservers distribution



Hosting by country



Main brands affected



Summary: May '17 ~ April '18

At least 9,35% (34.850 of 372.542) of the registered domains in last year hosted a fraudulent e-commerce site.

Registrars used were mainly 3 with more than 97% of fraudulent domains: 1st 70,16%, 2nd 16,36% and 3rd 10,50%.

Email providers used as domain admin or technical contact in whois were mainly not commonly used in Spain.
The top 3 email providers, 163.com, hxmail.com and yeah.net are present in 67,87% of suspicious domain registration data.

Expired and re-registered domains were the 85,34% of discovered fraudulent domains.

Improvement proposals for ccTLD Registry

- Bulk cancellation requests ✔
- Preventive suspension deleting domain from DNS
- Block domain after cancellation at least until original expiration
- Strengthen registration checks

Thank you!

Javier Berciano
javier.berciano@incibe.es

www.incibe.es www.certsi.es

@certsi_

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
SPANISH NATIONAL CYBERSECURITY INSTITUTE