COORDINATION CENTER FOR TLD.RU/.РФ

REPORT ON THE COOPERATION OF COMPETENT ORGANIZATIONS AND DOMAIN NAME REGISTRARS

UNDER THE AGREEMENT WITH THE COORDINATION CENTER ON COUNTERING ILLEGAL USE OF DOMAINS .RU AND .РФ

November 2020

In 2012, the Coordination Center for TLD .RU/.РФ introduced the practice of cooperating with organizations competent in detecting of malicious activity. These organizations provide the Coordination Center and accredited registrars with information on websites containing illegal content, incidents of phishing, unauthorized access to information systems and spreading malware via domain names in .РФ and .RU. Registrars have the right to terminate the domain name delegation for violating websites. The Coordination Center currently works with ten competent organizations: Safe Internet League, Group-IB, Kaspersky Lab, RU-CERT, ROCIT, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), BI.ZONE, the Bank of Russia, Dr.Web and the National Computer Incident Response and Coordination Center.

Safe Internet League

GROUP-IB

kaspersky

RU-CERT

РОЦИТ

ROSKOMNADZOR

BI.ZONE Cybersecurity

Bank of Russia

Dr.WEB

NCIRCC NATIONAL COMPUTER INCIDENT RESPONSE & COORDINATION CENTER

Any user can complain about detecting of malicious activity by calling the hotline of any of these organizations. Response measures will be taken as soon as possible.

CCTLD.RU / КЦ.РФ
127083, MOSCOW, 8 MARTA STR., 1, BLD.12

TEL. +7(495)730-29-71
FAX +7(495)730-29-68

Over the reporting period (November 2020), the competent organizations filed a total of 885 reports with registrars on the websites in .RU and .РФ that contain illegal content.

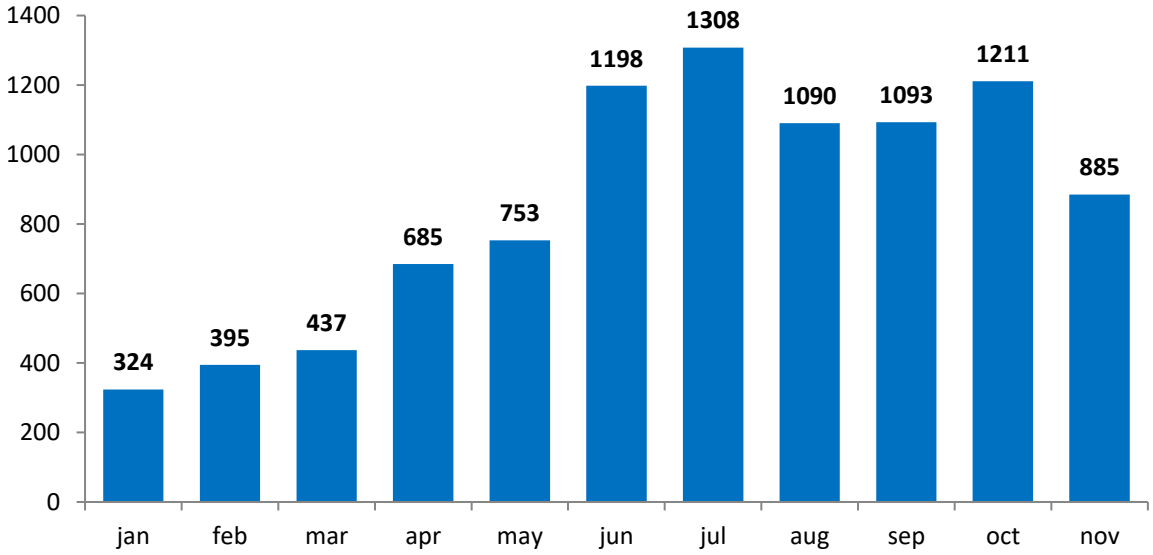

Fig.1 Reports filed with registrars

The analysis of domains by category of malicious activity detected over the reporting period indicates that the majority of domain names were involved in phishing (785 reports), followed by children porno (33 reports), spreading malware (38 reports), botnet controllers (2 reports). The competent organizations also filed 27 requests to verify registrants' identification data.

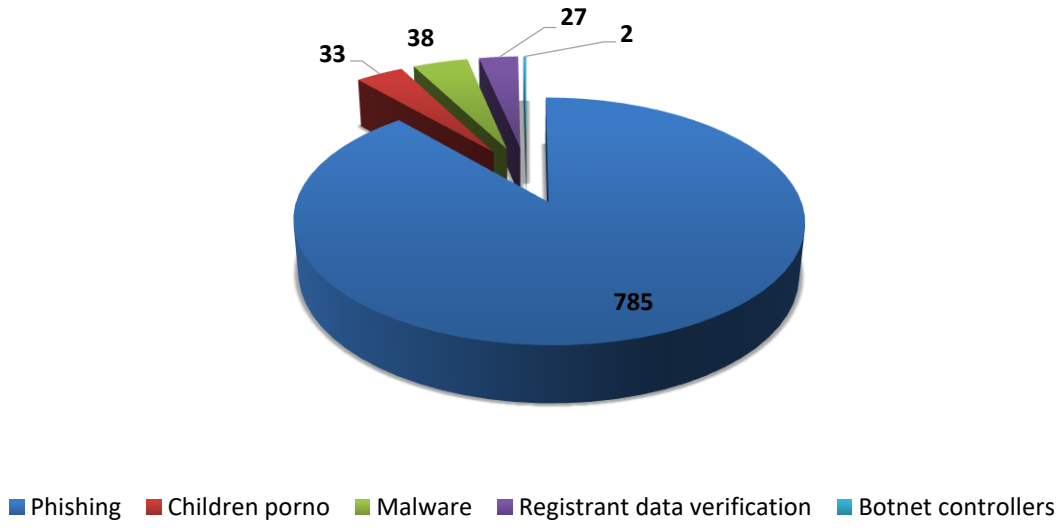

Fig.2 Breakdown by category of malicious activity (November 2020)

Delegation of 742 domain names was terminated over the reporting period following requests of the competent organizations. In 2 cases, termination of domain name delegation was not necessary as the domain registrants promptly verified its identification data. In 73 cases, termination of domain name delegation was not necessary as the violating website had been blocked by the hosting provider. In 37 cases, the registrar did not find sufficient grounds for terminating domain name delegation or initiating registrant verification. 21 reports were still being processed at the time of writing this report.

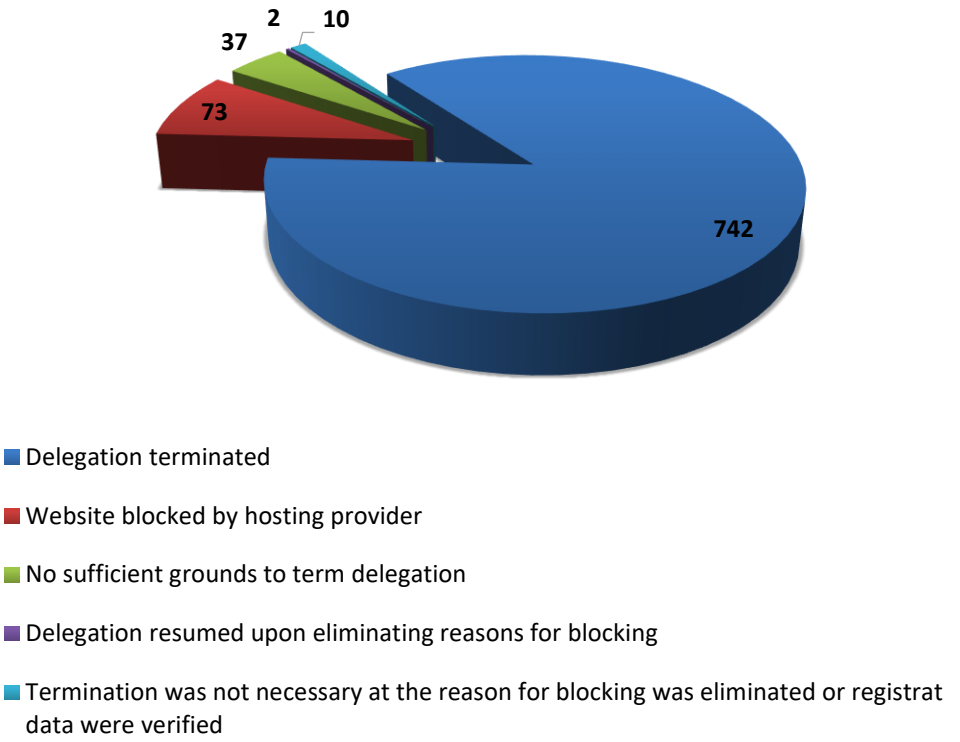

Fig.3 Outcome of termination of domain name delegation requests (November 2020)

Currently, 742 domain names remain blocked (in 10 cases, delegation was restored upon the request from the respective competent organization once the reason for blocking was eliminated).