

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 .PФ

August 2020

In 2012, the Coordination Center for TLD .RU/.PФ 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 .PФ 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.



Bank of Russia



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.

Over the reporting period (August 2020), the competent organizations filed a total of 1,090 reports with registrars on the websites in .RU and .PФ that contain illegal content.

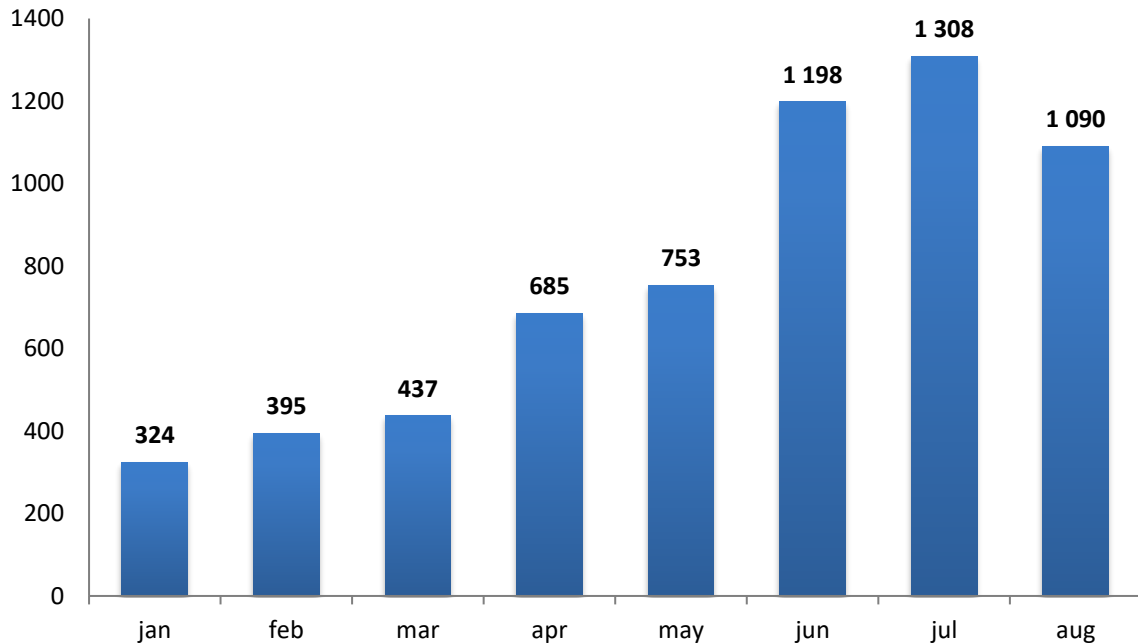


Fig.1 Reports filed with registrars

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 (976 reports), followed by children porno (50 reports), spreading malware (41 reports) and botnet controllers (1 report). The competent organizations also filed 22 requests to verify registrants' identification data.

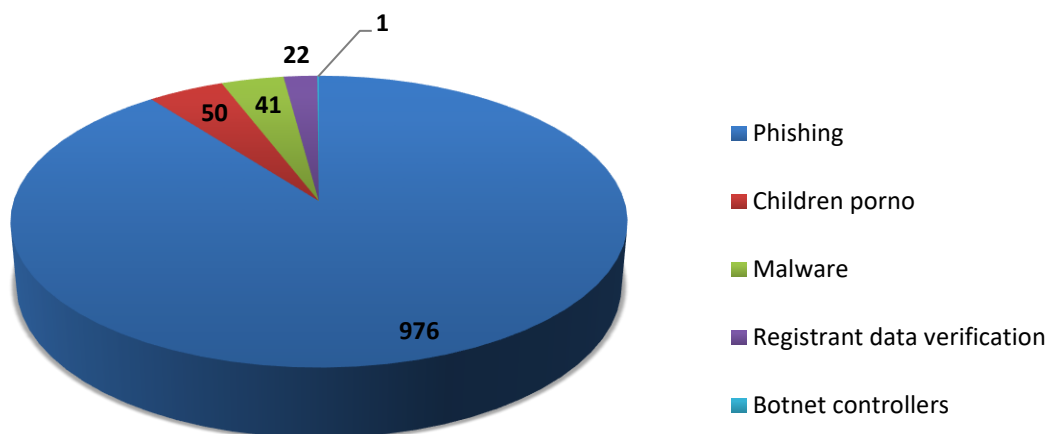


Fig.2 Breakdown by category of malicious activity (August 2020)

Delegation of 1,009 domain names was terminated over the reporting period following requests of the competent organizations. In one case, termination of domain name delegation was not necessary as the domain registrant promptly verified its identification data. In 42 cases, termination of domain name delegation was not necessary as the violating website had been blocked by the hosting provider. In 28 cases, the registrar did not find sufficient grounds for terminating domain name delegation or initiating registrant verification. Ten reports were still being processed at the time of writing this report.

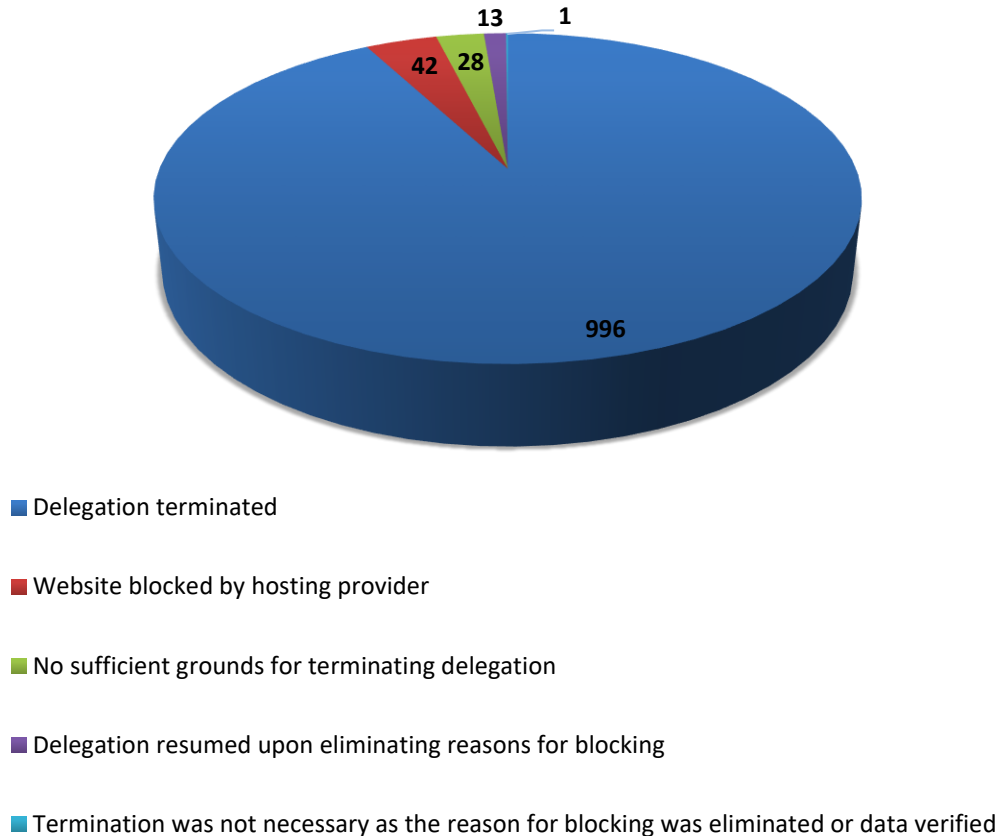


Fig.3 Outcome of termination of domain name delegation requests (August 2020)

Currently, 996 domain names remain blocked (in 13 cases, delegation was restored upon the request from the respective competent organization once the reason for blocking was eliminated).