Report on monitoring of phishing pages in 2016

This report presents results of analysis of phishing-related information acquired by RU-CERT in 2016.

Every day RU-CERT receives complaints against phishing sites, and actively carries out its own collection of information on new phishing attacks both in the Russian segment of the Internet and outside it.

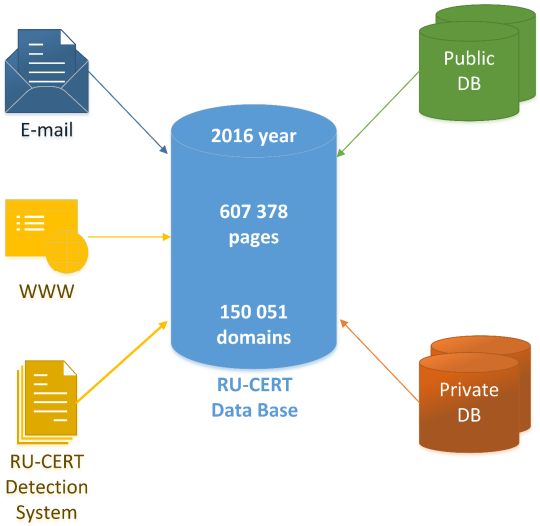
RU-CERT

Russian Computer Security Incident Response Team

RUSSIAN COMPUTER SECURITY INCIDENT RESPONSE TEAM
RU-CERT

Data sources

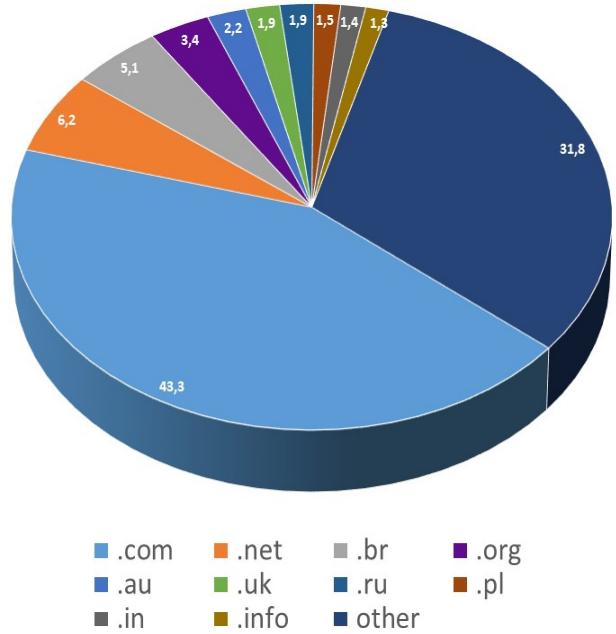
All received messages about phishing are entered in the RU-CERT database. In addition to complaints received via the web form available at www.cert.ru and by e-mail at info@cert.ru, RU-CERT performs its own analysis of a number of sources that provide access to their phishing databases.



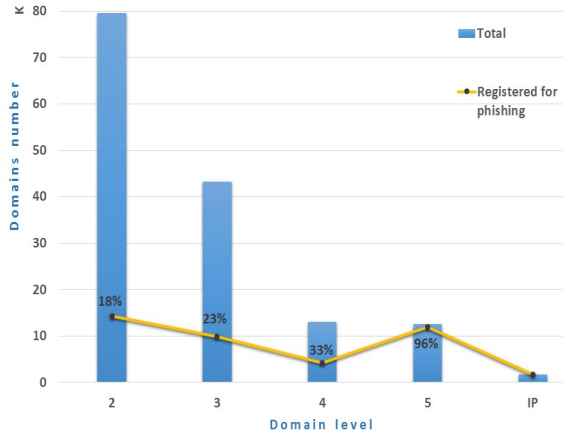
During 2016, RU-CERT through different channels received data about 607,378 phishing pages placed on 150,051 domains, i.e. on average there are 4.05 such pages on a domain.

Domains used

The analysis identified 207 different domain extensions (including gTLD) used for placing phishing pages.



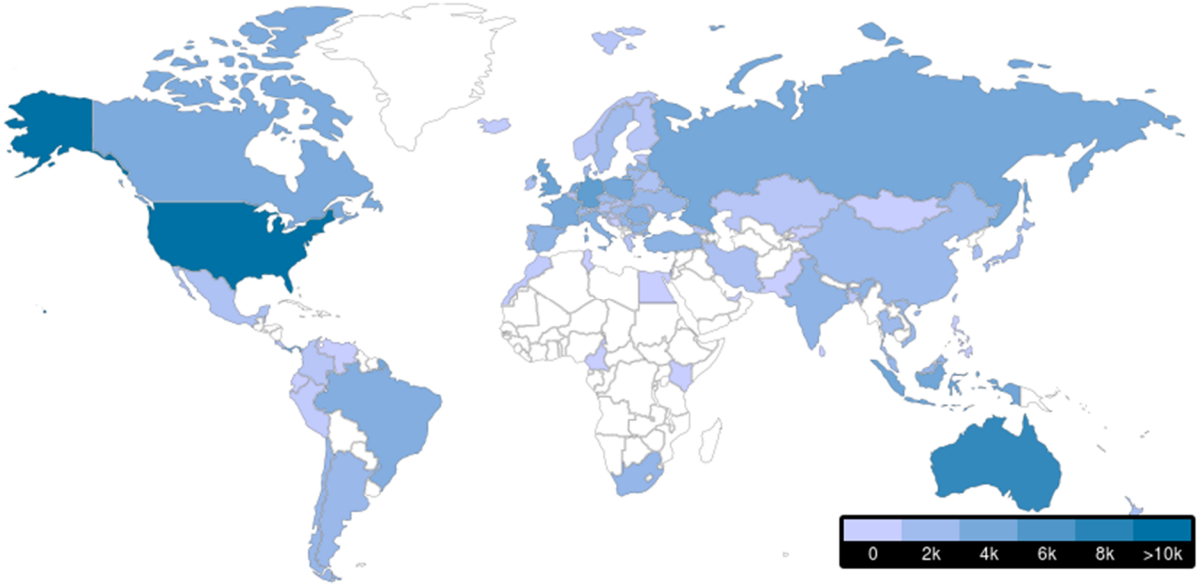
For the most part phishing was found on the second-level domains. The study revealed 19 domains of the level higher than 20, and the highest domain level observed is 32. The number of domains registered specifically for propagation of phishing increases with increasing domain level. This increase is explained by differing domain registration policies depending on the domain level. Domains of the third and higher levels are often issued by various services and free hostings without rigorous checks.



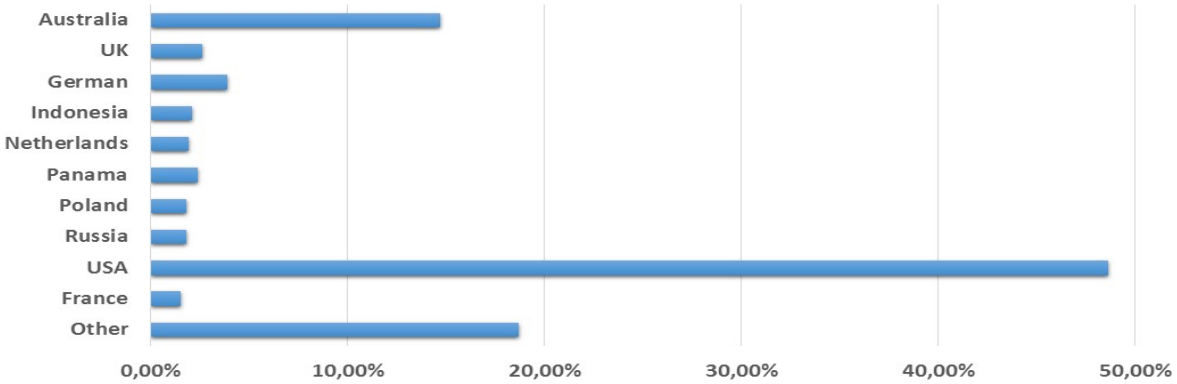
Specifically, 96% of level 5 domains where phishing pages were detected had been registered solely for phishing purposes. At the same time, the situation is different with the second-level domains: of about 80 thousand phishing pages detected on these domains only 18% were placed on domains registered specifically for this purpose, while the others were hacked.

Map of phishing distribution by countries

In 2016 RU-CERT established facts of placing phishing pages in 125 countries of the world.

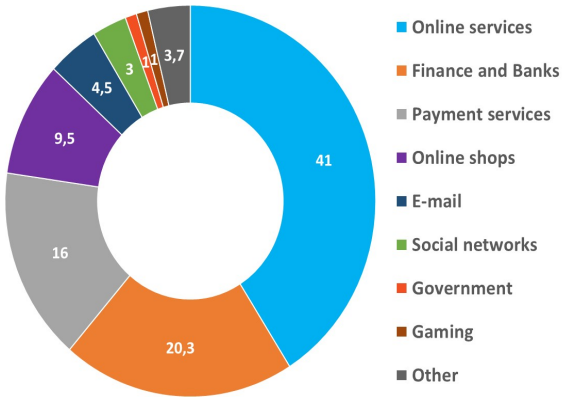


Leading countries in placing phishing

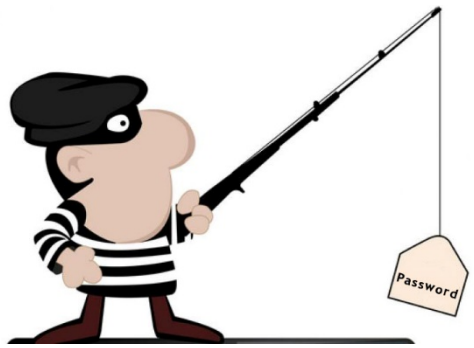


Compromised companies

As a rule, as their target group intruders choose users and clients of reputed banks, payment services, social networks and other companies providing services via Internet.

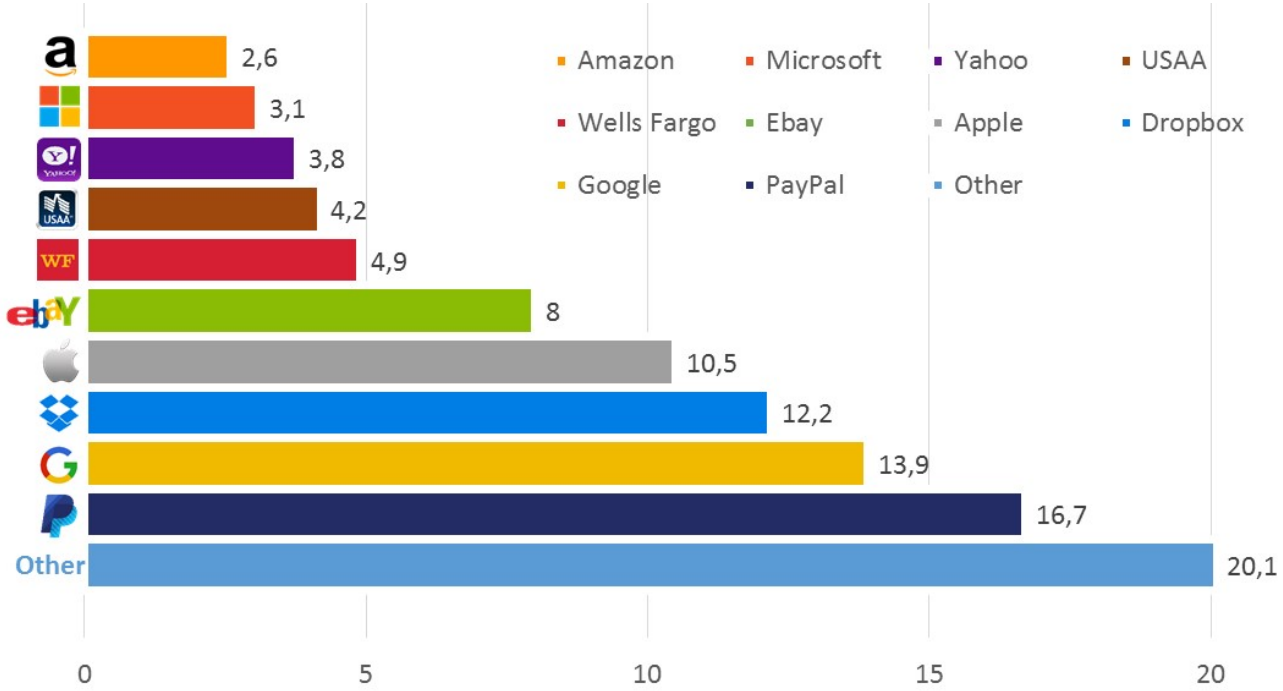


The majority of phishing attacks recorded in 2016 were directed at on-line services, banks and financial sector in general, as well as at various payment systems and online shops.



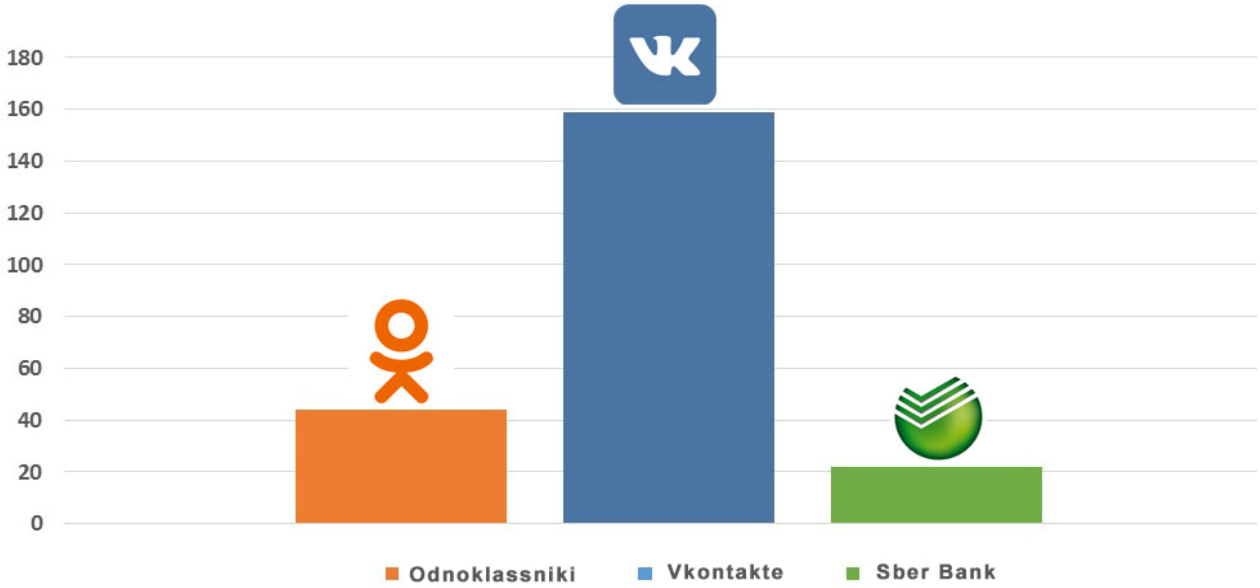
Global brands

PayPal payment service heads the list of major companies and services whose sites were targets of phishing attacks in the last year. Google and Apple services, and Dropbox file hosting are also at the top of the list.



Our national brands

261 phishing sites of domestic companies were detected in 2016 (0.2% of the total number of revealed phishing sites). The majority of recorded phishing attacks were directed at sites of VKontakte and Odnoklassniki social networks. The site of Sberbank of Russia was also attacked many times.



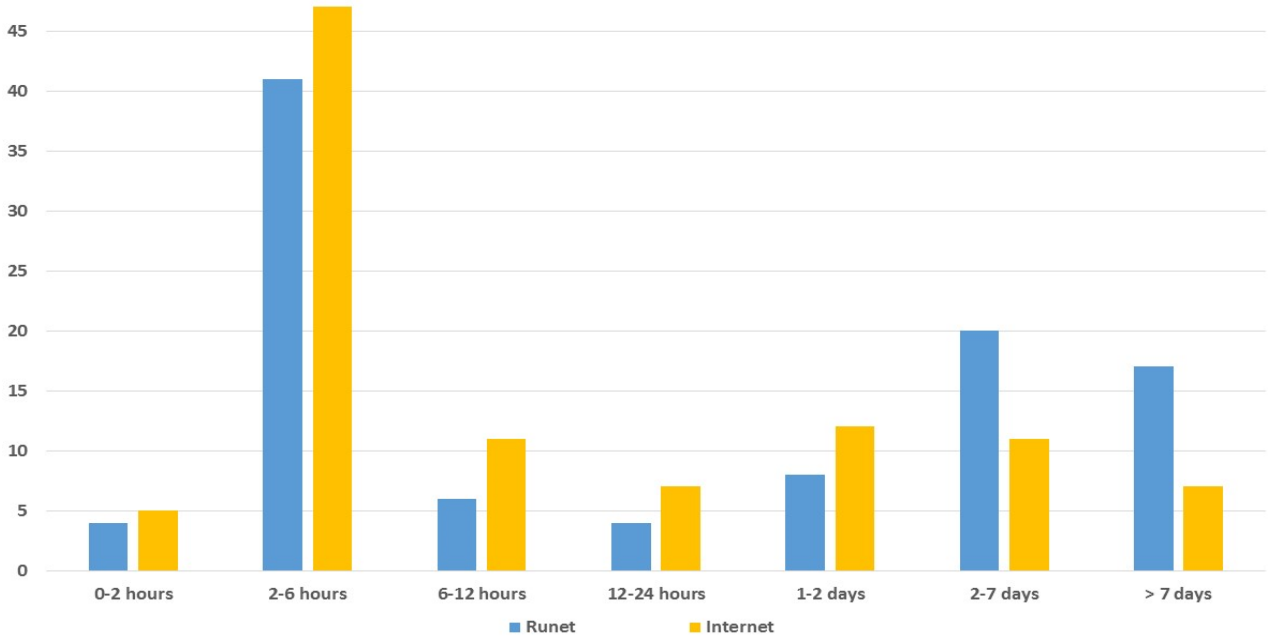
Hacking of content management systems

Intruders often use hacked sites for placing phishing pages. The sites are usually hacked through vulnerabilities of various content management systems (CMS). According to the 2016 statistics, such CMS as Wordpress and Joomla are leaders by the number of the detected hacking cases. For the most part these are old system versions without current security updates.

21%

2%

Lifetime of phishing pages



According to the data of RU-CERT, the average lifetime of a phishing page in 2016 was 35 hours with the median of 6 hours, i.e. half of the phishing pages remain available for visits during 6 and more hours from the time of their emergence. In the Russian segment of the Internet the average lifetime of a phishing page is 59 hours, and the median is 10 hours 30 minutes.

The lifetime also depends on specific features of placing phishing pages. Phishing placed on hacked sites usually closes 7 hours earlier as compared to that placed using maliciously registered domains.