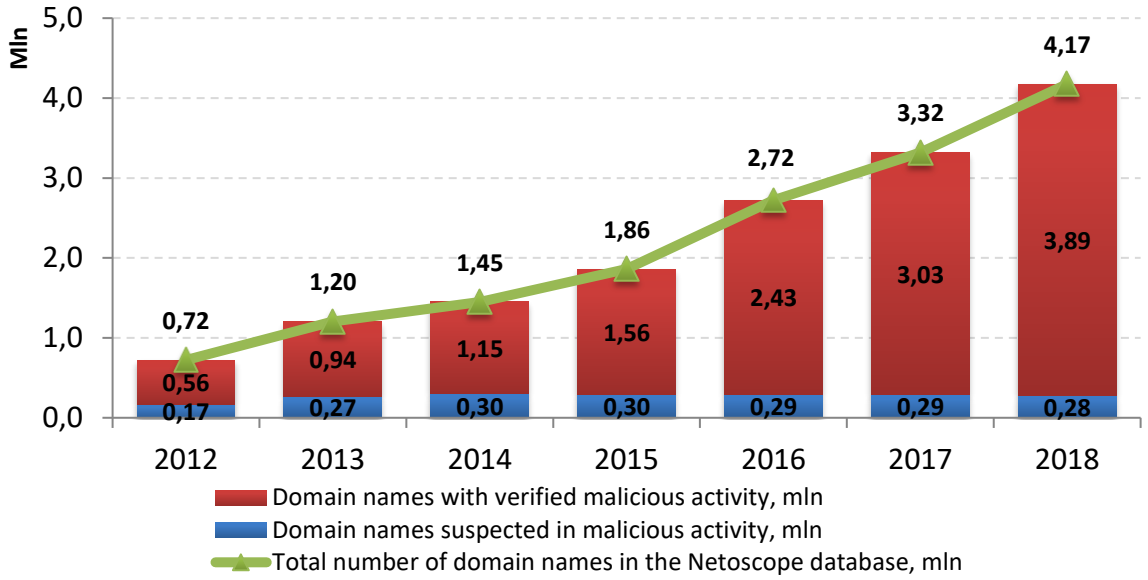
NETOSCOPE: STATISTICS

As of 31.12.2018

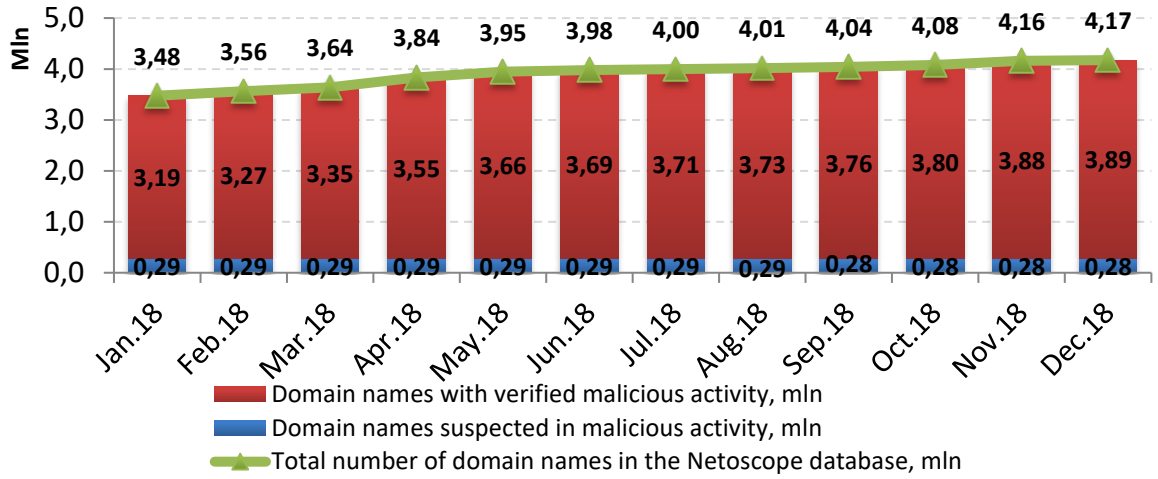
As of the end of December 2018, the database included 4,174,376 domain names (second-level, third-level and lower ones) that were suspected of malicious activities, or were engaged in such, at least once since November 2012 to December 2018.

Growth of the Netoscope database (by years)*



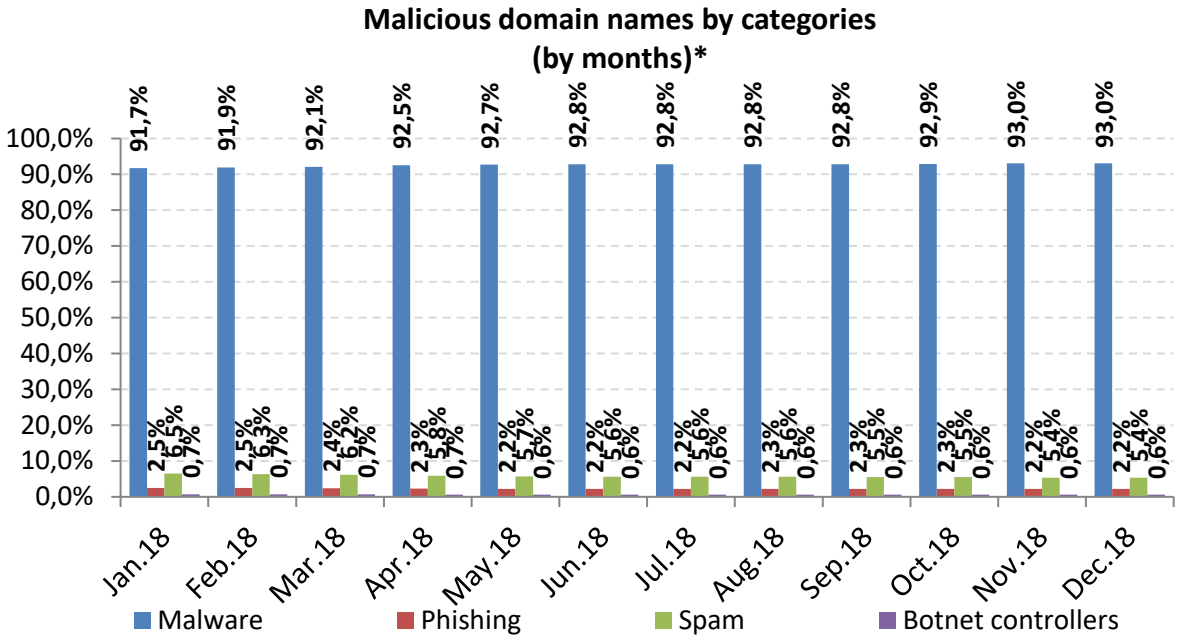
** Second-level, third-level and lower .RU, .РФ and .SU domain names are taken into account.*

Growth of the Netoscope database in 2018 (by months)*



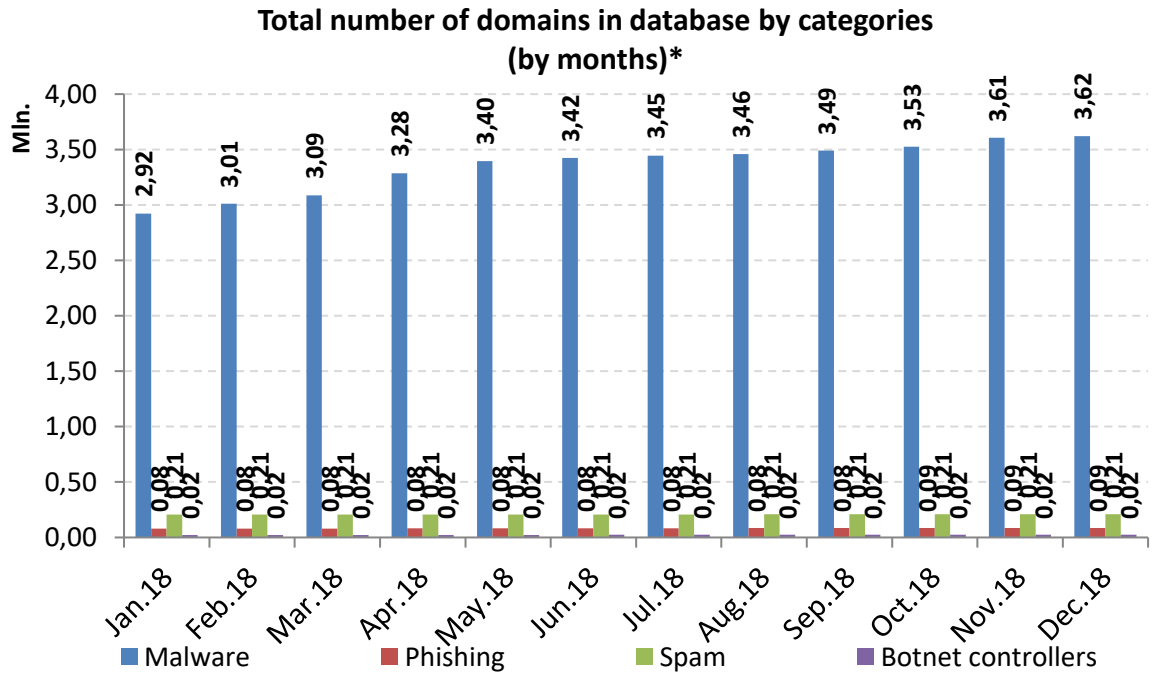
** Second-level, third-level and lower .RU, .РФ and .SU domain names are taken into account.*

The analysis of the base in December 2018 shows that hackers prefer posting malicious codes on websites (93.0% of all malicious domain names as of the end of December 2018).



** Second-level, third-level and lower .RU, .РФ and .SU malicious domain names are taken into account. One domain name can be associated with different types of malicious activity at once.*

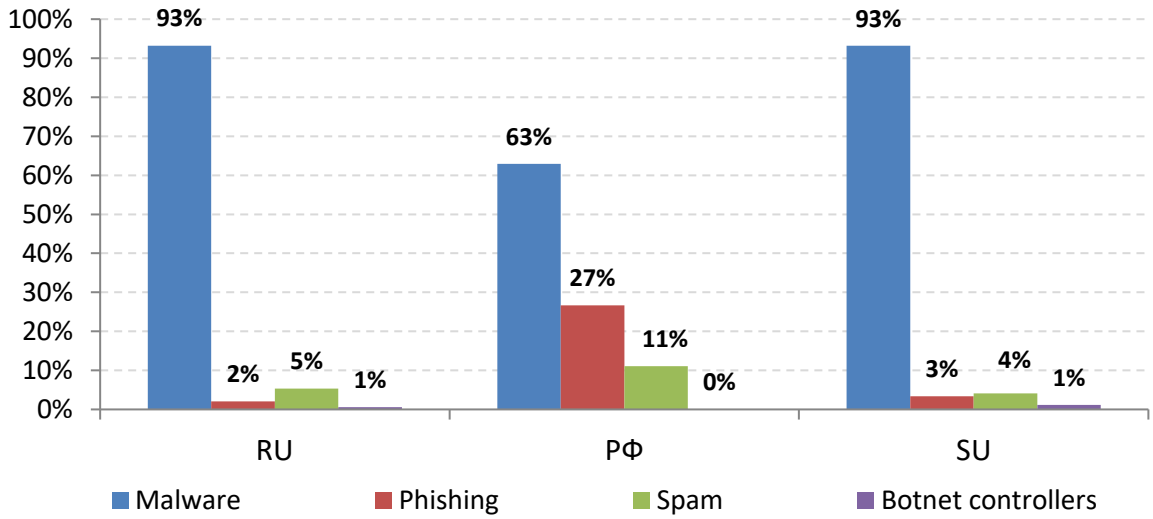
The graph below present detailed data on various types of malicious domain names (malware, phishing, spam, botnet controllers).



** Second-level, third-level and lower .RU, .РФ and .SU malicious domain names are taken into account.*

The statistics of different types of malicious domain names among .RU, .SU and .РФ reveals malware-spreading domains are prevalent in .RU and .SU (93%). As for .РФ, phishing attacks are 27% and malware-spreading domains are in the upward trend.

Malicious domain names in Runet by categories (December 2018)*



** Second-level, third-level and lower .RU, .РФ and .SU malicious domain names are taken into account. One domain name can be associated with different types of malicious activity at once.*

http://netoscope.ru