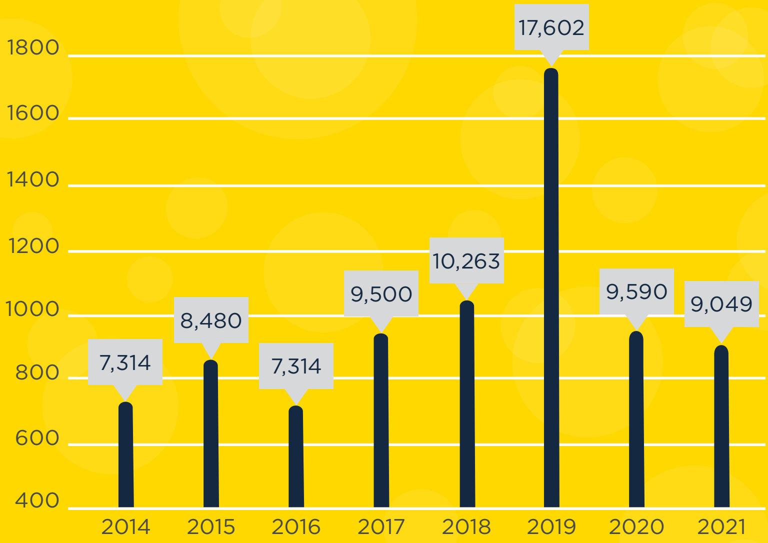
SPAMHAUS

2021 Annual Botnet Overview

In 2021, Spamhaus identified a total number of 9,049 botnet Command & Control servers (C&Cs) across 809 networks. More than a fourth (28%) of all Spamhaus Blocklist (SBL) listings issued by the Spamhaus Project were due to botnet C&Cs.

Annual numbers of botnet C&Cs

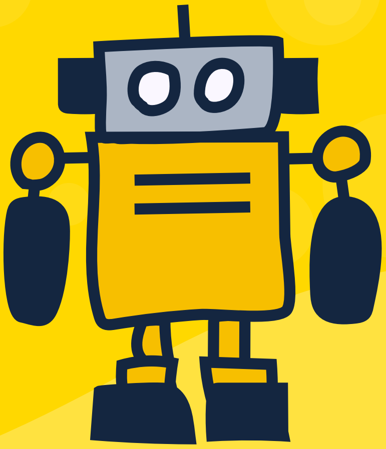
We observed that Russia, the United States, and the Netherlands accounted for a total of 42% of newly observed botnet C&Cs in 2021.

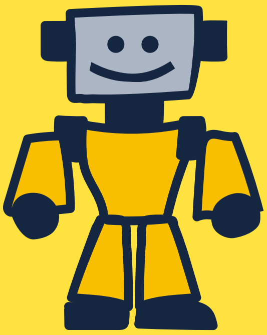


Identified

9,049

Botnet C&Cs





Spamhaus Blocklist Listings

28%

Related to Botnet C&Cs

Networks

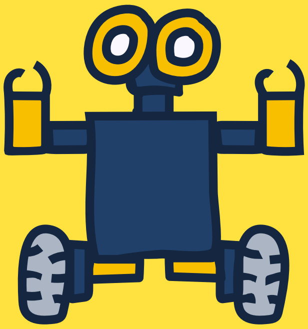
- uninet.net.mx (Mexico)
- severion.com (Netherlands) privacyfirst.sh (Germany)
- stc.com.sa (Saudi Arabia)
- alibaba-in.com (China)

= Over **15%** Botnet C&C traffic

Fraudulent sign-ups

90%

Botnet C&Cs hosted on dedicated infrastructure



Geolocation

- Russia
- United States
- Netherlands

= **42%** Botnet C&C traffic

How were miscreants hosting?

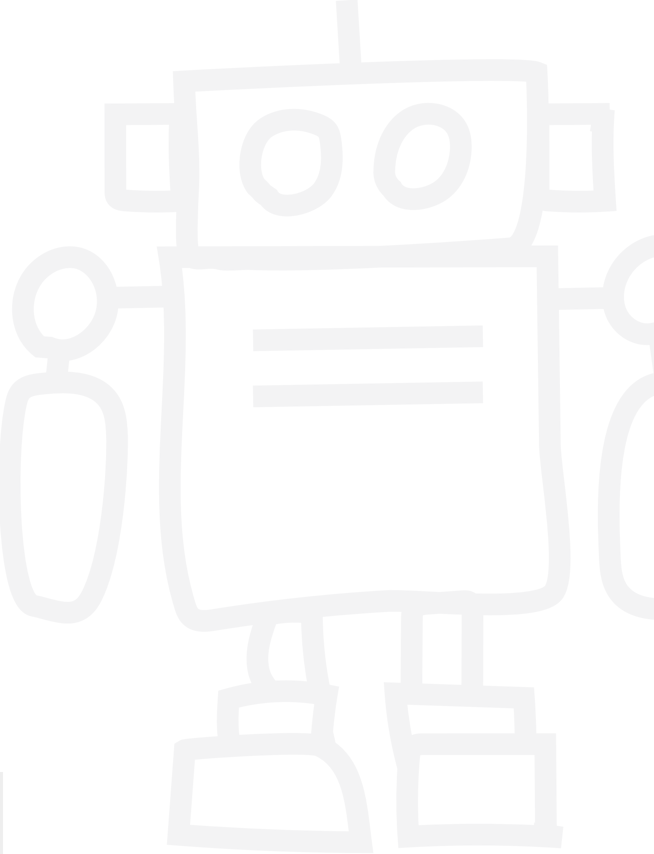
Almost 90% of our botnet C&C listings identified that hosts had been set up fraudulently by cybercriminals for the exclusive purpose of hosting a botnet C&C. This illustrates that using compromised hosts and websites for botnet C&Cs is no longer favored by miscreants.

Who was hosting?

Spamhaus detected a significant number of botnet C&C servers on uninet.net.mx (Mexico), severion.com (Netherlands), privacyfirst.sh (Germany), stc.com.sa (Saudi Arabia), and alibaba-in.com (China). Combined, these five networks alone were responsible for over 15% of all newly detected botnet C&Cs in 2021.

Where are they hosting?

We observed that Russia, the United States, and the Netherlands accounted for a total of 42% of newly observed botnet C&Cs in 2021.



What are botnet command & controllers?

A ‘botnet controller,’ ‘botnet C2’ or ‘botnet command & control’ server is commonly abbreviated to ‘botnet C&C.’ Fraudsters use these to both control malware infected machines and to extract personal and valuable data from malware-infected victims. Botnet C&Cs play a vital role in operations conducted by cybercriminals who are using infected machines to send out spam or ransomware, launch DDoS attacks, commit e-banking fraud or click-fraud or to mine cryptocurrencies such as Bitcoin. Desktop computers and mobile devices, like smartphones, aren’t the only machines that can become infected. There is an increasing number of devices connected to the internet, for example, the Internet of Things (IoT) devices like webcams, network-attached storage (NAS) and many more items. These are also at risk of becoming infected.