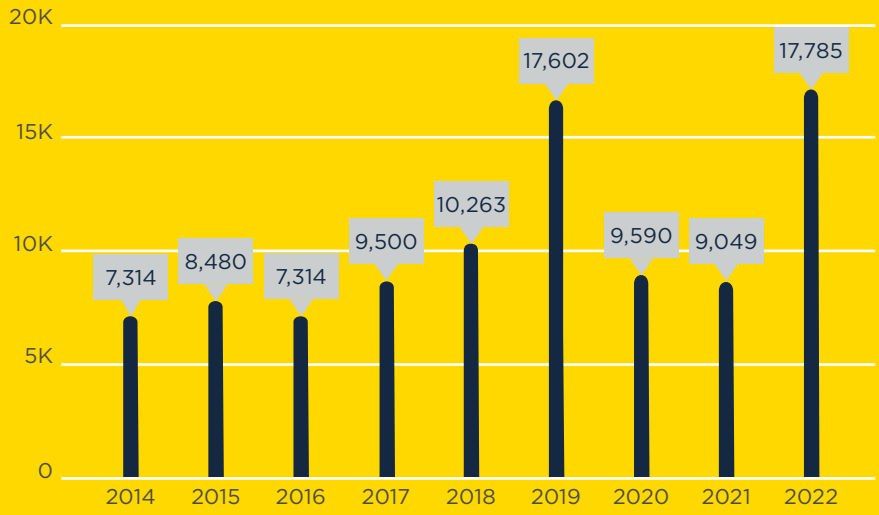
SPAMHAUS

2022 Annual Botnet Overview

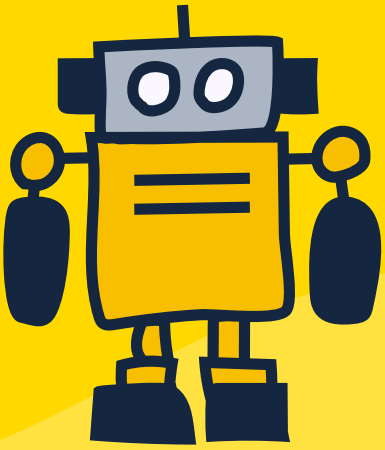
In 2022, Spamhaus identified a total number of 17,785 botnet command & controllers (C&Cs) across 770 networks associated with 97 different malware families.

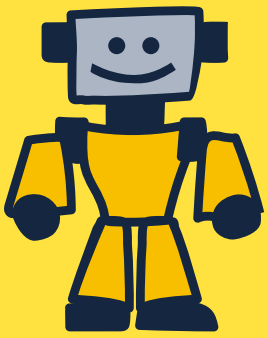
Botnet numbers by year

In 2022, the research team identified the largest number of botnet C&Cs since our records began. Figures almost doubled compared to 2021.



Identified
17,785
Botnet C&Cs





Botnet C&Cs
97%
increase year on year

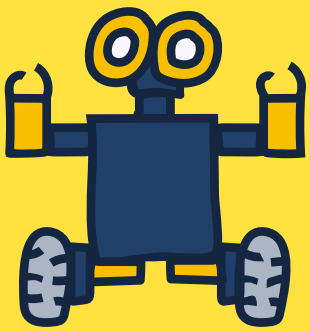
Networks

- tencent.com (China)
- alibaba-inc.com (China)
- uninet.net.mx (Mexico)
- stc.com.sa (Saudi Arabia)
- amazon.com (United States)

=

Over
21%
Botnet C&C traffic

Malware families
36%
Botnet C&Cs associated with Cobaltstrike



Geolocation

- United States
- Russia
- China

=

47%
Botnet C&C traffic

Who was hosting?

Spamhaus detected a significant number of botnet C&C servers on the following networks:

- tencent.com (China) - 1,022 botnet C&Cs
- alibaba-inc.com (China) - 618 botnet C&Cs
- uninet.net.mx (Mexico) - 538 botnet C&Cs
- stc.com.sa (Saudi Arabia) - 523 botnet C&Cs
- amazon.com (United States) - 449 botnet C&Cs

Combined, these five networks were responsible for over 21% of all newly detected botnet C&Cs in 2022.

Where were they hosting

We observed that the United States, Russia, and China accounted for nearly half (47%) of all newly observed botnet C&Cs in 2022.

What malware families were associated?

Our researchers identified 97 different malware families associated with the botnet C&Cs. Of those, the top three were Cobaltstrike (36%), Qakbot (10%), and RedLineStealer (9%).

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.