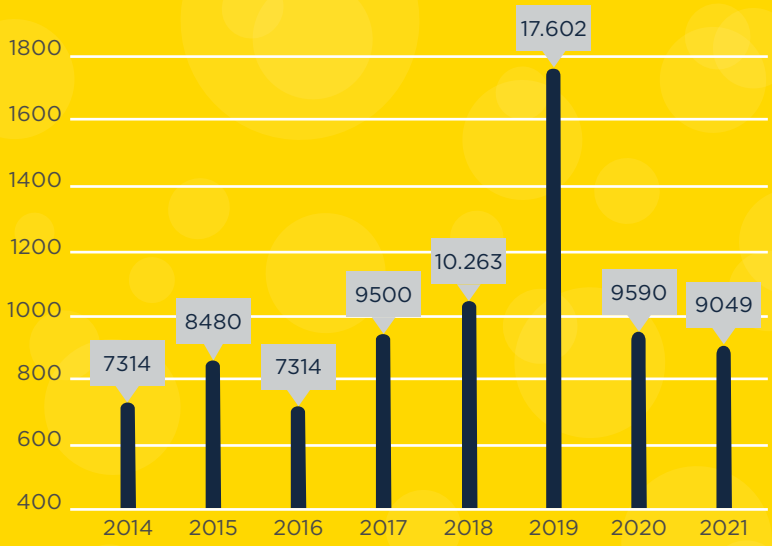
SPAMHAUS

Botnet-Jahresübersicht 2021

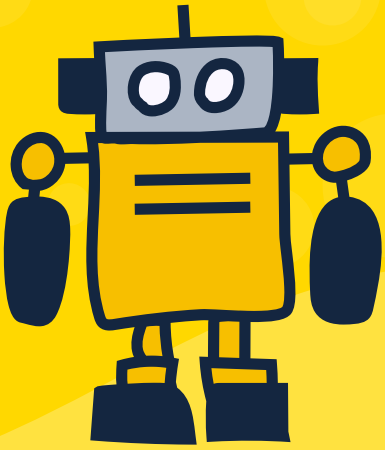
2021 identifizierte Spamhaus insgesamt 9.049 Botnet Command & Control Server (C&Cs) in 809 Netzwerken. Mehr als ein Viertel (28 %) aller von The Spamhaus Project herausgegebenen Blocklist-Einträge (SBL) betrafen Botnet C&Cs.

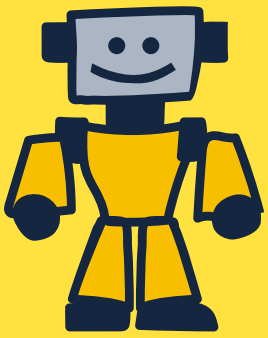
Die Jahreszahlen der Botnet C&Cs

Wir beobachteten, dass Russland, die USA und die Niederlande 2021 für insgesamt 42 % der neu beobachteten Botnet C&Cs verantwortlich waren.



Identifizierte
9.049
Botnet C&Cs





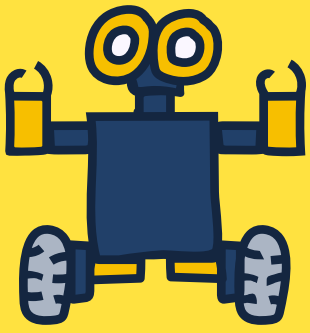
Spamhaus-Blocklist-Einträge
28%
Im Zusammenhang mit Botnet C&Cs

Netzwerke

- uninet.net.mx (Mexiko)
- severion.com (Niederlande)
- privacyfirst.sh (Deutschland)
- stc.com.sa (Saudi-Arabien)
- alibaba-in.com (China)

= Über **15 %** Botnet-C&C-Verkehr

Betrügerische Registrierungen
90%
Auf spezieller Infrastruktur gehostete Botnet C&Cs



Standort

- Russland
- USA
- Niederlande

= **42 %** Botnet-C&C-Verkehr

Wie wurden Bösewichte gehostet?

Fast 90 % unserer Botnet-C&C-Einträge waren darauf zurückzuführen, dass Cyberkriminelle Hosts ausschließlich zu dem Zweck eingerichtet hatten, einen Botnet C&C zu hosten. Dies veranschaulicht, dass Betrüger offensichtlich nicht länger darauf setzen, beeinträchtigte Hosts und Websites für ihre Botnet C&Cs zu nutzen.

Wer waren die Hosts?

Spamhaus erkannte eine erhebliche Anzahl von Botnet-C&C-Servern auf uninet.net.mx (Mexiko), severion.com (Niederlande), privacyfirst.sh (Deutschland), stc.com.sa (Saudi-Arabien) und alibaba-in.com (China). Zusammengenommen waren allein diese fünf Netzwerke 2021 für über 15 % aller neu erkannten Botnet C&Cs verantwortlich.

Wo sitzen die Hosts?

Wir fanden heraus, dass Russland, die USA und die Niederlande 2021 für insgesamt 42 % der neu beobachteten Botnet C&Cs verantwortlich waren.

Was sind Botnet Command-and-Controllers?

Ein „Botnet Controller“, „Botnet C2“ oder „Botnet Command & Control“-Server wird üblicherweise kurz als „Botnet C&C“ bezeichnet. Betrüger nutzen solche Botnet C&Cs, um mit Malware infizierte Rechner zu kontrollieren sowie personenbezogene und andere wertvolle Daten abzugreifen. Botnet C&Cs spielen eine wichtige Rolle bei Aktivitäten von Cyberkriminellen, die infizierte Rechner dazu missbrauchen, Spam oder Ransomware zu versenden, DDoS-Angriffe zu starten, E-Banking- oder Klickbetrug zu begehen oder Kryptowährungen wie Bitcoin abzuschöpfen. Desktop-Computer und Mobilgeräte wie Smartphones sind nicht die einzigen Geräte, die infiziert werden können. Immer mehr Geräte sind mit dem Internet verbunden, beispielsweise Geräte im Internet der Dinge (IoT) wie Webcams, Network Attached Storage (NAS) und vieles mehr. Auch diese Geräte laufen Gefahr, infiziert zu werden.