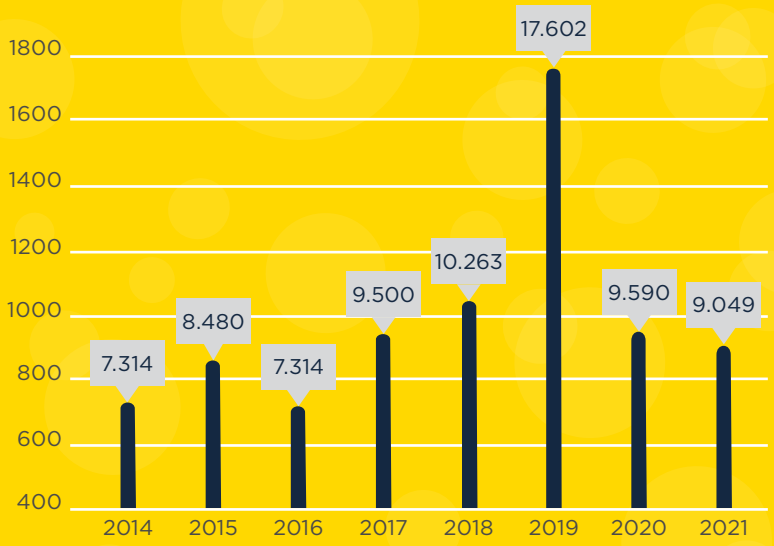
SPAMHAUS

Síntese anual sobre botnet 2021

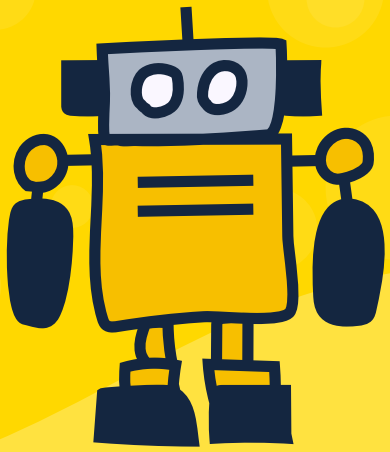
Em 2021, a Spamhaus identificou um total de 9.049 servidores de comando e controle (CCs) de botnet em 809 redes. Mais de um quarto (28%) de todas as inclusões na Spamhaus Blocklist (SBL) geradas pelo The Spamhaus Project foram devidas a botnet CCs.

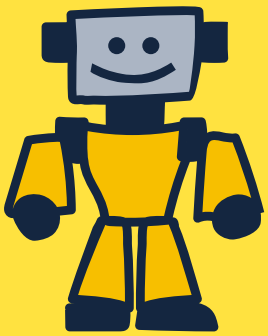
Números anuais de botnet CCs

Observamos que a Rússia, os Estados Unidos e os Países Baixos totalizaram 42% dos botnet CCs recém-observados em 2021.



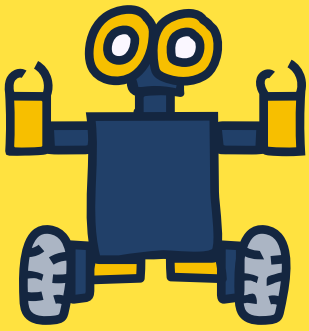
Indentificamos
9.049
Botnet CCs





Inclusões na Spamhaus Blocklist
28%
relacionadas a botnet CCs

Cadastros fraudulentos
90%
de botnet CCs hospedados em infraestruturas dedicadas



Redes

- uninet.net.mx (México)
- severion.com (Países Baixos
- privacyfirst.sh (Alemanha)
- stc.com.sa (Arábia Saudita)
- alibaba-in.com (China)

= Mais de **15%** de tráfego de botnet CC

Geolocalização

- Rússia
- Estados Unidos
- Países Baixos

= **42%** de tráfego de botnet CC

Como os impostores se hospedam?

Quase 90% de nossas listas de botnet CCs identificaram que os cibercriminosos configuraram hosts de forma fraudulenta com a finalidade exclusiva de hospedar um botnet CC. Isso demonstra que usar websites e hosts comprometidos para botnet CCs não é mais a opção preferida dos impostores.

Quem os hospedou?

A Spamhaus detectou um número significativo de servidores de botnet CC na uninet.net.mx (México), severion.com (Países Baixos), privacyfirst.sh (Alemanha), stc.com.sa (Arábia Saudita) e alibaba-in.com (China). Combinadas, essas cinco redes foram responsáveis por mais de 15% de todos os botnet CCs recém-detectados em 2021.

Onde se hospedam?

Observamos que a Rússia, os Estados Unidos e os Países Baixos totalizaram 42% dos botnet CCs recém-observados em 2021.

O que são controladores de botnet?

"Servidor de comando e controle de botnet", "controlador de botnet" ou "botnet C2" são maneiras comuns de nos referirmos ao "botnet CC". Os fraudadores usam essa rede para controlar computadores infectados por malware e extrair valiosos dados pessoais das vítimas infectadas pelo malware. Os botnet CCs desempenham um papel vital nas operações realizadas por cibercriminosos que usam computadores infectados para enviar spam ou ransomware, lançar ataques DDoS, aplicar golpes relacionados a bancos eletrônicos ou click fraud, ou minerar criptomoedas, como bitcoins. Computadores de mesa e dispositivos móveis, como smartphones, não são os únicos equipamentos que podem ser infectados. O número de dispositivos conectados à internet aumenta a cada dia, por exemplo, os dispositivos de Internet das Coisas (IoT), como webcams, unidades de armazenamento de dados em rede (NAS) e muitos outros. Eles também correm o risco de serem infectados.