Čo je to botnet

Last updated March 18, 2025

Botnet je sieť počítačov, ktoré boli infikované škodlivým softvérom (malvérom) a sú ovládané vzdialene, zvyčajne bez vedomia ich majiteľov.

Tieto infikované počítače („boti") môžu byť použité na uskutočňovanie rôznych nelegálnych činností, ako napr.:

- rozosielanie spamu
- krádež dát
- DDoS útoky
- šírenie malvéru

Botnet môže zahŕňať tisíce alebo dokonca milióny infikovaných počítačov.

Riadenie botnetu sa zvyčajne uskutočňuje prostredníctvom komunikačných kanálov, ako sú IRC kanály alebo skryté webové servery.

Ako sa z vášho počítača stane infikovaný bot?

Počítače sa zvyčajne stanú súčasťou botnetu prostredníctvom malvéru šíreného phishingovými e-mailami v infikovaných prílohách alebo softvéri, nezabezpečených sieťach a pod.

Niektoré botnety využívajú zraniteľné miesta v operačných systémoch alebo aplikáciách.

Ako zistiť, že sa z vášho počítača stal bot?

Aktivitu spojenú s botnetmi najlepšie detekuje antivírusový program.

Medzi symptómy toho, že váš počítač je súčasťou botnetu, patrí:

- výrazné spomalenie výkonu počítača
- neočakávané reštarty alebo zamŕzanie
- nezvyčajne vysoké využitie internetového pripojenia
- neznáme e-maily odoslané z vášho účtu
- nezvyčajná aktivita v sieťových protokoloch

Ako sa brániť?

Ak je váš počítač už infikovaný, použite spoľahlivý antivírusový softvér na odstránenie malvéru.

V niektorých prípadoch môže byť nevyhnutný kompletný reset systému.

Na prevenciu botnetu platí:

- pravidelná aktualizáciu softvéru
- pravidelné malvér scany
- aktivovaný firewall
- opatrnosť při otváraní e-mailových príloh a klikaní na neznáme odkazy