Co je botnet

Poslední aktualizace 11 října, 2024

Botnet je síť počítačů, které byly infikovány škodlivým softwarem a jsou ovládány vzdáleně, obvykle bez vědomí jejich majitelů.

Tyto infikované počítače („boti“) mohou být použity k provádění různých nelegálních činností, jako např:

- rozesílání spamu
- krádež dat
- DDoS útoky
- šíření malware

Botnet může zahrnovat tisíce nebo dokonce miliony infikovaných počítačů.

Řízení botnetu se obvykle provádí prostřednictvím komunikačních kanálů, jako jsou IRC kanály nebo skryté webové servery.

Jak se z vašeho počítače stane infikovaný bot?

Počítače se obvykle stanou součástí botnetu prostřednictvím malware šířeného phishingovými e-maily v infikovaných přílohách nebo softwaru, nezabezpečených sítích apod.

Některé botnety využívají zranitelných míst v operačních systémech nebo aplikacích.

Jak poznat, že se z vašeho počítače stal bot?

Aktivitu spojenou s botnety nejlépe detekuje antivirový program.

Mezi symptomy toho, že váš počítač je součástí botnetu, patří:

- výrazné zpomalení výkonu počítače
- neočekávané restarty nebo zamrzání
- neobvykle vysoké využití internetového připojení
- neznámé e-maily odeslané z vašeho účtu
- neobvyklá aktivita v síťových protokolech

Jak se bránit?

Pokud je váš počítač již infikován, použijte spolehlivý antivirový software pro odstranění malwaru.

V některých případech může být nutný kompletní reset systému.

Pro prevenci botnetu platí:

- pravidelná aktualizace softwaru
- pravidelné malware scany
- aktivovaný firewall
- opatrnost při otevírání e-mailových příloh a klikání na neznámé odkazy