Botnet

Botnet je skupina internetem propojených zařízení, z nichž každé běží jeden nebo více botů (škodlivých programů). Útočník, označovaný jako **Botmaster** nebo **Herder**, může tuto síť vzdáleně ovládat a využívat její společný výpočetní výkon a šířku pásma k masivním útokům.

Jednotlivá napadená zařízení v botnetu se nazývají **zombie**.

Architektura Botnetu

Způsob, jakým útočník dává příkazy své armádě „zombie“, se v čase vyvíjel:

1. Model Client-Server (Centralizovaný)

Všechny infikované stroje se připojují k jednomu centrálnímu serveru (C&C – Command and Control).

- **Nevýhoda:** Pokud bezpečnostní složky tento server odstaví, celý botnet přestane fungovat.
- **Protokoly:** Často se využívalo IRC (Internet Relay Chat) nebo HTTP.

2. Model Peer-to-Peer (Decentralizovaný)

Modernější botnety fungují jako P2P sítě. Instrukce se šíří z jednoho napadeného zařízení na druhé.

- **Výhoda pro útočníka:** Neexistuje žádný centrální bod, který by šlo vypnout. Botnet je extrémně odolný.

Životní cyklus Botnetu

```
1. **Infekce (Recruitment):** Útočník infikuje zařízení pomocí [[phishing|phishingu]], zranitelností v softwaru nebo hrubou silou (brute-force) na slabá hesla.
2. **Aktivace:** Malware se spojí s ovládacím centrem a čeká na instrukce.
3. **Expanze:** Botnet může být naprogramován tak, aby sám aktivně vyhledával a infikoval další zařízení v síti.
4. **Útok:** Botmaster vydá povel k provedení konkrétní škodlivé aktivity.
```

K čemu se Botnety využívají?

Botnety jsou v podstatě „superpočítače k pronájmu“ na černém trhu.

- **DDoS útoky:** Zaplavení cílového serveru takovým množstvím požadavků, že zkolabuje.
- **Rozesílání spamu:** Jeden botnet dokáže odeslat miliardy nevyžádaných e-mailů denně.
- **Těžba kryptoměn (Cryptojacking):** Využití výkonu tisíců cizích PC k těžbě (např. Monero).
- **Prolamování hesel:** Rozdělení výpočetně náročného hádání hesel mezi tisíce strojů.
- **Krádeže identity:** Sbírání hesel a bankovních údajů přímo z infikovaných zařízení.

Proč jsou ohrožena IoT zařízení?

V posledních letech (např. botnet **Mirai**) se útočníci zaměřují na chytré kamery, routery a domácí spotřebiče. Tyto přístroje mají často:

- Slabé nebo výchozí přihlašovací údaje (admin/admin).
- Zastaralý firmware bez bezpečnostních záplat.
- Nepřetržité připojení k internetu a slabý nebo žádný antivirus.

Jak poznat, že je vaše zařízení "Zombie"?

- **Náhlý pokles výkonu:** Počítač je pomalý bez zjevného důvodu.
- **Vysoký síťový provoz:** Odesílání velkého množství dat, i když nic neděláte.
- **Neznámé procesy:** Správce úloh ukazuje běžící programy, které jste neinstalovali.
- **Pády systému:** Časté chyby a restarty.

Prevence

- Používejte silná a unikátní hesla pro všechna zařízení (včetně routerů a kamer).
- Pravidelně aktualizujte firmware a software.
- Používejte kvalitní antivirus a firewall.
- Pokud zařízení nepotřebuje být viditelné z internetu, nepovolujte u něj funkci UPnP.

Související pojmy: Malware, DDoS, C&C Server, Zombie, IoT, Phishing, P2P.