Malware (Škodlivý software)

Malware je nadřazený termín pro celou rodinu digitálních hrozeb. Liší se způsobem šíření, cílem útoku i mírou nebezpečnosti – od otravných reklam až po sofistikované nástroje kybernetické špionáže.

1. Základní typy malwaru

Virus

Klasický typ malwaru, který se **připojuje k legitimním souborům** (např. .exe programům). K šíření vyžaduje aktivitu uživatele (spuštění infikovaného souboru). Podobně jako biologický virus se snaží replikovat a infikovat další soubory v systému.

Červ (Worm)

Na rozdíl od viru se červ **šíří samostatně** přes počítačové sítě. Využívá zranitelnosti v operačním systému a nevyžaduje pomoc uživatele. Dokáže velmi rychle zahltit síť nebo infikovat tisíce počítačů po celém světě.

Trojský kůň (Trojan)

Maskuje se jako užitečný nebo legitimní software (např. hra nebo nástroj zdarma). Jakmile jej uživatel nainstaluje, „Trojan“ aktivuje svou skrytou funkci – například otevře útočníkovi „zadní vrátka“ (Backdoor).

Ransomware

Jeden z nejnebezpečnějších typů současnosti. **Zašifruje data** na disku a za jejich odemčení vyžaduje výkupné (obvykle v kryptoměnách). Bez zálohy nebo zaplacení jsou data často nenávratně ztracena.

Spyware & Adware

- **Spyware:** Tajně sleduje aktivitu uživatele (stisky kláves, historii prohlížení) a odesílá ji útočníkovi.
- **Adware:** Agresivně zobrazuje nevyžádanou reklamu a často zpomaluje systém.

2. Způsoby infekce

Malware využívá různé vektory útoku, aby se dostal do systému:

- **Phishing:** Podvodné e-maily s infikovanou přílohou nebo odkazem.
- **Drive-by download:** Infekce pouhou návštěvou kompromitované webové stránky.
- **Nezáplatovaný software:** Využití bezpečnostních děr v zastaralém systému.
- **Fyzická média:** Např. infikované USB disky ponechané na veřejných místech.

3. Jak poznat napadený počítač?

- Náhlé a výrazné **zpomalení systému**.
- Časté pády aplikací nebo „Modrá obrazovka smrti“ (BSOD).
- Samovolné otevírání oken prohlížeče nebo vyskakování reklam.
- Zmizení souborů nebo změna jejich přípon (příznak ransomware).
- Vysoká síťová aktivita, i když počítač nepoužíváte.

4. Obrana a prevence

Obrana by měla být vrstvená (tzv. „Defense in Depth“):

```
1. **Antivirus / EDR:** Software, který skenuje soubory a procesy v reálném čase.
2. **Firewall:** Blokuje podezřelou komunikaci se servery útočníka.
3. **Aktualizace:** Pravidelné záplatování systému a aplikací.
4. **Zálohování:** Jediná 100% účinná ochrana proti ztrátě dat při napadení ransomwarem.
```

> **Zajímavost:** První experimentální virus, nazvaný **Creeper**, vznikl už v roce 1971. Nebyl škodlivý – pouze na obrazovkách tehdejší sítě ARPANET zobrazoval zprávu: „I'm the creeper, catch me if you can!“ (Jsem strašidlo, chyť mě, když to dokážeš!).

Zpět na Bezpečnost