Malware

2.1. Definire şi funcţii

2.1.1. Înţelegerea termenului de malware

- Prescurtarea de la „malicious software„ (software rău intenţionat), malware-ul se referă la programele software proiectate pentru a se instala pe un computer, fără consimţământul proprietarului, în scopul de a distruge sau executa alte acţiuni nedorite pe un sistem informatic.
- Exemple comune de malware includ:
  - Viruşi - pot provoca haos pe hard-diskul calculatorului prin ştergerea fişierelor sau informaţiilor din directoare
  - viermi
  - troieni
  - programe spion (spyware) pot colecta date de la sistemul unui utilizator, fără ca utilizatorul să ştie. Acest lucru poate include orice, de la paginile web pe care un utilizator le vizitează până la Informaţii personale, cum ar fi detaliile cardului de credit
- Este regretabil faptul că există programatori de software care proiectează programe rău-intenţionate, dar este bine să fim conştienţi de acest lucru.
- Pentru combaterea malware-ului, puteţi instala aplicaţii antivirus şi anti-spyware pe computer, care vor căuta şi distruge programe malware găsite pe Computer.

2.1.2. Recunoaşterea diferitelor moduri sub care malware se poate ascunde - trojan, rootkits şi back doors

- În domeniul computerelor, un **cal troian** (trojan) este un program în care codul maliţios sau dăunător se află în interiorul unei aplicaţii aparent inofensive sau în anumite date, astfel încât să poată prelua controlul computerului şi să execute forma aleasă de prejudiciu, cum ar fi ruinarea tabelului de alocare a fişierelor (FAT) de pe hard-disk.

- Un cal troian poate fi redistribuit pe scară largă ca parte a unui virus de calculator.
- Termenul provine din mitologia greacă referitoare la războiul troian. Conform legendei, grecii au prezentat cetăţenilor din Troia un cal mare de lemn în care şi-au ascuns războinicii. În timpul nopţii, războinicii au ieşit din calul de lemn şi au invadat orașul.

Rootkit

- Un **rootkit** este un tip de malware, care este activat de fiecare dată când sistemul de operare (de exemplu, Microsoft Windows) porneşte. Rootkit-urile sunt dificil de detectat, deoarece acestea sunt activate înainte ca sistemul dumneavoastră de operare să fie complet pornit.
- Rootkit-ul permite de multe ori instalarea ascunsă de fişiere, procese, conturi de utilizator în sistemul de operare. Acestea sunt capabile să intercepteze date atât de la terminale, conexiuni la reţea, cât şi de la tastatură.

Backdoor

- Un **backdoor,** numit şi „trapă", este un mod nedocumentat de a avea acces la un program, serviciu online sau un întreg sistem de calcul. Backdoor-ul este scris de programatorul care creează codul sursă pentru program, acesta devenind un risc de securitate.
- Un backdoor într-un sistem informatic sau algoritm este o metodă de ocolire a autentificarii normale, ce asigură accesul ilegal de la distanţă la un calculator şi resursele acestuia. Poate lua forma unui program instalat sau poate submina sistemul printr-un rootkit.