Malware

2.2. Tipuri de malware

2.2.1 Recunoaşterea tipurilor de malware şi cunoaşterea modului în care acţionează

- Un **virus** de calculator este un program care se poate reproduce şi răspândi de la un calculator la altul. Termenul „virus" este frecvent folosit în mod eronat, pentru a desemna alte tipuri de malware, inclusiv programe adware şi programe spyware care nu au capacitatea de reproducere.
- Virusul de calculator se ataşează la un program sau fişier şi acţionează când acestea sunt rulate (deschise). Ca un virus uman, un virus de calculator poate varia în severitate: unele pot provoca efecte doar uşor enervante, în timp ce altele pot deteriora hardware-ul, software-ul sau fişierele.
- Aproape toţi viruşii sunt ataşaţi la un fişier executabil, ceea ce înseamnă că virusul poate exista pe computerul dumneavoastră, dar nu poate infecta computerul dacă nu deschideţi programul dăunător.

Worm

- Un worm (vierme) este un mic program software care utilizează reţele de calculatoare şi găuri de securitate pentru a se multiplica. O copie a viermelui scanează reţeaua pentru a găşi un alt calculator cu o deficienţă de securitate specifică, după care se multiplică.
- Obiectivul principal al viermilor constă în blocarea calculatoarelor şi reţelelor.

Worm, trojan

- Viruşii, viermii şi caii troieni sunt toate programe malware, care pot provoca daiune la computer, dar există diferenţe între cele trei.
- O greşeală comună pe care oamenii o fac în privinţa programelor maliţioaise este de a se referi la un **vierme** sau **cal troian** ca la un virus, în timp ce cuvintele **vierme** şi **virus** sunt adesea folosite alternativ, ele nu sunt exact acelaşi lucru.
- Un vierme este similar cu un virus ca proiectare şi este considerat a fi o subclasă de virus. Viermii se răspândesc de la un calculator la altul, dar spre deosebire de viruși, aceştia au capacitatea de a se transmite fără nicio intervenţie din partea utilizatorului.
- Troienii, pe de altă parte, nu se reproduc prin infectarea altor fişiere şi nici nu se auto-multiplică.

2.2.2. Recunoaşterea viruşilor legaţi de furtul datelor, generarea de profit/extorsiune de fonduri şi înţelegerea modului lor de funcţionare adware, spyware, botnets, keystroke logging, diallers

- **Programele de tip adware** (advertising-supported software) reprezintă o formă de malware care se manifestă prin deschiderea automată a unor ferestre pop-up sau bannere ce afişează reclame nesolicitate la diferite produse şi servicii.
- Adware-ul poate fi ataşat unui program gratuit descărcat de pe Internet şi se poate activa sau fără ştiinţa utilizatorului prin acceptarea diferitelor facilităţi şi bare de instrumente, propuse în cadrul procesului de instalare a acelui program.

Adware

- Adware-ul poate avea ca efecte modificări ale paginii de pornire a browse-ului web și a motoarelor de căutare pentru a afişa mai mult conţinut publicitar.
- De asemenea, poate colecta, fără consimţământul utilizatorului, date despre paginile vizitate sau poate limita performanţele sistemului de calcul şi viteza de navigare pe internet.

Spyware

- Aplicaţiile spyware (spion) reprezintă software ce colectează informaţii despre o persoană sau organizaţie fără ştiinţa şi consimţământul acestora. Acest tip de program poate înregistra fiecare tastă apăsată, activitatea browser-ului, preferinţele și interesele utilizatorilor, urmând ca ulterior aceste date să fie trimise autorului programului sau unor terţe părţi.
- Tipul de informaţii furate variază de la nume şi parole de utilizatori, adrese IP şi DNS până la date utilizate în operaţiuni de plată folosind servicii de online banking şi magazine virtuale.
- Programele spion pot fi instalate cu sau fără ştiinţa utilizatorilor şi printre principalele manifestări se evidenţiază încetinirea vitezei de navigare pe Internet sau redirecţionarea către anumite site-uri web.

Keylogger

- **Keystroke logging** reprezintă procesul de înregistrare a fiecărei taste apăsate, software-ul care înregistrează, colectează şi trimite aceste înregistrări unor terţe părţi se numeşte **keylogger.** Prin intermediul acestei aplicaţii se pot fura nume de utilizatori, parole şi informaţii sensibile folosite în tranzacţiile electronice.
- Acest tip de program este banal, uşor de construit, însă devine foarte periculos atunci când este ataşat unui troian sau spyware. În momentul actual există câteva metode de a ne proteja de acest tip de software, cum ar fi folosirea unei tastaturii virtuale pentru introducerea informaţiilor confidenţiale.

Botnets

- **Botnets** se referă la un grup de computere controlate de mici programe numite bots. Termenul bots vine de la **„robots"** (roboţi) şi desemnează aplicaţiile proiectate pentru a prelua controlul asupra unui computer fără ştiinţa şi consimţământul utilizatorului.
- Prin intermediul acestora, deţinătorul programelor botnets poate descărca pe calculatoarele compromise diferite tipuri de malware, dar mai ales poate iniţia atacuri cibernetice asupra altor computere.

Dialler

- Un **dialler** este un program maliţios care se poate folosi de un modem şi o linie telefonică pentru a redirecţiona conexiunile la Internet. Acest lucru se realizează prin apelarea unor numere de telefon cu supratаxă pentru a cauza prejudicii financiare.
- Primul indiciu asupra existenţei unui dialler în calculator este legat de sumele foarte mari de plată a facturilor la serviciile de telefonie utilizate pentru accesarea Internetului.