Škodlivý softvér

V rámci prednášky budú použité nasledujúce podklady:

Primárny zdroj informácii k dnešnej prednáške:
[1] prof. Ing. Dušan Levický, CSc.
APLIKOVANÁ KRYPTOGRAFIA
od utajenia správ ku kybernetickej bezpečnosti
Elfa, Košice, 2018 (str.237-240)

[2] Soriano, S.: Informačná a sieťová bezpečnosť. ČVUT Praha (str.24-31):
http://techpedia.fel.cvut.cz/sk/download/?fileId=176&objectId=45

Ďalšie zaujímavé linky:

https://support.eset.com/kb186/?locale=en_US&viewlocale=sk_SK

https://www.virusradar.com/en/threat_encyclopaedia/

https://www.codewithc.com/how-to-develop-computer-virus-using-c/

Škodlivý softvér

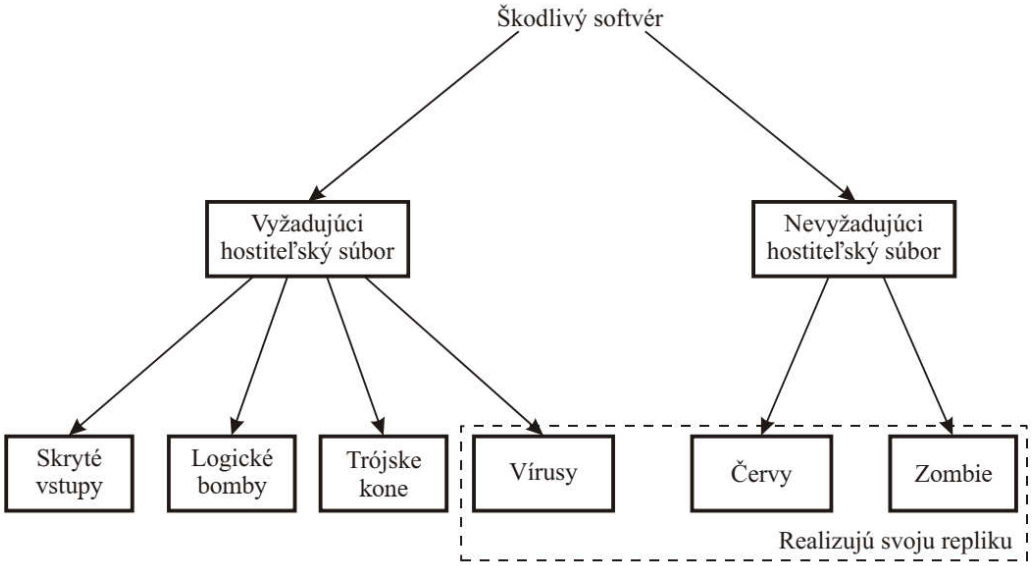
Škodlivý softvér (*malicious software*) je cieľavedome vytvorený počítačový program, ktorý predstavuje softvérové ohrozenie počítačového systému a môže spôsobiť straty, resp. škody v tomto systéme.

Uvedený druh softvérového ohrozenia možno rozdeliť do dvoch základných kategórií a to:

• škodlivý softvér vyžadujúci na šírenie hostiteľský súbor,
• škodlivý softvér nevyžadujúci na šírenie hostiteľský súbor, t. j. škodlivý softvér, ktorý je nezávislý

Možno tiež rozlíšiť škodlivý softvér, ktorý negeneruje svoju repliku a škodlivý softvér, ktorý svoju repliku generuje.

Základná kategorizácia škodlivého softvéru je uvedená na *Obr. 12.8.*



Obr. 12.8 Kategorizácia škodlivého softvéru

Skryté vstupy (Trap doors) sú utajené vstupy do programu, ktoré umožňujú získať prístup do systému obchádzaním mechanizmov bezpečnosti. Uvedené vstupy boli používané programátormi najmä pri ladení a testovaní programov. Počas ladenia a testovania programu z dôvodu urýchlenia týchto procesov, skryté vstupy umožňovali obchádzať najmä mechanizmy autentizácie a programátor získal špeciálne privilégia. Tieto skryté vstupy vyhľadáva škodlivý softvér a obchádza mechanizmy bezpečnosti, čím vzniká vážne softvérové ohrozenie počítačového systému.

Logické bomby (Logic bombs) predstavujú najstarší druh škodlivého softvéru, ktorý predstavuje softvérové ohrozenie. Je to program integrovaný do legitímneho programu, ktorý sa aktivizuje pri splnení určitých podmienok. Príkladom takýchto podmienok môže byť prítomnosť, resp. neprítomnosť určitého typu súboru v predvolený deň, týždeň alebo dátum alebo štart určitej aplikácie. Logická bomba môže spôsobiť straty, resp. škody v počítačovom systéme, napr. vymazať určité súbory, zastaviť prebiehajúci výpočet atď.

Trójske kone (Trojan horses) sú programy, resp. príkazy, ktoré vykonávajú určité užitočné funkcie, a ktoré okrem toho vykonávajú v pozadí nežiaduce a deštrukčné účinky, napr. vymazanie dát. Špeciálnym prípadom tohto typu škodlivého softvéru je špehovací softvér (spyware), ktorý zbiera heslá zadávané z klávesnice, zisťuje aké stránky sú navštevované, aký softvér je používaný a odosiela uvedené informácie po internete na zadané miesta.

Vírusy (viruses) sú programy, ktoré sú schopné pripojiť sa k inému programu, resp. súboru a vykonávať nežiaduce efekty. Na svoje šírenie vyžadujú iné súbory, ktoré môžu modifikovať napr. tak, že obsahujú repliku vírusu. Vírusy majú teda schopnosť napádať iné súbory, šíriť sa a vyvolávať straty, resp. škody v počítačových systémoch. To je dôvod na ich pomenovanie, ktoré bolo prevzaté z biológie.

Životný cyklus vírusu (virus lifetime) pozostáva zo štyroch fáz. Sú to:

• fáza nečinnosti (dormant phase)
• fáza šírenia (propagation phase)
• fáza aktivizácie (triggering phase)
• výkonná fáza (execution phase).

Vo fáze nečinnosti je vírus v kľudovom stave, teda neprejavuje životnú aktivitu. Je potrebné poznamenať, že nie každý druh vírusu má túto fázu.

Vo fáze šírenia vírus umiestňuje svoju identickú kópiu do iného programu, resp. do určitého sektora disku. Teda každý infikovaný program obsahuje klon vírusu, ktorý je schopný sa ďalej šíriť.

Vo fáze aktivizácie je vírus uvedený do aktívneho stavu. Táto fáza je inicializovaná rôznymi okolnosťami, resp. stavmi infikovaného programu.

Vo výkonnej fáze vírus vykonáva činnosť, ktorá bola naprogramovaná pri vytvorení vírusu. Ide obvykle o deštrukčné činnosti, ktoré vedú k stratám a škodám v napadnutom počítačovom systéme.

Kategorizácia vírusov je vzhľadom na dynamicky vývoj v oblasti tohto druhu škodlivého softvéru veľmi ťažká a dočasná. Prebieha neustály boj medzi autormi vírusov a autormi antivírových programov.

Jeden z možných prístupov ku kategorizácii vírusov delí vírusy do týchto skupín:

• vírusy šíriace sa pomocou spustiteľných súborov (parasitic viruses)
• vírusy šíriace sa cez zavádzacie sektory (boot sector viruses)
• neviditeľné vírusy (stealth viruses)
• polymorfné vírusy (polymorphic viruses)
• makrovírusy (macro viruses)
• e-mailové vírusy (e–mail viruses).

Vírusy šíriace sa pomocou spustiteľných súborov využívajú tieto súbory, ktoré sa veľmi často prenášali medzi počítačmi. Najčastejšie ide o súbory s príponou .com a .exe. Tento typ vírusov je však dnes už menej častý.

Vírusy šíriace sa cez zavádzacie sektory využívaju modifikáciu zavádzacich procedúr v počítačovom systéme. Vírus je zavedený do systému skôr ako operačný systém a skôr ako sa aktivizuje antivírový program.

Neviditeľné vírusy realizujú aktívnu ochranu proti svojmu odhaleniu. Môžu meniť veľkosť napadnutého súboru, ktorá je väčšia o dĺžku vírusu tak, aby tento súbor obsahujúci vírus mal rovnakú dĺžku ako nenapadnutý súbor. Jednoduchý test veľkosti súboru je potom neúčinný. Uvedené typy vírusov môžu napadať databázy vírusov, ktoré sú súčasťou antivírových programov, resp. môžu paralyzovať niektoré mechanizmy antivírových programov. Preto niekedy sa tieto vírusy označujú ako útočné (retrovírusy).

Polymorfné vírusy sa vyznačujú tým, že vytvárajú mutácie pôvodného vírusu, čo sťažuje ich detekciu. Každý vírus totiž obsahuje istý unikátny reťazec, ktorý sa označuje ako signatúra (signature) a ktorý vírus jednoznačne identifikuje. Uvedený fakt využívajú antivírové programy. Polymorfné vírusy menia svoje signatúry, pričom ich funkcia ostáva zachovaná.

Makrovírusy patria do skupiny vírusov, ktoré sa šíria pomocou nespustiteľných súborov. Využívajú určitú aplikáciu, ktorá je obsiahnutá v programových produktoch Microsoft ako sú napr. Word a Excel, ktoré využívajú techniku označovanú ako makro. Programovanie využívajúce makro bolo známe už dávnejšie a uľahčovalo programovanie často sa využívajúcich inštrukcií programu. Makrovírusy využívajú na šírenie skutočnosť, že makrá sa distribuujú spoločne s dokumentom alebovyužívajú vytvárané šablóny, ktoré si nahrávajú všetky otvorené dokumenty. Aktivizácia makrovírusu je riešená viacerými spôsobmi, napr. pri stlačení zlej klávesy, otvorenie určitej aplikácie atď.

Špeciálnu skupinu vírusov tvoria **vírusy šíriace sa pomocou elektronickej pošty** a využívajú zasielané prílohy. Aktivizujú sa otvorením prílohy v prijatej elektronickej pošte. Využívajú vytvorený zoznam adresátov elektronickej pošty (mailing list) a automaticky sa šíria cez tieto adresy ďalšímpoužívateľom. Zároveň napadajú všetky počítačové systémy, ktoré prijali, resp. v ktorý bola prijatánapadnutá elektronická pošta otvorená.

Ďalšiu skupinu programov škodlivého softvéru tvoria:

• červy (worms)
• zombie.

Červ je druh škodlivého softvéru, ktorý na svoje šírenie vo väčšine prípadov nepotrebuje hostiteľský súbor. Aktívne sa šíri cez počítačovú sieť, teda majú schopnosť šíriť sa z jedného počítačového systému na iný počítačový systém pokiaľ sú tieto systémy pripojené do počítačovej siete. Šírenie červov sa najčastejšie realizuje pomocou e–mailových klientov, resp. cez určité služby, ktoré ponúkajú týmto klientom.

Zombie je druh škodlivého softvéru, ktorý sa šíri cez počítačovú sieť (internet) a po úspešnom prieniku do počítačového systému umožňujú prevziať diaľkovú kontrolu nad napadnutým systémom. Niekoľko počítačov napadnutých rovnakým druhom tohto škodlivého softvéru vytvára **botnet**.

Botnety možno riadiť z jedného vzdialeného počítača tak, aby vykonávali rovnaké príkazy. To umožňuje realizovať útok typu DDoS.