**Počítačové vírusy**

**Čo je počítačový vírus?**

* Program alebo kód, ktorý sa dokáže sám šíriť bez vedomia používateľa
* Vkladá kópie svojho kódu do iných spustiteľných súborov alebo dokumentov
* Proces šírenia vírusu nazýva infekcia
* Napadnutému súboru sa hovorí hostiteľ
* Počítače sa môžu infikovať cez rôzne médiá

**Ako sa prejavuje?**

* Spomalenie a nestabilita systému
* Poškodenie dokumentov
* Zmena veľkosti alebo obsahu súborov

**Delenie**

* Podľa umiestnenia v pamäti:
* Rezidentné - po spustení napadnutého programu sa usadia v pamäti počítača
* Nerezidentné -  môžu spôsobovať nákazu len pri spustení napadnutého program
* Podľa cieľa infekcie:
* Bootovacie - aktivuje sa po zavedení systému z napadnutého disku
* Súborové - pripája alebo prepisuje spustiteľné súbory
* Podľa spôsobu infekcie:
* Predlžujúce - pripoja sa na koniec súboru a na začiatok pridajú inštrukciu skoku na telo vírusu
* Prepisujúce - nenávratne prepíšu úvod súboru, ktorý sa potom ako program stáva nefunkčný
* Adresárové - na disku sú uložené len raz, infikujú prepísaním odkazov priamo vo FAT tabuľke
* Kombinované - nachádzajúce sa naraz v súboroch i v boot sektoroch

**Činnosť vírusu**

* Prevzatie kontroly nad procesorom
* Riadenie stavu prostredia
* Inštalácia do pamäte
* Testovanie na spustenie škody
* Záškodnícka činnosť
* Vytvorenie svojej kópie na nájdenom mieste
* Zakódovanie

**Najznámejšie vírusy**

**ILOVEYOU vírus**

* Jeden z najväčších počítačových vírusov
* Spôsobil katastrofu v počítačových systémoch po celom svete a škody vo výške 8,88 miliárd EUR
* Vytvorený bol dvomi filipínski programátormi, ktorý použili sociálne inžinierstvo na to, aby ľudia klikli na prílohu v emaili
* Príloha vyznela ako vyznanie lásky a bol to vlastne skript s textovým súborom.
* V prípade aktivovania vírusu došlo k prepísaniu grafických GIF i JPEG súborov
* To na niektorých počítačoch znamenalo nenapraviteľné škody, ktoré viedli k zmene systémových registrov

**CryptoLocker**

* Ransomware, čo znamená, že je naprogramovaný tak, aby blokoval prístup k súborom alebo počítaču obete, až kým nebude zaplatená suma peňazí
* 5. september 2013 - máj 2014
* Prišiel cez e-mailové prílohy, a keď bol súbor aktivovaný, zašifroval všetky súbory obete
* Útočník dešifruje počítač obete len po zaplatení sumy 356 EUR

**Mydoom**

* Prvýkrát videný 26. januára 2004
* Šíril sa prostredníctvom e-mailu a bol najrýchlejšie sa šíriaci e-mailový červ
* Zaťažoval a upchával mailový server a znižoval výkonnosť podnikovej siete
* Infikoval približne 2 milióny počítačov

**Zeus**

* Zeus, trójsky kôň v sebe skrýval najbežnejšiu úlohu vírusu, a to keylogovanie a prehliadanie formulárov
* Prvýkrát identifikovaný v roku 2009
* Len v USA sa odhadovalo, že sa nakazilo viac ako 1 milión počítačov
* Ukradnutých bolo cca 62 miliónov eur

**Melissa Virus**

* Typ hromadného odosielania makrovírusov
* Vyvinutý 26. marca v roku 1999
* Úlohou vírusu je preťažovať sieť obete
* Spôsobila spoločnosti stratu približne 71 miliónov EUR