Vírusy

Vírusy sú súčasťou Internetu už od jeho počiatku. Vírus je teda program, ktorý je vytvorený tak, aby sám seba kopíroval a poškodzoval používateľove dáta.

1.1.2. Boot vírusy

Boot vírusy napadnú štartovací sektor pevného disku a sú naprogramované tak, aby sa spúšťali pri štarte počítača. V tom prípade ohrozujú počítač pretože antivírusové systémy ešte nie sú spustené.

1.1.3. Makrovírusy

Makrovírusy vyžívajú makrá, články kódu, ktoré sú súčasťou najmä kancelárskych aplikácií typu Office a zvyšujú ich funkcionalitu. Makrovírusy sú schopné sa kopírovať z dokumentu do dokumentu. Snažia sa zmeniť dáta aplikácie alebo modifikovať iné dáta v počítači, čím sa stávajú neželanými škodlivými kódmi. Môžu byť naprogramované pre viacero alebo len pre jeden typ aplikácie, napríklad pre Excel.

1.1.4. Parazitické vírusy

Parazitické vírusy sa správajú presne ako paraziti v prírode. Nájdu si hostiteľa, v tomto prípade program, a pozmenia jeho kód. To spôsobí, že pri každom ďalšom spustení programu sa súčasne aktivuje aj vírus, ktorý poškodzuje počítač obete.

1.1.6. Retrovírus

Retrovírus je typ vírusu zameriavajúci sa na odstránenie antivírusového programu. Ten môže byť zastavený alebo kompletne vymazaný z pamäte počítača. Tým sa stráca ochrana v sieti a počítač sa stáva zraniteľným.

1.2. Trójsky kôň

Hlavným účelom Trójskeho koňa nie je duplikácia, ale spôsobenie škody. Nedokáže sa kopírovať a väčšinou stojí samostatne. Najčastejšie má príponu .exe alebo .com a obsahuje len samostatný škodlivý kód. Trojan môže mať rozlišné funkcie od nainštalovania vírusov až po mazanie súborov.

1.3. Phishing

Názov phishing je odvodený od anglického originálu, password fishing, čo doslova znamená rybolov hesiel. Je to činnosť, pri ktorej sa podvodník snaží získať prístup k heslám používateľov. Väčšinou je k tomuto účelu založená aj webstránka, ktorá na pohľad vyzerá presne ako už existujúca dôveryhodná stránka. Ponúka výhody, ktoré sa majú aktivovať až po prihlásení. Obeť je tak navedená aby vyplnila prihlasovací formulár a následne ho odoslala. Tento formulár však putuje k podvodníkovi, a informácie, v ňom obsiahnuté, sú zneužité. Najčastejšie sa phishing používa na získanie informácií o bankovom konte. Obeti príde e-mail so správou, že jeho banka potrebuje potvrdiť zmenu účtu alebo jeho obnovenie. V správe je priložený aj odkaz, ktorý užívateľa zavedie na stránku banky. Tento odkaz je však podvod a po kliknutí je užívateľ presmerovaný na nepravú stránku. Taktiež sa môže stať že podvodník sa bude vydávať za administrátora a bude požadovať aby mu používatelia poslali dôverné informácie o ich účte pre overenie. Phishing je dodnes populárna metóda a aj keď sa to nezdá, ľudia si nedávajú pozor a posielajú citlivé informácie neznámym v domnienke, že nebudú zneužité.

1.4. Spam

Spam je hromadne rozosielaná nevyžiadaná správa, ktorá väčšinou slúži na reklamu. Šíri sa pomocou e-mailu alebo instantných správ. Tieto správy obsahujú linky na rôzne produkty, ktoré sú takýmto masovým spôsobom propagované. Nevyžiadaná pošta sa môže síriť aj prostredníctvom fór. Do diskusnej skupiny sa pošle správa, ktorá propaguje hlavne pornografický materiál alebo farmaceutické výrobky. Spam sa objavuje aj pri otvorení niektorých stránok ako nové okno oznamujúce, že sme práve vyhrali neskutočnú sumu peňazí alebo podobnú cenu. Po kliknutí na tento odkaz sa do nášho počítača stiahne adware, program, ktorý zahrnie počítač spamom, a môže spôsobiť až nefunkčnosť. Niektorí ľudia zarábajú tým, že zhromažďujú e-mailové adresy do databáz, ktoré neskôr predajú.

1.5. Hoax

Hoax je podvodná reťazová správa, šíriaca sa predovšetkým prostredníctvom e-mailu, vyzývajúca na to aby ju používateľ preposlal. Takáto správa väčšinou varuje pred nejakým nebezpečenstvom, ktoré je v nej podrobnejšie opísané. Tento opis sa skladá z opisu hrozby, spôsobu šírenia a taktiež jeho ničivých účinkov. Následne sú v správe spomenuté aj dôveryhodné zdroje, ktoré nás majú presvedčiť, že správa je skutočná