Škodiace programy - MALWARE

Malware (skratka z *malicious software*) je všeobecné označenie škodlivého softvéru.

Klasické počítačové vírusy

Počítačový vírus je program, ktorý dokáže rozmnožovať sám seba pridávaním svojho kódu do iných programov. Pre svoje rozširovanie teda potrebuje hostiteľa – iný program. Do počítača sa môže dostať jedine tak, že spustíme nainfikovaný program. Spolu so spustením nainfikovaného programu sa aktivuje vírus v operačnej pamäti, a potom napadne i ďalšie súbory v počítači.

Základný algoritmus činnosti vírusu pozostáva: 1. nainfikuj zdravý objekt, 2. vykonaj akciu, 3. vráť riadenie objektu, z ktorého si bol spustený.

Druhy vírusov:

1. v minulosti tzv. boot vírusy, napádali miesto na nosiči dát, z ktorého sa dá zaviesť operačný systém.

2. Makro vírusy, rozšírené v prostredí kancelárskeho balíka MS Office, prípadne aj v iných programoch.

Internetové červy

Červ je tá časť vírusu, ktorá je zodpovedná za jeho šírenie, najčastejšie prostreníctvom e-mailov. Klasickým súborovým vírusom trvalo mesiace až roky, kým sa rozšírili, internetovým červom na to stačí niekoľko dní až niekoľko minút. Kým súborový vírus potrebuje našu pomoc, aby sa dostal z jedného počítača na druhý pomocou diskety, CD alebo iného nosiča, internetový červ sa dokáže rozšíriť i sám pomocou počítačovej siete. Funguje tak, že sa skúša pripojiť na každý možný počítač v počítačovej sieti a na svoj prenos využiť slabé miesto zle zabezpečeného počítača. Na tomto počítači sa červ aktivuje a znovu sa skúša šíriť do ďalších počítačov. Počet nakazených počítačov teda stúpa lavínovite.

Trójske kone

Ide o škodlivý kód pribalený k zdanlivo neškodnému softwéru. Nevie sa šíriť sám. Škodlivá činnosť sa prejavuje napríklad mazaním súborov, formátovaním disku, zasielaním informácií z PC.

Spyware

- monitorovací program, ktorý zhromažďuje a zasiela prostredníctvom internetu informácie z PC bez vedomia používateľa. Ide o informácie o navštevovaných stránkach, nainštalovaných programoch a pod. Do PC sa dostavajú pri inštalácii programov, návšteve niektorých stránok.

Adware

Do tejto skupiny patria programy, ktoré zobrazujú reklamu. Najčastejšie sú súčasťou iného programu, ktorý nie je škodlivý. Je to cesta, akou sa snažia programátori získať peniaze za svoj program. Nebezpečenstvo týchto programov je v tom, že integrované reklamné systémy sú často spywarom.

Spammer

Spammery sú programy, šíriace sa podobne ako vírusy, ktoré rozosielajú spam – nevyžiadanú poštu, ktorá obsahuje reklamu. Každý napadnutý počítač sa stáva odosielateľom nevyžiadanej pošty.

Dialery

- programy, ktoré sa snažia nepozorovane zmeniť dial-up pripojenie k providerovi a presmerovať používateľa na iné číslo, za ktoré sa platí oveľa vyššia tarifa. Niektoré dialery dokonca nastavia spojenie tak, aby zostalo otvorené aj po zatvorení prehliadača. Najčastejšie sa programy nachádzajú na stránkach s erotickým a pornografickým materiálom ponúkajúcich „Instant Access“ (priamy prístup), bez nutnosti použitia šekov a kreditných kariet. Z toho vyplýva, že sa aktivuje pričinením používateľa, a preto ani poskytovateľ pripojenia neuzná reklamáciu vysokej faktúry. Našťastie sa dnes už vytáčané linky stávajú raritou, no svoj počítač môžete ochrániť i programom antidialerom, ktorý zabráni zmene nastavenia internetového pripojenia.

PopUp a Hijackery

Do tejto kategórie patria programy vložené do webových stránok, ktoré otvárajú okná s reklamou. Tieto okná sú najčastejšie také agresívne, že pri pokuse zatvoriť ich, sa otvoria ďalšie. Takéto programy sa nachádzajú na stránkach s pornografickými materiálmi, hudbou, či zvonení do mobilov. Tieto okná však dnes už blokuje väčšina moderných prehliadačov.

Niektoré druhy malware (tzv. Hijackers) spôsobujú "samovoľné" otváranie okien prehliadača i v čase, keď používateľ žiadne webové stránky neotvára, prípadne menia nastavenie Vašej domovskej stránky, stránok s chybovými hláseniami prehliadača a vyhľadávacie stránky na svoje vlastné. Nepríjemné je to, že znemožnia nastavenie týchto stránok späť. Ďalšou nepríjemnosťou je, že sú to najčastejšie stránky s pornografickým obsahom, na ktorých sa môže nachádzať ďalší škodlivý malware.

Hoaxy

Časté sú falošné správy nazývané tiež Hoax, čo sú poplašné správy napríklad varujúce pred počítačovými vírusmi, nebezpečenstvom zneužitia mobilných telefónov, e-mailové petície (ktoré v skutočnosti nemajú nijakú právnu váhu), prosby o darovanie krvi (ktoré môžu byť spočiatku legitímne, ale po strate aktuálnosti sa často šíria reťazovo ďalej, čím sa stávajú hoaxom) a mnoho ďalšieho.

Phishing

Existujú i také správy, ktoré sú písané s cieľom podvodu. Takéto správy sa odborne nazývajú Phishing. Typickým príkladom sú e-maily, ktoré vyzývajú na zmenu kódu k bankovému účtu. V takomto e-maile je umiestnený odkaz, na ktorom si heslo máte zmeniť. Odkaz však nesmeruje na stránku banky, ale na jej dokonalú napodobeninu. Takéto správy sú väčšinou veľmi formálne napísané. Niektoré dokonca vyzerajú tak, akoby ich odosielateľom bola samotná banka. Pri každej takejto správe treba spozornieť, keďže banky nikdy nevyzývajú na podobné operácie e-mailom.

Pharming

Najzákernejší spôsob je Pharming. Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu. Ak zadáte mennú adresu do Vášho prehliadača, miesto stránky banky sa zobrazí jej dokonalá napodobenina. Vy teda ani nezbadáte, že ste na inej stránke. Po zadaní údajov, ich získa neoprávnená osoba, ktorá takúto falošnú stránku vytvorila.

Boj proti malwaru

Odporúčania sú tieto:

- **Zálohujte všetky svoje údaje na disky chránené proti zápisu**. Zálohovaním dát sa vyhnete i strate konzistencie dát následkom výpadku prúdu alebo tvrdého reštartu.
- **Používajte menej rozšírený operačný systém, prehliadač a poštového klienta**. Väčšina malwaru pracuje pod operačným systémom MS Windows, prehliadačom Internet Explorer a poštovým klientom Outlook.
- **Zabezpečte svoj počítač proti neoprávnenému vniknutiu**. Tento krok môžete urobiť použitím tzv. Firewallu, ktorý vytvára ochranu medzi vaším počítačom a potenciálne škodlivým obsahom na Internete.
- **Nenavštevujte nebezpečné stránky a nesťahujte programy na sťahovanie hudby, filmov a programov**.
- **Pred stiahnutím každého Freeware programu si pozorne prečítajte, či jeho súčasťou nie je niektorý z uvedených nebezpečných programov.**
- **Nezverejňujte svoju emailovú adresu**.
- **Neotvárajte neznáme prílohy**.
- **Nepripájajte neoverený zásuvný modul ActiveX**.
- **Majte vždy najaktuálnejšiu verziu Java Runtime Enviroment**.
- **Nespúšťajte neoverené makrá v dokumentoch**. V súčasnosti sa i makrá podpisujú digitálnym podpisom. Preto si pred jeho spustením overte platnosť digitálneho podpisu a neaktivujte neznáme makro.
- **Udržujte všetky súčasti systému aktuálne, používajte najnovšiu verziu prehliadača a poštového klienta**.
- **Chráňte svoj počítač aktuálnym antivírovým systémom**.
- **Chráňte svoj počítač proti špionážnym programom**. Na ochranu proti takýmto programom sú najvhodnejšie programy Windows Defender priamo od spoločnosti Microsoft.
- **Znížte svoje oprávnenie**. Nikdy nepracujte s internetom a poštou s oprávneniami správcu počítača.