KAJ JE TO

Škodljiva programska oprema je ustvarjena za izvajanje nelegitimnih posegov v računalniški sistem, kot so uničevanje, nepooblaščen dostop do podatkov in oviranje delovanje sistema.

 V splošnem deluje tako, da se namesti na računalnik (ga »okuži«) in nato prikrito spreminja njegovo delovanje v korist hekerja, pri čemer izkorišča ranljivost [operacijskega sistema](https://sl.wikipedia.org/wiki/Operacijski_sistem) ali druge programske opreme, nameščene na žrtvinem računalniku.

Veliko programov se namesti na računalnik tako, da uporabnik izvede neko dejanje – nevede požene na videz neškodljiv program ali odpre [datoteko](https://sl.wikipedia.org/wiki/Datoteka), ki vsebuje zlonamerno kodo. (Virus, črv trojanski konj,…) Ti pa ne nujno takoj povzročijo škodo in je to odvisno od kode, ki jo je nekdo napisal. Lahko začne delovati po nekem času

VRSTE ŠKODLJIVIH PROGRAMSKIH OPREM

Trojanski konj je najbolj razširjen zlonameren program. Ime je dobil po trojanskem konju iz preteklosti. Njegova naloga v računalniku je, da nastavi backdoor, to so stranska vrata v vaš računalnik s pomočjo teh lahko heker vdre v vaš računalnik z daljave in vam pokrade podatke. Trojanski konj se sam razmnožuje in ne spada pod viruse.

Računalniški črv se samodejno širi po računalniškem omrežju. Podobno kot virus se brez vednosti uporabnika namesti na računalnik, od samega črva pa je odvisno, kaj bo na okuženem sistemu naredil. Lahko prisluškuje tipkovnici, sodeluje pri napadu na tuj računalnik ali pa briše, spreminja in napadalcu pošilja podatke iz računalnika.

Računalniški virus je dobil ime po biološkem virusu zaradi podobnih nalog, ki jih izvršujeta. Računalniški virus lahko vašemu računalniku zbriše podatke na trdem disku, stalno se vam pojavljajo razni zapisi. Virus vam lahko tudi obremenjuje procesor in zapolnjuje pomnilnik.

* makro virusi, ki se aktivirajo z odprtjem okuženega dokumenta
* virusi zagonskega sektorja, ki začnejo delovati ob zagonu računalnika
* programski virusi, ki začnejo delovati ob odprtju programa
* bootstrap virusi, ki spremenijo vašo vsebino s svojo
* parasitic virusi, ki vam okužijo vse .com in .exe datoteke in spremenijo njihovo kodo tako, da programi ne delujejo več

Zajček deluje tako da se hitro razmnožuje, da se na koncu računalnik žrtve upočasni in crash

Bomba pa zbriše vse datoteke na računalniku

DRUGA ŠKODLJIVA PROGRAMSKA OPREMA

* Vohunska programska oprema ali spyware (to beleži dejanja npr. vtipkanje gesla ali sezname obiskanih spletnih strani.
* Oglasna programska oprema ali adware (prikazuje uporabniku neželene oglase)
* Boti (to je oprema, ki samodejno pošilja neželene e-poštne sporočila, naročila)
* Izsiljevalska programska oprema ali ransomware ( onemogoči dostop do podatkov, dokler žrtev ne plača odkupnine)
* Strašilna programska oprema ali scareware (prestraši žrtev da je njen računalnik okužen, potem ponudi lažen antivirusni program, ki lahko vsebuje zlonamerno kodo.

KAKO SE ŠIRIJO

Poznamo več načinov širjenja zlonamernih programov, najpogostejši so:

* Če imate nameščeno starejšo verzijo nekega programa, za katerega je znana varnostna ranljivost (hujša napaka v kodi programa), lahko napadalec izkoristi to ranljivost tako, da preko nje okuži vaš računalnik.
* Preko USB-ključev
* Preko družbenih omrežij
* Preko elektronske pošte
Nekoč najpogostejši način širjenja zlonamernih programov prek elektronske pošte danes zaradi antivirusnih filtrov na poštnih strežnikih ni več tako razširjen.

KAKO SE ZAVAROVARI

Protivirusni program je [računalniški program](https://sl.wikipedia.org/wiki/Ra%C4%8Dunalni%C5%A1ki_program) oziroma skupek programov, ki so namenjeni za preprečevanje in odstranjevanje [virusov](https://sl.wikipedia.org/wiki/Ra%C4%8Dunalni%C5%A1ki_virus) in druge zlonamerne programske opreme saj se [računalnik](https://sl.wikipedia.org/wiki/Ra%C4%8Dunalnik) brez protivirusnega programa lahko okuži takoj, ko je povezan z [internetom](https://sl.wikipedia.org/wiki/Svetovni_splet). Ker se dnevno pojavlja več tisoč novih oblik zlonamerne programske opreme, morajo podjetja, ki izdelujejo protivirusne programe, le-te konstantno posodabljati in enako morajo storiti tudi njihovi uporabniki.

Poznamo več vrst protivirusnih programov: avast, ESET, panda, microsoft security, malware

njihov način delovanja pa se lahko razlikuje:

1. Pregledovanje oz. skeniranje datotek na računalniku. Tak protivirusni program ima zbirko kod za posamezne viruse. Če pri skeniranju zazna katero od teh kod, poskuša datoteko zbrisati ali popraviti.

2. Pregledovanje programov, ki so sumljivi in predstavljajo grožnjo.

3. Sandbox je pa program, ki naredi simulacijo operacijskega sistema, v katerem analizira delovanje nekega programa.