Štetni programi (MALWARE) (engl. **Mal**icious Soft**wer**)

1. virus: - su programi koji, za razliku od ostalog softvera, posjeduju neka svojstva slična zloglasnim pandanima iz (polu)živog svijeta na kojima temelje svoje maliciozno djelovanje. Jedno od njih je svojstvo samoumnožavanja. Jednom pokrenut računalni virus će potražiti druge datoteke na računalu koje će nastojati inficirati.Virusi se najčešće šire s jednog računala na drugo u obliku izvršnog zlonamjernog koda putem Interneta, privitaka u e-mail porukama ili medija poput, eksternog hard diska, CD, DVD ili USB sticka.

   Da bi se virus umnožio pokretanjem izvršenja malicioznog koda, virusi se **vežu za izvršne datoteke** legitimnih programa. Tako se u slučaju pokretanja zaraženog legitimnog programa, istovremeno pokreće izvršavanje i virusnog koda.

   Prema svom načinu djelovanja, virusi se dijele se na dvije vrste, nerezidentne i rezidentne.
   Nerezidentni virusi se nalaze u RAM memoriji samo u vrijeme njihovog izvršenja, odnosno od njihovog pokretanja pa do završetka rada.
   Rezidentni virusi se prilikom njihovog izvršenja učitaju u memoriju i njihov kôd ostaje u memoriji cijelo vrijeme rada računala. Na taj način se postiže efekt zaraze i nad novim instaliranim aplikacijama.

2. crv:

Crv je samostalan program koji se za širenje oslanja prvenstveno na vlastite mehanizme i na računalnu mrežu. Iznimno su zloglasni tzv. mass mailing crvi koji se šire u privitku e-mailova:obično će se poslati na sve e-mail adrese koje zateknu u adresaru na inficiranom računalu, pri čemu često koriste ugrađeni vlastiti mail-poslužitelj. Osim maila, crvi redovito zlorabe razne druge mrežne komunikacijske protokole kako bi se u što kraćem vremenskom roku proširili Internetom.

3. trojanski konj (trojan)

-program koji se **pretvara** da izgleda kao i svaki drugi korisnički program. Za razliku od crva, virusa i nekih drugih vrsta malicioznog softvera, trojanski konji ne mogu raditi samostalno.

Tipovi trojanskih konja:

Postoji više tipova trojanskih konja a karakterizirani su prema više kriterija:

- prema načinu djelovanja,

- prema akcijama koje čine na korisnikovom računalo i drugim kriterijima.

Neki od najraširenijih tipova uključuju:

- RAT (Remote Access Trojans) – Trojanski konji s udaljenim pristupom
- DST (Data Sending Trojans) – Trojanski konji koji šalju podatke
- Destrucitve Trojans – Trojanski konji koji uništavaju datoteke i općenito sadržaje na računalu
- Proxy Trojans - Trojanski konji koji djeluju na proxy servere ili ih iskorištavaju za svoje djelovanje
- FTP Trojans – Trojanski konji koji djeluju na File Transfer Protocol ili ga iskorištavaju za svoje djelovanje

http://www.cert.hr – Croatian National Computer Emergency Response Team

Metode otkrivanja i zaštite od virusa

Postoje dvije metode kojom se antivirusni programi koriste u svrhu otkrivanja malvera.

Prva metoda je korištenjem baze poznatih otkrivenih definicija malvera. Ovo je najkorištenija metoda detekcije koja pretražuje sadržaj memorije računala, boot sektora i sadržaja svih foldera. Jedini nedostatak ove metode je što su računala zaštićena od infekcije trenutnim postojećim definicijama virusa kojima se ažurira njihova baza.

Druga metoda je korištenje heurističkog algoritma za otkrivanje malvera baziranih na istom načinu djelovanja. Heuristički algoritam ima mogućnost ponuditi prihvatljivo rješenje za nastali problem u raznim slučajevima, ali isto tako i ne znači da daje točne rezultate provedene detekcije virusa.

Preventivne mjere od zaraze štetnim programima

- upotreba antivirusnog softvera s ažuriranom bazom podataka mogućih napada (npr: NOD32, Norton Antvirus, Kaspersky, Avira, Avast i dr.)
- redovito nadograđivati (update) operacijski sustav i najkorištenije aplikacije kao što su Microsoft Office, Adobe Reader, Mozilla Firefox i dr.
- redovita izrada rezervnih kopija podataka ili operativnog sustava
- treba biti oprezan i NE aktivirati bilo kakve izvodljive datoteke ponuđene mailom ili nekim drugim Internet servisom (datoteke koje imaju ekstenziju exe, bat, cmd, pif, i dr.)
- uključen firewall (hrv. vatrozid)

Mjere nakon zaraze

- potrebno je uvijek očistiti računalo odmah nakon infekcije i nikako ne ignorirati upozorenja virus skenera.
- malver se može očistiti i softverom za deinstalaciju pojedinog primjerka. Takav softver se često može pronaći na stranicama antivirusnih kompanija.
- ako se malver ne može očistiti, potrebno je reinstalirati operacijski sustav i vratiti s kopije izgubljene podatke. Podaci moraju biti kopirani prije infekcije.

https://docs.google.com/forms/d/1QU_BjmrcUa0Q0FijL9nL8cUvQ2OiP1yJ038Ee65b92g/viewform?usp=send_form