

Zlonamjerni softver

MALWARE



Pojam i definicija

- Riječ **Malware** nastala od riječi **Malicious** i **Software** i prevodi se kao „zlonamjerni (maliciozni) softver“
- Malware je zlonamjerna i neželjeni program koji pristupa računaru bez odobrenja korisnika i ima za cilj da nanese štetu računaru, stekne neovlašćen pristup računarima ili mreži i zloupotrijebi informacije koje se u njemu nalaze.
- Malver je poput digitalnog virusa koji može zaraziti računare i druge elektronske uređaje. Baš kao što vas virus može razboleti, malver može učiniti da se vaš računar ponaša čudno ili da ne radi ispravno.

Simptomi infekcije

Usporen rad računara

- Sporije otvaranje aplikacija
- Zamrzavanje računara

Nepoželjne promjene u postavkama

- Promjene podešavanja operativnog sistema, web pretraživača

Nepoželjna reklamiranja

- Pop-up prozori, baneri
- Neželjeno preusmjeravanje na reklamne stranice

Gubitak podataka

- Brisanje ili šifrovanje vaših fajlova

Nestabilnost sistema

- Padovi sistema, neočekivano restartovanje
- Plavi ekrani

Povećana upotreba resursa

- Opterećivanje CPU i RAM

Nedostupnost antivirus programa

- Blokiranje rada antivirus programa
- Blokiranje preuzimanja i instalacije antivirus programa

U malware spadaju:

1. VIRUS
2. CRV
3. TROJANAC
4. Spyware
5. Adware
6. Ransomware
7. Browser Hijacker

VIRUS



Mali samokopirajući program.

Prikači se za neki program ili fajl

Širi se kada pokrenemo zaraženi program ili otvorimo zaraženi fajl

Može izazvati različite posljedice – oštetiti računar, formatira disk, preuzme lozinke, lične podatke i dr., do potpunog preuzimanja kontrole nad računarom

CRV (worm)



Program koji se sam replicira tj. kopira na više mjesta i najčešće se širi putem elektronske pošte ili zaraženog fleš memorijskog uređaja

Samostalan program - nije potrebno da se veže za neku datoteku ili program (za razliku od virusa)

TROJANAC



Zlonamjerni program koji je „maskiran“ u koristan program (npr. prikazuje se kao antivirus program a u stvari omogućava virusima ili hakerima ulaz u rač.sistem)

Nema mogućnost da sam sebe umnožava

Termin potiče od grčke priče o trojanskom konju

SPYWARE



Spyware se prevodi kao „špijunski program“

Program koji se tajno instalira na nekom računaru, prikuplja informacije o korisniku zaraženog računara i šalje ih svom autoru.

Može da prikuplja privatne informacije, informacije o posjećenim stranicama, korisnička imena, lozinke, brojeve platnih kartica i sl.

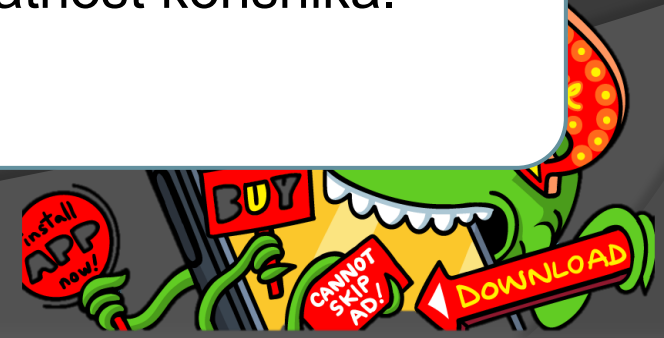
Posebna vrsta špijunskih programa su Keylogger programi koji pamte sve što korisnik otkuca na tastaturi i te podatke zloupotrebljavaju

ADWARE

Advertising supported software – softver čiji je cilj reklamiranje

Adware je bilo koji program koji automatski pušta, pokazuje ili preuzima reklame na vaš računar. Ove reklame mogu biti u više formata, a najčešći je pop-up prozor koji se pojavljuje prilikom surfovanja internetom.

Adware sam po sebi ne nanosi nikakvu štetu korisniku ali može u sebi sadržati i spyware pa se svrstava u programe koji narušavaju privatnost korisnika. Može da prati i aktivnost korisnika na internetu i to koristi u marketinške svrhe.



RANSOMWARE



Ransomver vas zaključava van vašeg sopstvenog računara ili šifruje vaše datoteke, a zatim traži novac (otkup) da vam ponovo omogući pristup.

ransom = otkup

Ransomware obično ulazi u računar putem zlonamjernih email priloga, linkova, ili preuzimanjem zaraženih programa ili fajlova sa nesigurnih izvora.

Kada se ransomware aktivira, šifruje fajlove na žrtvinom računaru, čineći ih nedostupnim.

Može ciljati pojedince, a i velike organizacije, institucije i kompanije

BROWSER HIJACKER

HIJACKER= razbojnik, otmičar

Browser hijacker je tip zlonamjernog softvera koji ima za cilj preuzeti kontrolu nad vašim veb pregledačem (browserom) i izmijeniti njegove postavke bez vašeg odobrenja

Većina hijacker-a promijeni početnu stranicu (home page), alate za pretragu (search engine) i dodati neke ekstenzije i trake sa alatima na pregledač

Browser hijacker često prikazuje veliku količinu reklama u obliku iskaćućih prozora, banner-a ili automatskih preusmjeravanja na reklamne stranice. Ove reklame mogu biti iritantne i ometati normalno surfanje internetom.

Web sajt koji se otvara pomoću ovog programa može da prikuplja informacije o računaru i internet ponašanju čiji je browser napadnut, i šalje ih trećoj strani bez vašeg znanja i odobrenja

PREVENCIJA I ZAŠTITA

- ⦿ Upotreba **antivirus programa** – softvera koji pruža zaštitu, otkrivanje i uklanjanje malware-a.
- ⦿ **Budite Oprezni:** Ne preuzimajte datoteke niti otvarajte linkove sa nepoznatih ili sumnjivih izvora. Budite oprezni prilikom otvaranja email priloga, posebno od nepoznatih pošiljalaca.
- ⦿ **Ažurirajte Svoj Softver:** Redovno ažurirajte operativni sistem, veb pretraživače i druge programe. Ažuriranja često sadrže sigurnosne popravke.
- ⦿ **Napravite Rezervne Kopije Vaših Podataka:** Redovno pravite rezervne kopije važnih datoteka na eksternom disku ili servisu u oblaku.
- ⦿ **Obrazujte Se:** Budite svjesni uobičajenih online prevara i pokušaja phishing-a. Ne dijelite lične informacije na mreži osim ako to nije apsolutno neophodno.

Najpoznatiji antivirus programi koji su besplatni:

- Avast Free antivirus
- Avira Free antivirus
- AVG Antivirus Free
- Bitdefender Antivirus Free edition
- Malwarebytes



Najpoznatiji antivirus programi koji se plaćaju:

- **Avast Pro antivirus**
- **ESET NOD32**
- **Kaspersky Antivirus**
- **Bitdefender Antivirus Plus**
- **Norton Antivirus**

Pravila za antivirus programe

- ⦿ Najbolje je instalirati jedan antivirus program, jer više antivirus programa previše opterećuju sistem i smetaju jedan drugom
- ⦿ Antivirus program mora redovno da se ažurira (update). Postoje dvije vrste ažuriranja kod antivirusa: ažuriranje samog softvera i ažuriranje podataka o virusima (virus database)
- ⦿ Kad se priključi fleš memorija ili skine neki fajl sa interneta, treba odmah skenirati pomoću antivirus programa