ONLINE SIGURNOST

I

ZAŠTITA PODATAKA

Samir Mujović

VP

Uvod

- Ko je i šta je Samir Mujović?
- Ko je i šta je Zemana?
- Firma koja se bavi izradom globalnih sigurnosnih rješenja
- Stručni tim za borbu protiv programa sa uzrokom finansijske štete i krađama identiteta,
- Bezbjednosne aplikacije sa niskom potrošnjom resursa,
- 10 miliona krajnjih korisnika širom svijeta,
- Naš portfolio korisnika seže od običnog građanstva do telekomunikacijskih kompanija, vojne i nuklearne industrije, finansijskih institucija, univerziteta itd.

Kratki pregled

Online Opasnosti:

- Historijat online opasnosti
- Vrste i funkcije određenih opasnosti?
- Vrste online opasnosti
- Kako prepoznati online opasnosti?
- Globalni trendovi na polju sigurnosnih opasnosti
- Koji su oblici zaštite i najčešće zablude o njima?

Zaštita podataka:

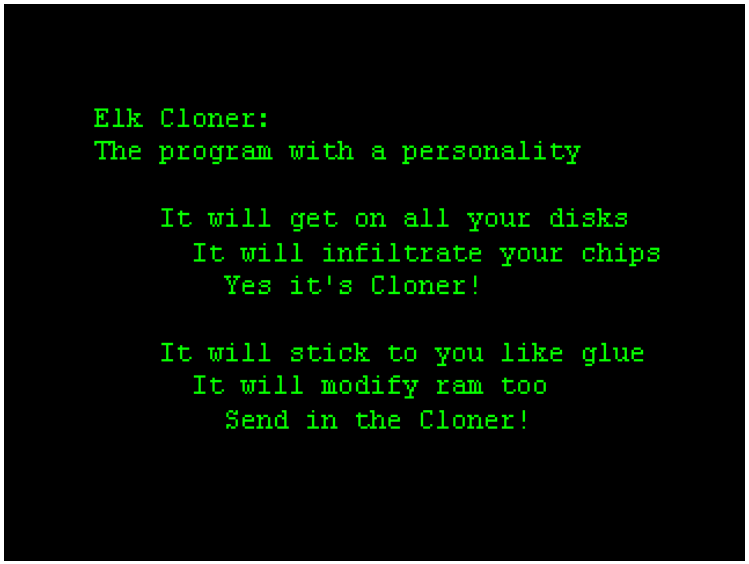
- Da li je samo jedan način zaštite dovoljan?
- Kako se efikasno zaštiti od online opasnosti?
- Kreiranje „sigurnog okruženja“
- Edukovanje korisnika o potencijalnim opasnostima
- Pitanja

Historijat (prije internet ere)

Zloćudni softveri prije ere interneta prenosile su se teže i to je uglavnom bilo fizički putem floppy disk drive-a ili fabričke greške.

Neki od poznatijih zloćudnih virusa tog doba su:

- Brain (1986),
- Lehigh, Stoned, Jerusalem (1987),
- the Morris worm (1988),
- Michelangelo (1991),
- DMV (1994),
- Cap.A (1997),
- CIH poznatiji kao "Chernobyl" (1998),
- Melissa (1999)
- Kak (1999-2000)

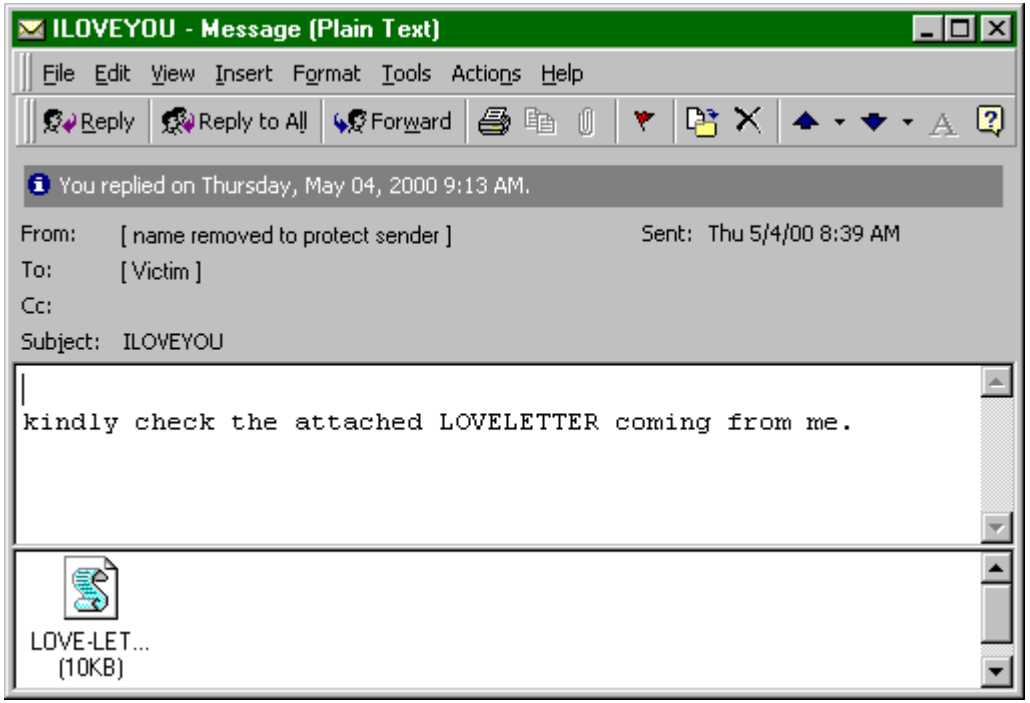


1982 je oficijalno godina nastanka prvog Zloćudnog softvera („Elk Cloner“, Rich Skrenta)

Historijat (sa internet erom)

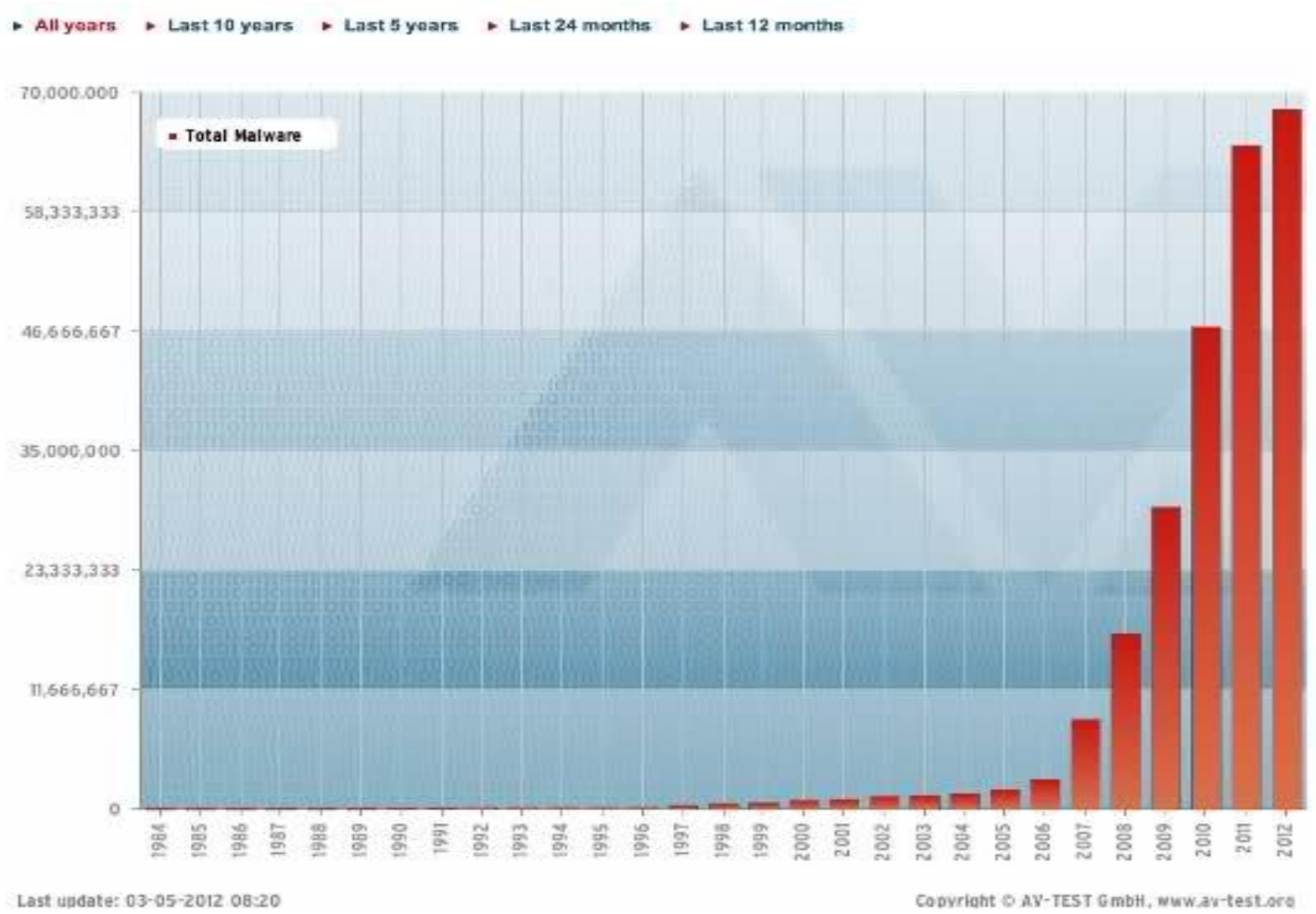
Zloćudni softveri početkom internet ere prenose se puno lakše i to je uglavnom bilo putem e-mailing servisa, zatim webservisa, IRC konekcija do konačnih remote konekcija.

- Loveletter (Maj 2000),
- Anna Kournikova (Feb. 2001),
- Magistr (Mart 2001),
- Sircam (Maj 2001),
- CodeRed (Jun 2001),
- Nimda (Avgust 2001),

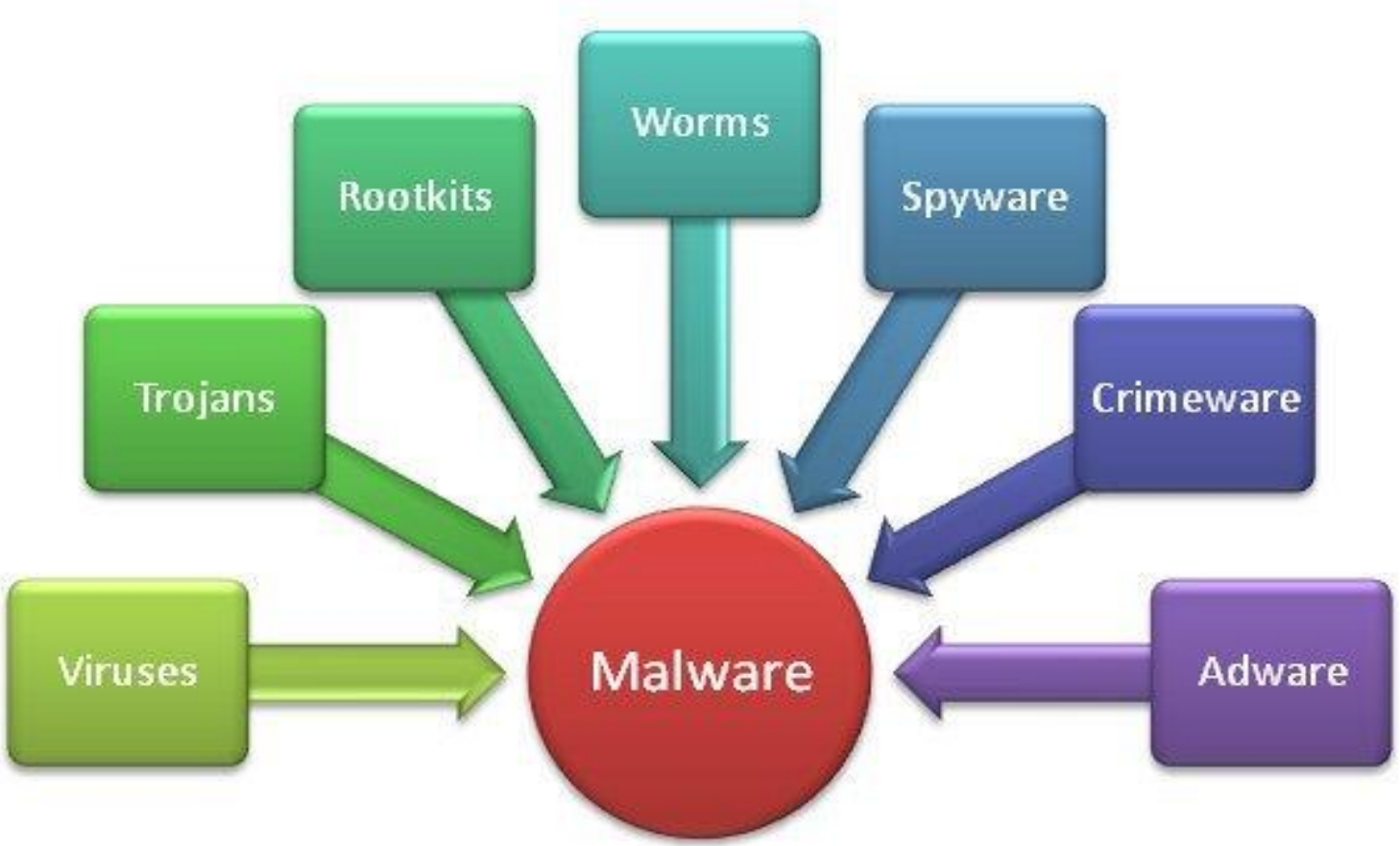


2002 godina je godina prekretnica za zloćudne softvere

Ekspanzija malware



Vrste online opasnosti



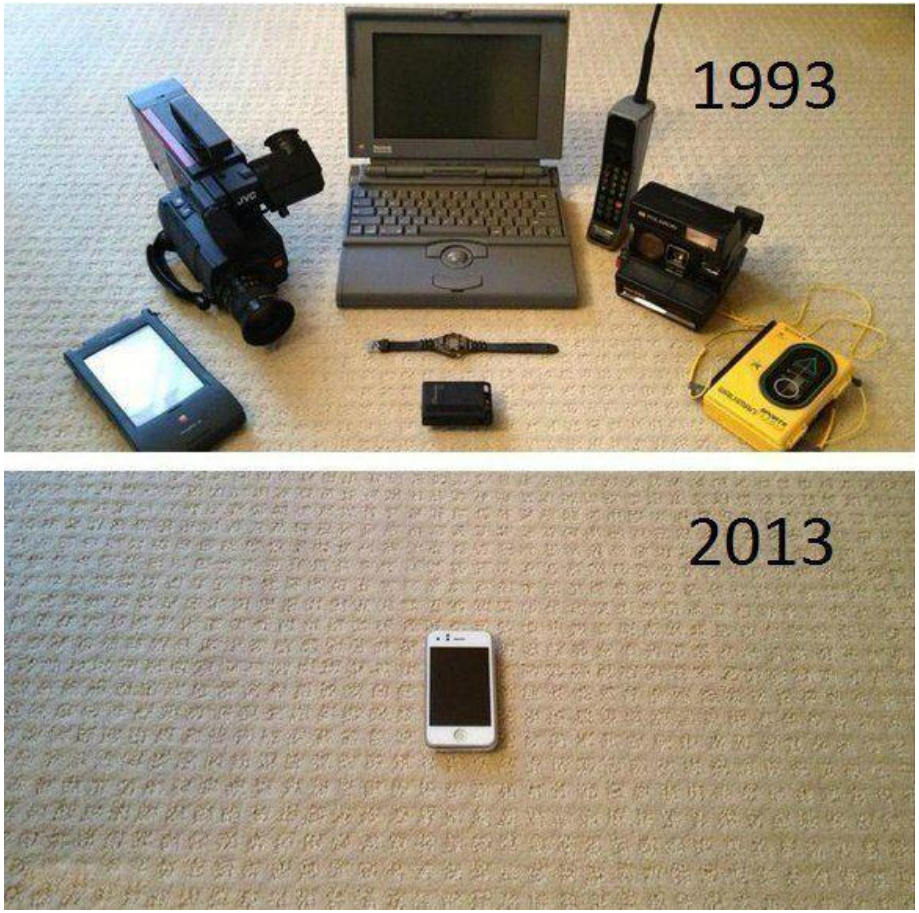
Karakteristike i funkcije opasnosti

- **Virus**: Inficira programske datoteke i / ili lične datoteke
- **Spyware**: Softver koji prikuplja lične podatke
- **Worm**: Malware koji se može replicirati preko mreže
- **Trojanac**: Malware koji izgleda, a možda čak i radi, kao legitiman program
- **Browser hijacker**: Softver koji modifikuje /otima vaš web preglednik.
- **Malvertising**: Korištenje legitimnog onlIne marketinga za širenje zlonamjernog softvera.
- **Rootkit**: Softver koji dobija administratorska prava za zlonamjernu upotrebu.
- **Ransomware:** Malware koji zarazi računarski sistem, šifrira podatke korisnika, a potom zahtjeva novac da dešifruje podatke.
- **Persistent Malware**: ponavljajuća i neotklonjiva opasnost.
- **Firmware-based Malware:** najstrašniji od svih oblika malwera je vrsta koja se instalira u hardverske komponente kao što su hard diskovi, sistemski bios i druge periferije.

Trendovi online sigurnosti

Stvari koje je zamijenio Smartphone:

Pejdžer, Kamere, Radio, CD plejer, Kalkulator, Diktafon, GPS, Svjetlo blica, Kompas, Prijenosni uređaj za igre, gaming konzole, Skener barkoda, video plejer, Walkie-Talkie, Telefonski štand, Sat / budilnik, Ručni sat, Tajmer Štoperica, Knjige, Kalendar, Notepad / Sketchpad, Novine, Foto album, Lista kontakata / imenik, Igre na tabli, Provjera e-pošte, Internet surfanje, Video Chat klubove, Termostat, Mjerna traka, Mjerač svetlosti, Bankomat / debit / kreditne kartice, Avionske karte, Poslovne kartice, Daljinski upravljač, Car Keys, Papirni novac / kovani novac, Kablovska TV, Prenosivi računari, Weather Channel, Lični kupac, Uređivač enterijera, Krosword Puzzle, Mašina za slotove, Komunikacijske veštine, Vodič za TV, Lupo, Faks mašina, Ljubavna pisma, Razglednice, Markice...



Opasnosti na mobilnim uređajima su u trendu porasta

Postoje dva glavna razloga zašto zlćudni programi koji ciljaju mobilne uređaje predstavljaju toliku opasnost :

1. Mobilni uređaji se sve više proizvode i koristi ih sve veći broj korisnika.

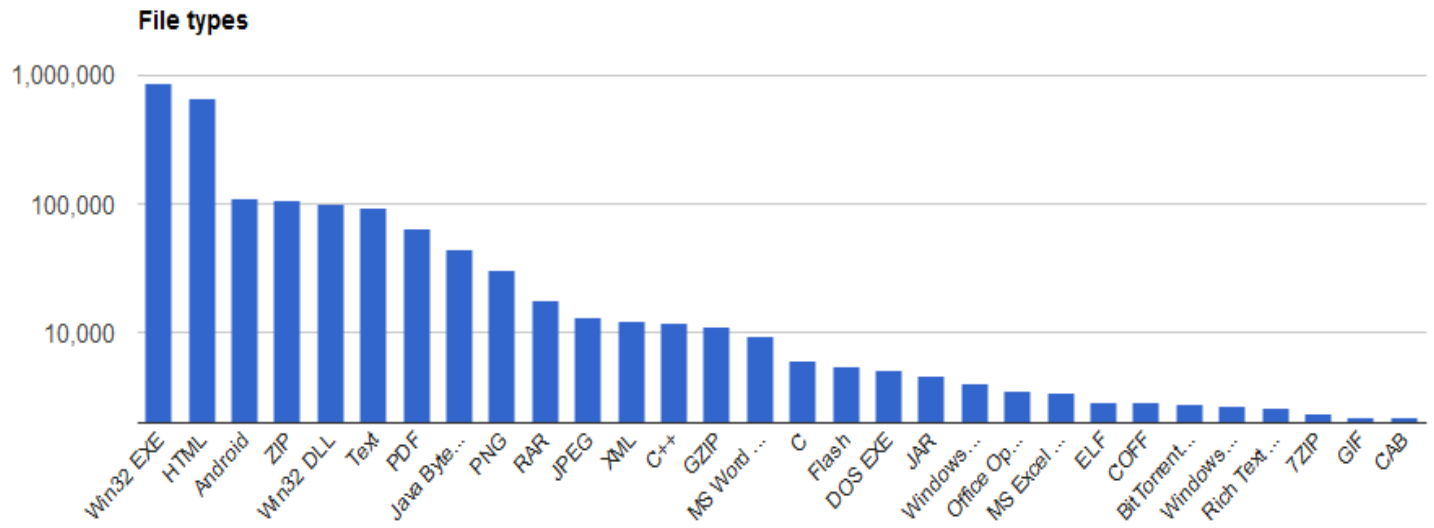
2. Korisnici nisu svjesni prijetnji mobilnim uređajima i ne posjeduju znanje o postojanju takvih prijetnji uprkos širokoj upotrebi mobilnih uređaja.

(Stručnjaci za zlćudne programe su utvrdili da su zlćunih programi za mobilne uređaje u istoj fazi u kojoj su bili i zlćudni programi za Windows platformu za vrijeme njihovog slavnog perioda od 1990. do 2010.

Prema posljednjim izvještajima sigurnosnih kompanija, 99% svih mobilnih zlćudnih programa ciljaju Android platformu. Statistike pokazuju da je 1 od 10 Android uređaja zaraženo zlćudnim programima, što je jasan pokazatelj toga kako je loša situacija sa mobilnim zlćudnim programima.

Opasnosti na mobilnim uređajima

Više korisnika privlači više uređaja. Više uređaja privlači više prijetnji.



Sigurnost podataka na mobilnim uređajima

Programi koji ciljaju mobilne uređaje su daleko opasniji od zlćudnih programa koji ciljaju Windows platformu jer oni mogu:

- preusmjeriti, prisluškivati i ozvučiti sve telefonske razgovore, glasovnu poštu i čitati sve SMS-ove.
- otkriti lokaciju korisnika pomoću GPS-a
- ozvučiti i snimiti sve korisnikove razgovore u prostoriji pomoću mikrofona mobilnog uređaja
- pristupiti svim tonskim, video ili foto zapisima koji su spremljene na mobilnom uređaju
- obrisati ili oštetiti bilo koji ključni dio sistemskog softvera mobilnog uređaja
- da ponište sistemsku performansu i oštete bateriju mobilnog uređaja ili neku drugu hardversku komponentu
- mogu preusmjeriti, snimiti ekran i ukrasti povjerljive finansijske podatke dok korisnik koristi online bankovne aplikacije kao i identifikacijske podatke kroz aplikacije društvenih mreža (npr. PIN, lozinke itd.)
- izvršiti ‘’phishing’’ napade, slanjem spam poruke putem SMS-a sa skrivenim linkove za skidanje potencijalno neželjenih programa
- itd. .....

Oblici zaštite od malware

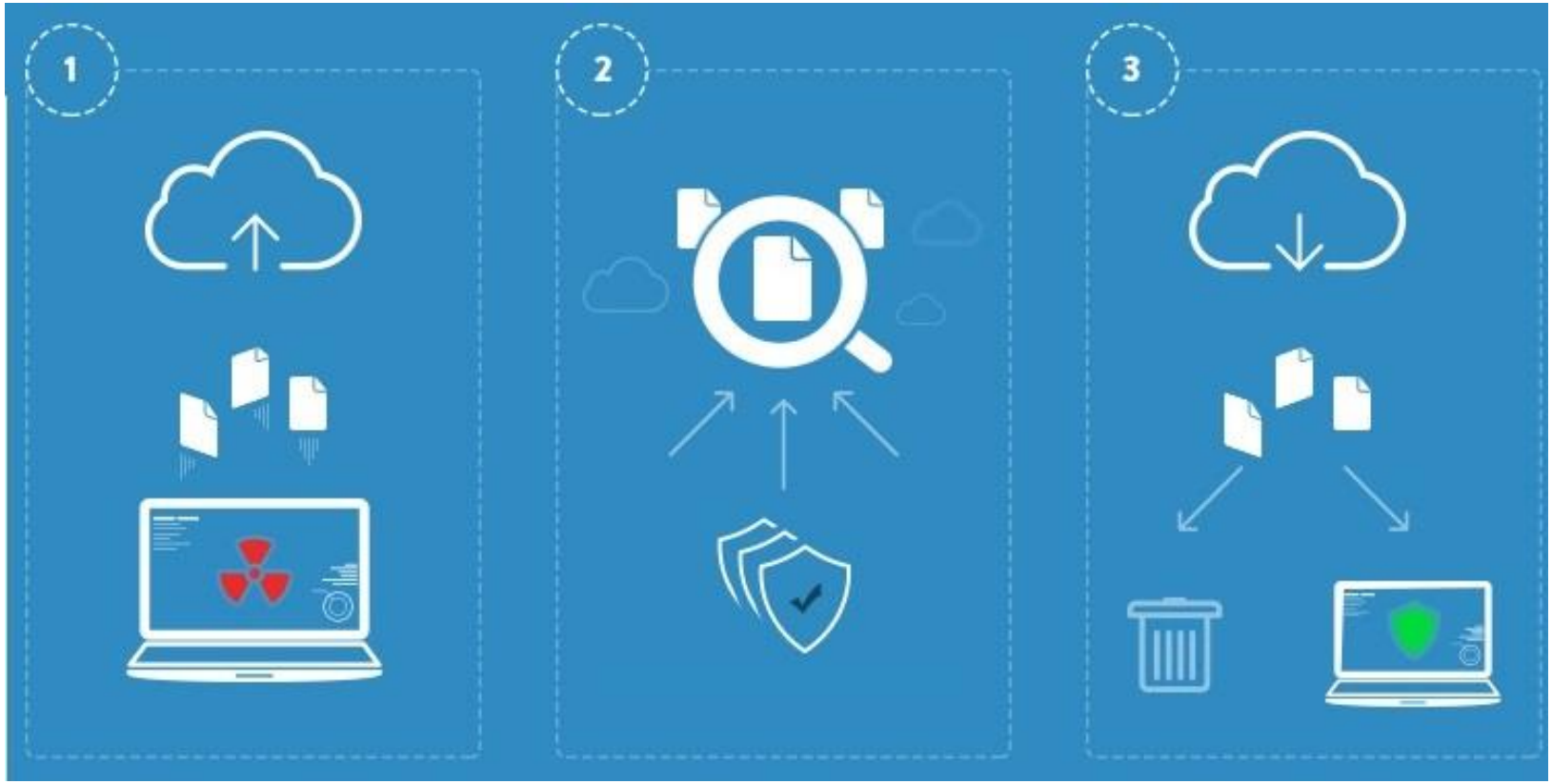
Šta je AntiVirus?

Antivirus je softver, prvobitno dizajniran da otkrije i ukloni viruse sa računara, a danas može zaštititi od širokog spektra pretnji, uključujući i druge vrste zlonamjernog softvera tj. malware

Antivirusni softver obično obavlja ove osnovne funkcije:

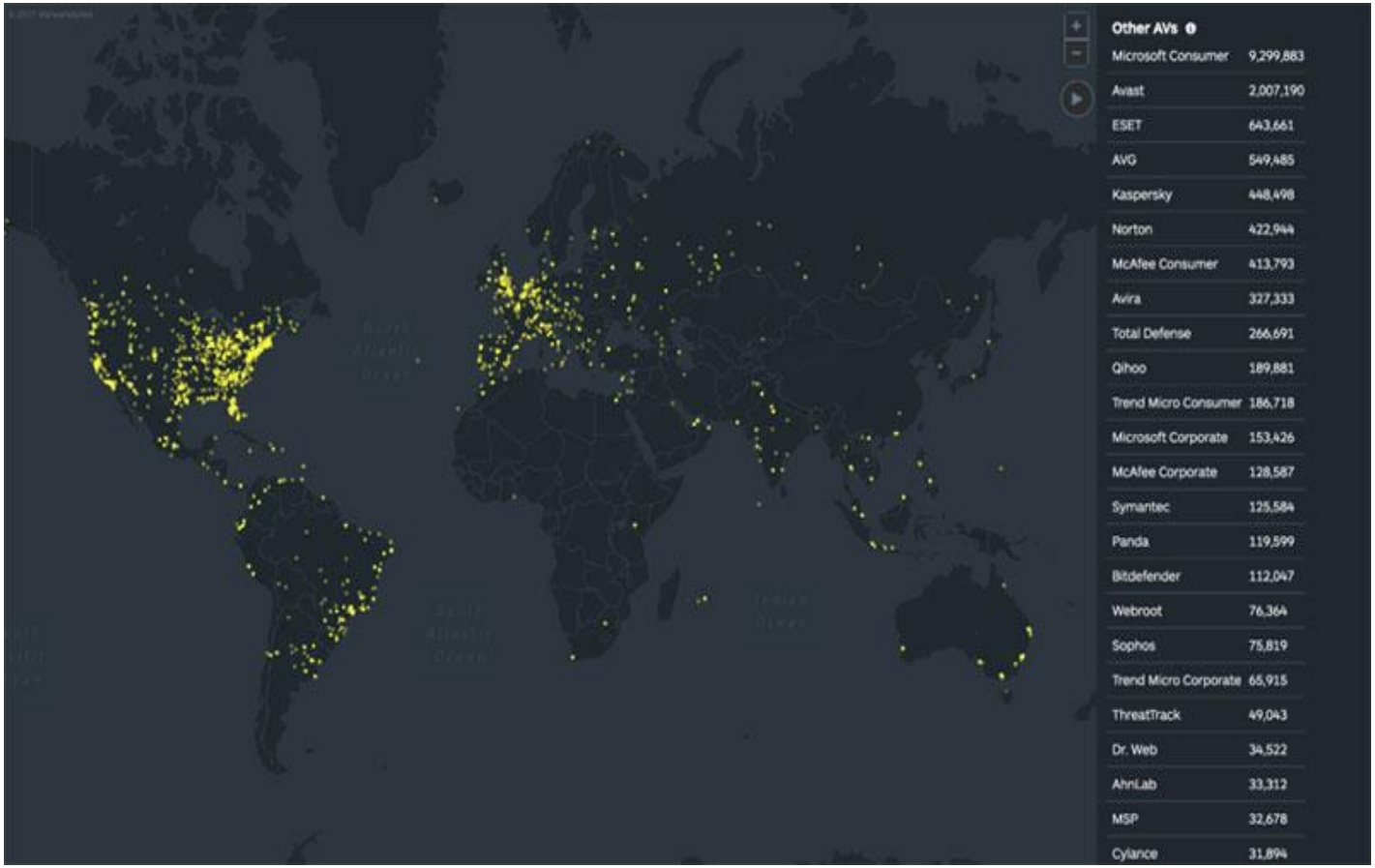
a) Skeniranje direktorija ili određenih datoteka za poznate zlonamjerne šeme koji ukazuju na prisustvo zlonamjernog softvera;
b) Dozvoljava korisnicima da rasporede skeniranje tako da se pokreću automatski;
c) Dozvoljava korisnicima da započnu nove skenere u bilo kom trenutku; i
d) Uklanjanje bilo kakvog zlonamjernog softvera koji otkrije. Neki antivirusni programi to rade automatski u pozadini, dok drugi obavještavaju korisnike o infekcijama i pitaju ih da li žele da očiste datoteke.

Kako danas radi jedan AntiVirus?



Koji je AntiVirus najbolji?

Samo u oktobru 2017, bilo je oko 4 miliona slučajeva kada je tradicionalni AV bio neefikasan protiv današnjih pretnji.



Top 5 AV proizvođača po količina malware-a koji su propustili su:

1. Avast - 2.007.190
2. ESET - 643,661
3. AVG - 549,485
4. Kaspersky - 448,498
5. Norton - 422.944

Kako se efikasno zaštiti od online opasnosti?

Sedam zlatnih pravila kako bi se sačuvali od opasnosti:

1. **Obavezno koristite AntiVirus**
2. **Obavezno koristiti dodatni nivo zaštite (AntiMalware, Firewall, etc.)**
3. **Koristite licencirane programe**
4. **Uvedite praksu principa najmanje privilegije (PoLP)**
5. **Uvijek održavajte trenutni softver i imajte praksu ažuriranja**
6. **Redovno raditi back-up važnih dokumenata i datoteka**
7. **Ne riskirajte svoje podatke!**

Kako izbjeći rizik od ugrožavanja podataka.

- Nikada ne dijelite lozinku ili lozinke.
- Koristite dva koraka (Duo)
- Prijavite se za obavještenja o stranim prijavama
- Nemojte kliknuti na slučajne veze
- Pazite na e-poštu ili priloge od nepoznatih ljudi
- Ne skidajte nepoznat softver sa Interneta
- Nemojte propagirati viruse ili lanac pošte
- Odjavite se ili zaključajte svoj računar
- Isključite lab / test računare
- Uklonite nepotrebne programe ili usluge
- Ostavite udaljeni pristup
- Veoma pažljivo tretirajte osjetljive podatke
- Bezbjedno uklonite podatke
- Osiguranje kućne mreže
- Izbjegavajte stranice sumnjivog sadržaja

Kreiranje bezbjednog online okruženja

Cyberbuiling kao najaktulniji problem maloljetničke delikvencije se može uveliko suzbiti adekvatnim obrazovanjem ili edukacijom o tome kako koristiti današnju tehnologiju u bezbjednom okruženju.

„Nekada je djecu odgajala mahala, a danas se to radi preko Facebook-a“
(Prosvjetna radnica)

Edukovanje o potencijalnim opasnostima

Edukujte sebe, roditelje i djecu da

- virtualan (online) svijet, nije ništa različitiji od onog stvarnog.
- ne daju lične informacije na internetu, chat-u, blog-u ili web stranica.
- da budu pažljivi kome daju svoj broj mobitela.
- da nikome, osim roditeljima ne govore svoju šifru, čak ni prijateljima.
- ako dobiju poruku s nepoznatog broja, da ne odgovaraju.
- ne trebaju odgovarati ni na poznate brojeve ako se zbog sadržaja poruke osjećaju loše ili neugodno.
- da ne otvaraju e-mailove koje im šalje neko koga ne poznaju
- se nasilje ne prikriva i da treba da odmah obavijeste odrasle.
- da se na internetu se poštuju pravila ponašanja kao i u svakodnevnom životu.
- da sve što vrijedi za čuvanje njihovih podataka, vrijedi i za čuvanje tuđih.

Hvala Vam na pažnji.

Pitanja?