SVEUČILIŠTE U SPLITU  
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

SEMINARSKI RAD

RAČUNALNI VIRUSI

Duje Glavina

Split, srpanj, 2023.

**SADRŽAJ**

[1 UVOD 1](#_Toc139224536)

[2 RAČUNALNI VIRUSI 2](#_Toc139224537)

[2.1 Rutine 2](#_Toc139224538)

[2.2 Pojmovi 3](#_Toc139224539)

[2.3 Povijest 4](#_Toc139224540)

[3 POZNATI SLUČAJEVI VIRUSA 5](#_Toc139224541)

[3.1 Michelangelo 5](#_Toc139224542)

[3.2 I LOVE YOU 5](#_Toc139224543)

[3.3 WannaCry 6](#_Toc139224544)

[4 ZAŠTITA 10](#_Toc139224545)

[5 ZAKLJUČAK 11](#_Toc139224546)

[LITERATURA 12](#_Toc139224547)

[SAŽETAK I KLJUČNE RIJEČI 13](#_Toc139224548)

# UVOD

Računalni virusi predstavljaju jednu vrlo zanimljivu vrstu software-a koja se pojavila   
1970-tih.

U radu ćemo istražiti različite vrste računalnih virusa, mehanizme njihovog širenja, posljedice koje mogu imati na uređaje i pojedince, te mjere koje se mogu poduzeti za zaštitu od ovih prijetnji.

Rad se sastoji iz tri djela. Prvi dio objašnjava što su računalni virusi, njihovu klasifikaciju i kratku povijest područja. Drugi dio rada bavi se primjerima poznatih virusa. Treći dio govori o metodama zaštite od računalnih virusa.

# RAČUNALNI VIRUSI

Najčešća definicija koju ćete dobiti ako pitate nekoga što je to računalni virus je nešto kao „Maliciozni software“. Iako postoji signifikantno preklapanje između virusa i malicioznog software-a to nije prava definicija. Računalni virus je računalni program koji ima sposobnost preuzeti kontrolu nad računalom i stvoriti svoje funkcionalne kopije, tj. reproducirati se.

Prava tehnička definicija za ono što mi smatramo virusom bila bi SRA „self reproducing automata“, odnosno samoreplicirajući automat.

Kako sama reprodukcija ne mora biti maliciozna, program ne mora biti maliciozan da bi se klasificirao kao SRA. Doduše nekada replikacija može biti vrlo intenzivna i značajno remetiti rad računala. Također valja razlikovati SRA od „virusa“ koji se ne repliciraju pa prema tome tehnički nisu SRA. U daljnjem tekstu virus će se referirati na maliciozni SRA.

## Rutine

Svaki virus bi trebao imati dvije osnovne rutine, traženje i kopiranje.

Traženje locira nove direktorije ili dijelove diska koje virus može zaraziti. Ono sadržava sve detalje o načinu širenja virusa i odlučuje koliko se virus brzo širi. Ako je rutina traženja dobra ona omogućuje brzo širenje virusa. Pre kompleksna rutina širenja povećava veličinu virusa i olakšava detekciju.

Druga rutina, kopiranje, treba moći kopirati virus u područje koje je dano rutinom traženje. Njena veličina ovisi o tome koju vrstu datoteke kopira.

Te dvije rutine su sve što virus treba imati da bi se mogao smatrati SRA. Osim tih rutina virusi često sadrže dodatne rutine.

Među njima su najčešće rutine za izbjegavanje detekcije, bilo od strane antivirusa ili korisnika. Osim njih virusi mogu imati različite rutine šaljive naravi koje su ustvari velika mana virusa jer olakšavaju detekciju i uklanjanje istoga.

A diagram of a virus

Description automatically generated with medium confidence

Slika ‑ Rutine Virusa[1]

A screen shot of a computer program

Description automatically generated with low confidence

Slika 2‑2 „virus“

## Pojmovi

Termini korišteni u daljnjem tekstu:

* File Infectors – ovi virusi inficiraju izvršne datoteke kao što su .com ili .exe datoteke, šire se izvršavanjem tih datoteka.
* Makro virusi – inficiraju datoteke koje sadrže makroe, doc, sheets,… Iskorištavaju makro podršku u MS Officeu
* Boot Sektor Virusi – virusi koji ciljaju boot sektor uređaja. Izvršavaju se prilikom pokretanja sustava
* \*Multipartite\* virusi – istovremeno mogu inficirati i datoteke i boot sektor
* Polimorfni virusi – imaju sposobnost mijenjanja svojega koda svaki puta kada se repliciraju, na taj način otežavaju antivirusnom softveru da ih otkrije
* Crvi – Samoreplicirajući programi koji se šire putem računalnih mreža, ne zahtijevaju host datoteku za širenje
* Trojanci – Programi koji se maskiraju kao legitimni softver a sadrže malware
* Ransomware – vrsta malvera koja enkriptira datoteke na računalu i od žrtve traži otkupninu za ključ

## Povijest

Prvi akademski rad na temu SRA objavio je John von Neumann 1948. godine, bio je to esej „Theory of self-reproducing automata“ u kojem opisuje kako se računalni program reproducira.

1971. godine pojavio se prvi računalni crv Creeper kojeg je napisao Bob Thomas. Zadaća mu je bila micati se po mainframe računalima koristeći ARPANET. Kasnije je Ray Tomlinson (email) preradio taj program da se kopira umjesto da se pomiče. Cijela zadaća programa bila je da ispisuje: „I'M THE CREEPER : CATCH ME IF YOU CAN“. Kasnije je Tomlinson napisao Reaper koji je bio prvi antivirusni softver. Uloga mu je bila brisanje Creepera pomičući se po ARPANET-u.

Prvi boot sektor virus Brain 1986. godine na IBM ovim osobnim računalima.

Morris crv 1988. godine je bio jedan od prvih crva distribuiranih putem interneta i prvi koji je dobio medijsku pozornost. Morris tada student na diplomskim studijima na Cornellu napisao je crva i pustio ga na mrežu MIT-a, da prikrije svoje stvarno mjesto studiranja. Kasnije je rekao da je crv napisan da ukaže na sigurnosne propuste u mrežama tog doba. Zbog Morrisove pogreške u kodu za repliciranje crv bi više puta inficirao isto računalo i sa svakom novom iteracijom sve ga više i više usporavao. Efektivno crv je radio uspješan DOS napad. Prava šteta koju je crv napravio se ne zna, ali se procjenjuje da je bila između milijun i deset milijuna dolara. Morris je postao prva osoba u SAD-u osuđena za računalnu zlouporabu. Kasnije je postao profesor na MIT-u.

1989. godine Ghostball, prvi multipartitni virus. Inficirao je .COM datoteke i boot sektor MS-DOS systema.

A picture containing text, screenshot

Description automatically generated

Slika 2‑3 Enkriptiranje datoteka oko fajla

# POZNATI SLUČAJEVI VIRUSA

## Michelangelo

Boot sektor virus Michelangelo imao je zanimljivu priču u veljači 1992, iako je primijećen godinu dana ranije. Napravljen je tako da inficira master boot record tvrdog diska i svakog floppy diska ubačenog u računalo (s kojim se dalje širi). Većinu godine ne radi ništa ali se aktivira 6. ožujka svake godine, na rođendan slavnog umjetnika (po kojem je dobio ime) i prebriše prvih 100 sektora tvrdog diska samo s nulama.

Kako je virus otkriven mjesec dana prije aktivacije, a nije se znalo koliko računala je zaraženo nastale je panika predvođena medijima i „stručnjacima“. John McAffee je tvrdio da su zaraženi milijuni računala (tada je još bio na čelu svoje kompanije koja je imala prvi komercijalno dostupni antivirus Virus Scan). Kada je došao taj 6. ožujka 1992 ispostavilo se da je zaraženo samo desetak tisuća računala. Narednih godina različiti mediji su sugerirali da ne palite računalo 6. ožujka ili da promijenite datum, ali to je bilo to.

## I LOVE YOU

Bio je crv koji je 2000. godine zarazio deset milijuna računala ili 20 milijardi USD štete i ušao u Guinessovu knjigu rekorda kao najvirulentniji računalni virus svih vremena.

Ime dolazi od toga što se širio emailom koji bi primili od nekoga s kim ste prethodno razmjenjivali mailove na MS Outlooku naslovljen sa „ILOVEYOU“.

Najviše su bili pogođeni korisnici tada novoga Windowsa 2000 koji je došao sa novom značajkom koja je bila da po defaultu ne prikazuje ekstenzije datoteka. Za prikaz ekstenzija korisnici su morali tu opciju uključiti ručno.

Mail je dolazio sa sljedećom porukom: „kindly check the attacked LOVELETTER comming from me“ i datotekom „LOVE-LETTER-FOR-YOU.TXT.vbs“. Kada bi prosječan korisnik skinuo datoteku na računalo samo je vidio „LOVE-LETTER-FOR-YOU.TXT“ što bi ga navelo da misli da se radi o tekstualnoj datoteci.

Kad se taj visual basic skripta pokrene napravi više kopija same sebe, neke budu skrivene a neke zamjene mp3, jpg, i druge skripte. Napravi izmjene na registry key-evima. Konačno, pošalje email svim žrtvinim kontaktima.

## WannaCry

Napad WannaCry (skraćenica za WannaCryptOr 2.0) kriptocrv dogodio se 12 svibnja 2017. godine. Ransomwareom je bilo pogođeno više od dvjesto tisuća računala u više od sto pedeset zemalja.

Na početku napada smatralo se da se WannaCry širio phishing napadom što nije bilo točno.

Ransomware nakon inficiranja računala enkriptira određene datoteke na računalu, onda od žrtve traži novac za dekripcijski ključ. Žrtve WannaCry-a bi otkrile da su im sve bitne datoteke enrkiptirane i dočekao bi ih ovaj wallpaper:

A screenshot of a computer error

Description automatically generated with low confidence

Slika 3‑ WannaCry Wallpaper [2]

Žrtva bi dobila i „ Wana Decrypt0r 2.0“ koji je imao upute kako mogu dobiti ključ za dekriptirati podatke nakon uplaćivanja 300 USD u bitcoinu.



Slika 3‑ Ransomware [32]

Za objasniti kako se širio moramo spomenuti jednu priču.

Mnoge državne agencije angažiraju grupe skupine da za njih odrađuju napade na druge države. Jedna od takvih grupa je i Equation group [3] (ime dobili zbog ekstenzivne uporabe enkripcije) koja ima navodne veze sa NSA (Nacionalna Sigurnosna Agencija – SAD).

U kolovozu 2016. godine Equation grupu su hakirala grupa Shadow Brokers [4] (ime vam je vjerojatno poznato ako ste igrali Mass Effect). Ukradeni su razni alati koji je NSA imala na raspolaganju. Alate nastale tako što je NSA je detektirala razne propuste u Windows operacijskim sustavima i pronašla efikasne načine njihovog iskorištavanja.

Naravno propuste nisu prijavili Microsoftu, već su ih koristili kao oružje u napadima na države i druge. Shadow Brokeri su počeli prodavati te alate na webu na aukcijama.

Naravno NSA je demantirala da oni posjeduju bilo kakve ilegalne alate, pa su mnogi bili skeptični prema tim početnim aukcijama. Aukcije su propale pa su malo po malo davali razne alate besplatno. Posebno su zanimljivi DoublePulsar [6] i EternalBlue [5].

Windows je koristio SMB (Server Message Block) komunikacijski protokol, razvijen 80' ih za komunikaciju na LAN-u. Starija verzija tog protokola je imala propust koji je omogućavao remote code execution na računalu žrtve. EternalBlue je iskorištavao taj propust. Hakeri su koristili EternalBlue za instaliranje DoublePulsara za stvaranje backdoor-a. Koristeći taj backdoor u računala je ubacivan ransomware WannaCry.

Nakon infekcije WannaCry se pokuša spojiti na sljedeću domenu: „iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com“ koja nije bila registrirana. Ako ne uspije ostvariti vezu onda skenira port 445 (port za SMB) i ako je taj otvoren propagira se po mreži i enkriptira datoteke.

Microsoft je znao za propust u SMB-u mjesec dana prije napada, i objavili su zakrpu koja je ispravila propust. Problem je nastao sa starijim operativnim sistemima (xp) koji više nisu bili podržani, računalima sa isključenim automatskim skidanjem zakrpa i piratiziranim kopijama.

Tada 23. godišnji istraživač Marcus Hutchins analizirao je malware u virtualnom okruženju i otkrio da se pokušava spojiti na prije spomenutu domenu. Kupio je tu domenu i zaustavio propagaciju virusa. Pristupanje domeni bio kill switch, vjerojatno ugrađen da bi se virus teže analiziralo u sandbox okruženjima. Iz nekoga razloga virus nije koristio slučajno izabranu domenu nego uvijek statično gore spomenutu. Par sati kasnije počeli su DDOS napadi na stranicu koji su na kraju bili neuspješni.

Na kraju je WannaCry zarazio oko 230.000 računala. Od kojih je više od pola bilo u Rusiji, također dosta su bile pogođene Indija i Ukrajina. Najveća pojedinačna žrtva bio je NHS (National Health Service) Britanska zdravstvena služba sa 70.000 zaraženih računala, magnetskih rezonanci i druge dijagnostičke opreme. NHS je napad koštao oko 92 milijuna eura, a globalno oko 8 milijardi dolara.

Na kraju su 98% žrtava bili korisnici koji su koristili Windows 7 bez potrebnih zakrpa, a samo 0.1% su bili korisnici Windows xp operacijskog sustava. Microsoft je poslije izbacio zakrpu i za sustave koji više nisu imali podršku.

# ZAŠTITA

Lako je uočljivo da ja najčešći razlog zaraze računalnim virusom korisnik koji neadekvatno rukuje sa svojim računalom. Kako bi spriječili infekciju vašeg računala računalnim virusom virusa, važno je slijediti sljedeće:

* Držite svoj softver ažuriranim: Redovito ažurirajte svoj operativni sustav, web preglednike i ostali softver kako biste osigurali da imate najnovije sigurnosne zakrpe i ispravke pogrešaka. Omogućite automatska ažuriranja kad god je to moguće.
* Koristite pouzdani antivirusni softver: Instalirajte pouzdan antivirusni program. Njega također redovito ažurirajte, te provodite redovna skeniranja.
* Budite oprezni s privicima e-pošte i preuzimanjima: Koristite softver za skeniranje pošte i budite izrazito oprezni sa poštom pristiglom od nepoznatih izvora. Ne otvarajte nikakve sumnjive linkove pristigle emailom.

# ZAKLJUČAK

Iako prolaskom vremena virusi predstavljaju sve manje značajnu prijetnju našim računalima, oni ipak nisu zanemarivi. Korisnik treba razumjeti da način na koji rukuje s računalom najviše utječe na vjerojatnost da to računalo bude inficirano virusom.

Važno je držati se dobrih praksi za zaštitu računala kao što su redovito ažuriranje softvera, korištenje anti virusa i oprezno korištenje interneta.

Puno je lakše prevenirati infekciju računalnim virusom nego spašavati podatke i uklanjati virus.

LITERATURA

1. Mark A. Ludwig (1991*) The Little Black Book of Computer Viruses: The Basic Technology*, ISBN-13: 978-0929408026
2. Wikipedia, *WannaCry,* s Interneta  
   https://en.wikipedia.org/wiki/WannaCry\_ransomware\_attack zadnji pristup: 2.7.2023.
3. Wikipedia, *Equation Group,* s Interneta  
   https://en.wikipedia.org/wiki/Equation\_Group zadnji pristup: 2.7.2023.
4. Wikipedia, *The Shadow Brokers,* s Interneta  
   https://en.wikipedia.org/wiki/The\_Shadow\_Brokers zadnji pristup: 2.7.2023.
5. Wikipedia, *EternalBlue,* s Interneta  
   https://en.wikipedia.org/wiki/EternalBlue zadnji pristup: 2.7.2023.
6. Wikipedia, *Double Pulsar,* s Interneta  
   https://en.wikipedia.org/wiki/DoublePulsarzadnji pristup: 2.7.2023.

SAŽETAK I KLJUČNE RIJEČI

**Sažetak**

*Tema ovog seminarskog rada je dati uvod u računalne viruse. Rad objašnjava funkcionalne dijelove virusa, a potom daje primjere različitih virusa u zadnjih 30 godina. Objašnjava računalne viruse kao što su Michelangelo, ILOVEYOU i na kraju WannaCry napad koji se dogodio 2017. godine. Na kraju daje preporuke za zaštitu korisnika.*

**Ključne riječi**

*Računalni virusi, malware, ransomware, Michelangelo, ILOVEYOU, WannaCry*