

**Софийски университет „Св. Кл. Охридски”**

Факултет по математика и информатика

специалност : „Защита на информацията в компютърните системи и мрежи“

**Дисциплина : Злонамерен софтуер(Malware)**

**Курсова работа на тема Rootkit**

*Автор:*

Иван Ивов Чучулски, фак. номер: 4MI3400043

*Ръководител:*

доц. д-р Димитрина Полимирова

зимен семестър, 2021/2022г.

Съдържание

[1. Въведение 2](#_Toc94697411)

[2. Какво представлява rootkit 2](#_Toc94697412)

[2.1 Дефиниция за rootkit 2](#_Toc94697413)

[2.2 История на rootkit 2](#_Toc94697414)

[2.3 Актуалност на проблема 2](#_Toc94697415)

[3. Използвана литература 2](#_Toc94697416)

# Въведение

Целта на този проект е да опишем какво представлява rootkit, каква заплаха представлява за нашите системи и по какъв начин може да се заразим с такъв злонамерен софтуер. Ще обърнем внимание на практики, чрез които можем да се предпазим и ще предложим инструменти, с помощта на които да премахнем rootkit от заразен компютър.

# Какво представлява rootkit

## Дефиниция за rootkit

Rootkit представлява съвкупност от софтуерни инструменти, които имат за цел да предоставят на атакуващия различно ниво на достъп в дадена система. Обикновено целта е да се предостави отдалечен и неоторизиран достъп до системата на жертвата, което да позволява подслушване, кражба или изтриване на данни, отдалечено изпълнение на код и контролиране на машината с цел осъществяване на други атаки. Произходът на термина rootkit можем да свържем с профила на администратора на една Linux система, а именно root потребителя.

Особеността на този вид злонамерен софтуер е, че след успешно осъществена атака, rootkit процесите се изпълняват незабелязано от обикновения потребител на системата и той няма възможност да разбере за тяхното наличие. В допълнение на това rootkit може да остане скрит и за много от стандартните проверки на антивирусните програми, поради факта че неговият код е може да бъде вмъкнат в най-ниските нива на абстракция на софтуерната система – ядрото на операционната система, частта за зареждане на операционната система, bootloader и във firmware, който най-често се съхранява в ROM паметта.

Това прави отстраняването на такъв вид програми значително по-трудно, защото са необходими по-специфични инструменти, които да могат да сканират и модифицират тези части от паметта, където се съхраняват bootloader и firmware.

Интересно е, че има примери за rootkit, които са умишлено инсталирани от някой хардуерен производител или вървят заедно с някакъв софтуерен продукт и не целят да причиняват щети на клиентския компютър. Примери за това са различни софтуери за засичане на помощни средства към игри, например Valve Anti-cheat, а друга възможност са crack/patch при пиратски софтуер, който позволява инсталиране и използване на софтуер без закупуване на лиценз.

## История на rootkit

Rootkit за първи път се появява в началото на 90-те години на 20-ти век като първите опити са били насочени срещу Unix базирани системи. Преди това са съществували компютърни вируси, които са имали подобно поведение на rootkit, тъй като са се опитвали да скрият свое копие в секторите за начално стартиране на твърдите дискове. Примери за такива вируси са Brain и Stoned.

Един от първите rootkit е NTRootkit, създаден в края на 90-те от изследователя по сигурност Greg Hoglund специфично за операционната система Windows NT. Той има за цел да докаже възможността за създаване и успешна работа на подобен тип злонамерен софтуер и публикува своя резултат в онлайн списание.

## Актуалност на проблема

Тенденциите са атаките с rootkit да стават все по-комплексни

# Видове rootkit

# Как работи rootkit

# Как да се справим с rootkit

# Заключение

# Използвана литература