

**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](#_Toc94730626)

[2. Какво представлява rootkit 2](#_Toc94730627)

[2.1 Дефиниция за rootkit 2](#_Toc94730628)

[2.2 История на rootkit 3](#_Toc94730629)

[3. Видове rootkit 4](#_Toc94730630)

[4. Как работи rootkit 4](#_Toc94730631)

[5. Как да се справим с rootkit 4](#_Toc94730632)

[6. Заключение 4](#_Toc94730633)

[7. Използвана литература 4](#_Toc94730634)

# 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

Първите опити за създаване на програма, която за позволява неоторизиран достъп до администраторски правомощия са в началото на 90-те години на 20-ти век, като са били главо насочени срещу Unix базирани системи. Появилите се компютърни вируси от 80-те са имали другия елемент от поведението на rootkit, а именно характеристиката да се опитат да скрият свое копие в секторите за начално стартиране на твърдите дискове. Примери за такива вируси са Brain и Stoned. Техниките, които използват тези вируси са използвани по-късно за създаването на първите rootkit инструменти, които обаче имали за цел Windows базирани системи.

Един от първите популярни rootkit софтуери е “NTRootkit”, който е създаден в края на 90-те от изследователя по сигурност Greg Hoglund за операционната система Windows NT. Той има за цел да докаже възможността за създаване, внедряване и успешна работа на подобен тип злонамерен софтуер, който се изпълнява на нивото на ядрото на операционната система. Последва бавно, но сигурно създаване на rootkit, даващи все повече контрол и възможност за злонамерени действия на атакуващия. По-известни са “he4hook”, създаден през 2000г., “HackerDefender” от 2002г. и “Vanquish” от 2003г. Те имат възможността да премахнат видимостта на определени файлове и да четат стойностите на регистрите на операционната система.

След това се появяват инструменти като “Haxdoor” и “FU”, които след успешно инсталиране имат възможност да прикрият дейността си, чрез скриване на процесите си и могат да предоставят отдалечен административен достъп до системата(backdoor). След появата на тези инструменти започва голямо нарастване на бройката на rootkit програмите, като най-често те представляват модифициран вариант на вече споменатите “HackerDefender”, “Haxdoor” и “FU”. Започва вграждането на rootkit в други злонамерени програми, като троянски коне и mass-mail червеи, които се използват като посредник за успешното инсталиране на програмата rootkit. Известни представители са на троянския кон е “Goldun” и вариантите на червея “Bagle”.

През 2009 е създаден “Machiavelli“, който е първия rootkit за операционната система Mac OS. Други известни атаки с rootkit, които са предизвикали кражба на данни и включване на инфектираните компютри в botnet са “ZeroAccess” открит през 2011 и “Necurs” през 2012.

С нарастването на броя на успешните атаки с rootkit производителите на антивирусен софтуер започват да имплементират методи за откриване на вредителските програми в своите продукти. Появяват се и инструменти от независими автори, които имат единствена цел за открият и премахнат rootkit програми.

Атаките с rootkit продължават да представляват сериозна заплаха за потребителите и днес. Откриват се примери за rootkit, които се възползват от уязвимости на технологиите за стартиране UEFI или от някои функционалности на Windows 10, като например Windows Platform Binary Table, която позволява на производителите на хардуер да включат цифрово подписани изпълними програми във firmware-а на машината.

# Видове rootkit

# Как работи rootkit

# Как да се справим с rootkit

# Заключение

# Използвана литература