
**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 – характеристики, предпазване и отстраняване”

*Автор:*

Иван Ивов Чучулски, фак. номер: 4MI3400043

*Ръководител:*

доц. д-р Димитрина Полимирова

зимен семестър, 2021/2022г.

# Съдържание

# 1. Въведение

Целта на този проект е да опишем какво представляват rootkit програмите, каква заплаха са те 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.

# 2. Какво представлява rootkit

## 2.1 Дефиниция за rootkit

Rootkit представлява съвкупност от софтуерни програми, които имат за цел да предоставят на атакуващия привилегировано ниво на достъп в дадена система. Обикновено целта е да се предостави постоянен, отдалечен и неоторизиран достъп до системата на жертвата, който 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, root потребителя, както и характеристиката тези програми да са съставени от множество компоненти, които работят заедно.

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 от обикновените антивирусни програми почти значително по-трудно, защото са необходими по-специфични инструменти, които да могат да сканират и тези части от паметта, където се съхраняват bootloader и firmware.

Интересно е, че има примери за програми наподобяващи rootkit, които са умишлено инсталирани от производителя на хардуера, вървят заедно с някакъв софтуерен продукт или дори потребителя сам инсталира и не целят да причиняват щети на клиентския компютър. Примери за това са различни

софтуери за засичане на помощни средства към игри или т.нар. “crack” програми при пиратски софтуер, който позволява инсталиране и използване на софтуер без закупуване на лиценз.

### 2.2 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 вече имали за цел набиращата популярност операционна система за настолни компютри Windows.

Един от първите популярни rootkit софтуери е “NTRootkit”, който е създаден в края на 90-те от изследователя по сигурност Greg Hoglund за 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.

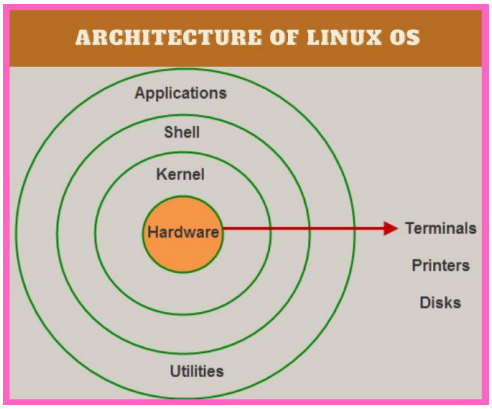
След това се появяват инструменти като “Haxdoor” и “FU”, които след успешно инсталиране имат възможност да прикрият дейността си, чрез скриване на процесите си и могат да предоставят отдалечен административен достъп до системата(backdoor). След появата на тези инструменти започва голямо нарастване на 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 използвани представители са троянския кон е “Goldun” и вариантите на червея “Bagle”.

През 2009 е създаден “Machiavelli“, който е първия rootkit за операционната система Mac OS. Той също е бил създаден от изследователи по сигурността. 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.

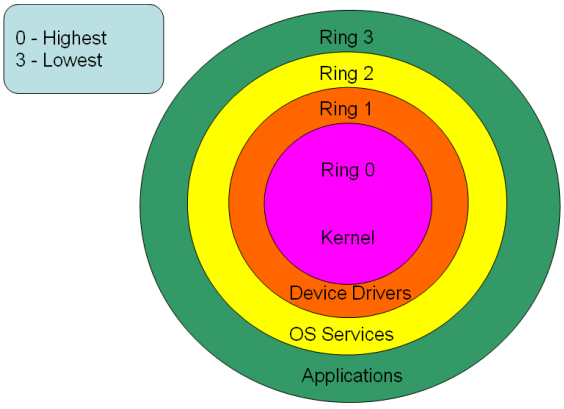
С нарастването на броя на успешните атаки с rootkit производителите на антивирусен софтуер започват да имплементират методи за откриване на вредителските програми в своите продукти. Появяват се и инструменти от независими автори, които са били насочени единствено, за да открият и премахнат rootkit програми.

## 3. Слоеве на привилегированост

Преди да разгледаме различните типове rootkit софтуер е необходимо да разгледаме различните нива(слоеве, пръстени) на привилегированост за изпълнимите процеси в съвременните операционни системи. Под привилегированост разбираме възможността за директен контрол и модификация на системните ресурси като памет и входно-изходни устройства.




*Фигура 1. Архитектура на ОС Линукс*




*Фигура 2 Слоеве на привилегированост*

Слоевете, които се засягат от rootkit можем да определим следните нива в нарастващ ред спрямо тяхната привилегия и възможност за контрол над системата:

- слой на приложенията(application/user space)
- слой на системните драйвери и слой на ядрото на операционната система((device drivers/kernel space)
- виртуализационен слой(hypervisor),

- слой на firmware и hardware

С така дефинираните слоеве можем да направим класификация на rootkit софтуер, спрямо в кой слой те се съхраняват и изпълняват.

## 4. Rootkit в слоя на приложенията

Тези програми се изпълняват по същия начин като програмите, които крайният потребител ползва, като уеб браузър, музикален плейър или текстов редактор. Обикновено rootkit програмата се инсталира на компютъра на жертвата посредством друг тип злонамерена програма, наречена dropper(програма-носител), която носи в себе си инсталатора на rootkit или негов архивиран и компресиран вариант. Потребителите изтеглят dropper софтуера като най-често това се случва при отваряне на прикачени файлове към писма или изпълнение на програми от неопределен източник.

След като успешно са стартирани на машината на жертвата се инсталира rootkit програмата и носителят автоматично се премахва. Съществува и вариант, при който той се копира в скрит файл или в някой регистър на операционната система като по този начин дори след премахване на rootkit компонента и рестарт на машината съществува възможност в по-късен момент носителя отново може да се изпълни. Кодът на rootkit програмата може да бъде записан по същия начин в скрит от потребителя файл на твърдия диск и при всяко стартиране на компютъра той да бъде стартиран автоматично.

Начинът на работа на този тип rootkit програми в случая на Windows операционна система е те да се прикрепят към някоя легитимна програма чрез зареждане на .dll файл в процеса на програмата чрез т.нар. „закачане“, още “hooking” механизъм, например при ОС Windows изпълнявайки функцията “SetWindowsHookEx”. След като това е се изпълни успешно .dll кодът има достъп до интерфейса на програмата  и може да го използва за засичане действията на потребителя при изпълнението ѝ. Друг възможен сценарий е rootkit програмата да намери системен .dll файл, към който се обръща легитимната програма и да промени неговия интерфейс, така че извикването да се обръща към rootkit програмата.

Поведението на програмата остава непроменено за потребителя и той не разбира, че всъщност неговите действия се записват. Съвременните антивирусни

програми могат да засекат такива намеси в адресното пространство на изпълнимите програми, както и да разпознаят процесите на rootkit програмата и да блокират неговото изпълнение.

Атаки с този тип rootkit са осъществявани най-често срещу банков, като целта е откradване на чувствителни данни като потребителски имена, пароли или номер на банкова сметка. Пример за такъв злонамерен софтуер е “Carberp”, който е имал за цел приложения за онлайн банкиране на руски и украински банки. Той е модифицирал байткода на Java приложението за онлайн банкиране “BIFIT iBank 2”, като за целта използва безплатен инструмент с отворен код “Java Programming Assist”. Идеята е, че са подменени модулите, които се грижат за осъществяване на транзакции и пренасочват транзакциите към техни сметки.

## 5. Rootkit в слоя на системните драйвери и ядрото

Rootkit програми от този тип представляват значително по-голяма заплаха за потребителите, тъй като процесите, които се изпълняват на ниво системен драйвер и ядро на ОС имат пълни права за достъп до всички файлове на системата, до данните на всички останали процеси в приложния слой и контролират техния достъп до хардуера на компютъра. Ядрата на съвременните операционни системи като Windows и Linux са монолитни по архитектура, но позволяват динамично зареждане и премахване на модули, които се изпълняват със същото ниво на достъп като самото ядро. Възможни приложения на тази функционалност е разпознаване на ново хардуерно устройство без нужда от рестарт на ОС, чрез зареждане на неговия драйвер в този слой или възможност за добавяне на нова функционалност на самото ядро, като поддръжка на нови файлови системи и оправяне на бъгове.

Начините за заразяване с такъв тип rootkit програми са използване на открити уязвимости на системата, които позволяват атака от тип „превишаване на правомощията“, за да се извърши инсталирането. Друга възможност е да се използва междинна програма, която има за цел да накара потребителя да я изпълни и тя от своя страна инсталира rootkit-а. Това може да са програми троянски коне, които например имитират легитимни програми за поправяне на грешки и обновяване на драйверите на системата или дори антивирусен софтуер, което кара потребителя да им се довери напълно. Самото пренасяне на кода на rootkit в слоя на ядрото е сложен за създаване процес и обикновено изисква

наличието на софтуерни грешки, които пораждат уязвимости за избраната операционна система. Поради високата сложност съществува по-голям шанс да възникнат грешки и добър антивирусен софтуер да засече опита за атака. Това е непрестанна борба между хакерите и производителите на антивирусен софтуер.

Успешно инсталиран rootkit в слоя на ядрото и системните драйвери има повече и по-мощни похвати за осъществяване на злонамерени действия. При операционните системи с монолитни ядра, като Windows, Linux и Mac OS за осъществяване на всяко действие от потребителска програма, свързано с достъп до ресурсите на системата, като заделяне на памет за даден обект, отваряне на мрежов сокет или записване на данни във файл на твърдия диск, отговорността се прехвърля на едно или няколко системни извиквания, които се изпълняват в слоя ядрото на ОС. Това се случва на точно определени места, наречени gates, където се определя кое точно системно извикване ще обработи заявката на приложението. Rootkit може да манипулира тези места, като пренасочи изпълнението към свой код, като по този начин може да се получи информация за данните на извикването.

Друг начин за манипулиране на потока на изпълнение е rootkit да промени съдържанието на таблицата, в която се съхраняват указатели към адресите на системните функции на ядрото. Тази таблица в Windows се нарича “system service descriptor table”, а при Linux е “system call table”. Тъй като rootkit процеса се изпълнява на същия слой има достъп и възможност за промяна на тази памет, той може да промени някой от указателите и да пренасочи изпълнението към своя функция.

Този вид rootkit се открива значително по-трудно от другите, тъй като имайки достъп до паметта в слоя на ядрото, той може да промени съдържанието на структурите от данни, които съхраняват информация за изпълняващите се процеси. По този начин rootkit програмата може да „скрие“ своето присъствие, като просто премахне от там своя процес и всички, използвани от нея процеси за манипулация на системните извиквания. Това прави възможен сценарий, при който rootkit програма в слоя на ядрото да прикрива процесите и на друг злонамерен софтуер, който се изпълнява на приложното ниво, като keylogger или криптокопач.

Съществува вариант на този вид rootkit, който цели да промени сектора от твърдия диск на компютъра, в който се съхранява частта за зареждане на операционната система, т.нар. bootloader и съответно името на програми от този тип - “bootkit”. Те използват техники, които са вдъхновени от някои от първите популярни вируси като “Brain” и “Stoned”. Основната идея е да бъде подменен booloader софтуера на компютъра с такъв, който трябва първо да зареди код на злонамерена програма преди или заедно с ядрото на операционната система. Представител на този вариант е “TDSS”, който се появява за първи път през 2008г. и причинява множество щети като подслушване и подмяна на заявките на потребителя в уеб браузъра и включване на компютъра в botnet.

Съществуват варианти на този тип rootkit, които са се използвали за заобикаляне на нуждата от валиден лиценз на даден софтуер. Един такъв пример са т.нар. активатори за операционните системи Windows Vista, Windows 7.

В много от съвременните онлайн мултиплейър игри се включва софтуер против мамене, като при някои присъства и модул, работещ на нивото на ядрото и драйверите на операционната система. Примери за популярни такива програми са “Easy Anti-cheat”, “Punkbuster”, “Vanguard” и други. Тяхната функция е да сканират за някои специфични драйвери и програми в системата, за които производителите имат информация, че може да бъдат използвани за измама от играчите. Това е възможно, отново поради факта, че модулът на системата против мамене се стартира заедно с модулите на операционната система и може да се докладва за съмнителни събития, които се случват след като системата е заредена.

Съществуват разнопосочни мнения за безопасността на този тип софтуер, тъй като има докладвани случаи за блокирани програми за overclocking на процесора и драйвери на периферни устройства. Също така не е ясно дали програмите не използват високото си ниво на привилегированост за достъпване на потребителски файлове, записване на потребителската активност и докладване на данни без неговото съгласието. Самите програми против мамене могат да представляват цел за хакери и през 2013 софтуерът против мамене на организацията за онлайн мачове ESEA е използван за успешна атака с rootkit “Zero Access”, която е включил компютрите на потребителите в ботнет за копаене на криптовалута.

## 6. Rootkit във виртуализационния слой

Примери от този вид rootkit програми са създадени за пръв път от изследователи в областта на сигурността, които се опитват да докажат възможността за тяхното успешно реализиране и прилагане. Този вид rootkit се възползва от възможността за хардуерна виртуализация на процесорите на Intel и AMD, която се появява съответно в 2005 и 2006г. самата операционна система, която потребителят използва и е инсталирана на неговия компютър да бъде вкарана във виртуална машина, изпълнявана от hypervisor, който се контролира от rootkit програмата. По този начин се премахва нуждата от модифициране на някакви данни в ядрото или по приложните процеси, с които потребителя си взаимодейства. Успешна атака от този тип може да бъде потенциално много трудна за засичане и спиране.

Известни са два варианта, за които създателите им твърдят, че са успешно тествани върху операционната система Windows Vista. Това са “SubVirt” създаден от Microsoft съвместно с научни изследователи от университета в Мичиган през 2006г. и по-късно същата година се появява “BluePill”, разработван главно от Joanna Rutkowska, тогава част от “COSEINC”. Двете програми се различават по обстоятелствата за провеждането на атаката, тъй като при “SubVirt” е необходимо rootkit програмата да се изпълни по време на стартирането на операционната система, т.е. има bootkit част, чрез която инсталираната ОС се пуска в контролирана виртуална машина, като VMWare. При “BluePill” атаката се осъществява, когато системата е работеща и се прилагат серия от стъпки, които подготвят и активират виртуална машина, в която да преместят главната ОС. При успешна атака при “SubVirt”, хардуерът, като процесор, твърд диск, мрежова карта, звукова карта, който атакуваната ОС ще вижда, ще бъде виртуално създаден от съответния hypervisor и това би позволило по-лесно засичане. При “BluePill” продължават да се използват реалните компоненти и при успешно приложен такъв тип rootkit може да използва регистрите на процесора за дебъгване, за да прихваща данните в определени системни извиквания към ядрото на ОС във виртуалната машина и да манипулира отговорите.

Мненията за реалната приложимост на този вид rootkit са противоречиви и възникват спорове между изследователите. Аргументите против успешна атака са, че тъй като няма бъгове в самата имплементация на виртуализацията на процесорите, има и може да се разчита на техники за засичане наличието на

hypervisor и вземане на ответни мерки. Ответен аргумент е, че бъдещето е всяка система да има разрешена виртуализация и нейното активно използване ще направи много трудно засичането на определен вид злонамерен hypervisor.

Към днешна дата проекти от такъв вид изглежда да имат известно развитие отново в академичните среди, като примери за това са “Cloaker”, “CackeKit” и “rHV”, които са разработени за процесори с ARM архитектура и използват нови техники за разполагане на rootkit програмата в кеша на процесора. Авторите предлагат и методи за справяне със заплахите.

## 7. Rootkit във firmware слой

При този тип rootkit злонамерената програма цели да модифицира регионите от компютърната система, където се съхранява софтуер за взаимодействие с хардуерните компоненти, като например BIOS или UEFI. При успешно извършена атака rootkit програмата може да продължи да работи и при преинсталация на операционната система, форматиране или подмяна на твърдия диск, тъй като обикновено firmware софтуерът се съхранява в специален вид памет, която рядко бива проверявана за интегритет и изисква по-специфична процедура за промяна.

Обикновено атаките с този вид rootkit са най-трудни за успешно осъществяване, защото е нужно да се фокусират върху характеристиките на даден firmware, който варира между производителите. Следователно атаките не са толкова разпространени сред потребителски компютри и най-голям брой се разработват главно като изследователска дейност по сигурността.

Начините за осъществяване на атака преминават през няколко стъпки. Първата стъпка е същата както при другите видове rootkit и тя е да се използва dropper програма, която има за цел да подлъгва потребителя да я изпълни и да инсталира друга програма. Втората стъпка е товара на dropper програмата да достигне до нивото на ядрото и системните драйвери, тъй като единствено процеси от този слой може да достъпва системния firmware. Щетите, които този тип rootkit причинява може да са създаване на задни вратички за друг вид rootkit в нивото на ядрото, прихващане и спиране на обновявания на firmware софтуера или изтриване на всички данни в компютъра.

Един от първите свободно открити и работещи във firmware rootkit програми е “Mebroni” през 2011г. Тя използва всичко споменато досега, като в допълнение

инфектира и сектора за стартиране на твърдия диск. При анализ на програмата изследователи заключват, че тя реализира на практика концепциите за осъществяване на атаката, дефинирани от демонстративния “IceLord” rootkit, прицелвайки се в компютри, използващи конкретен модел BIOS и към конкретна група потребителски, поради факта че проверява за наличието на антивирусни програми, характерни за Китай.

Един възможен сценарий за осъществяване на атака е наличието на някаква уязвимост във firmware софтуера или в ядрото на ОС. Пример за такава уязвимост е “CVE-2016-8222”, която чрез грешка в драйвер е позволила атака към някои модели лаптопи от серията Lenovo ThinkPad, която позволява извикване на инструкции от “System Management Mode” режима на процесора, който се грижи за отправяне на инструкции към системния firmware.

Съществуват и варианти на атака, при които е нужен физически достъп за определено време до машината, за да може злонамерената програма може да бъде заредена директно от физически носител като преносим флаш диск. Пример за такава rootkit програма е “DEITYBOUNCE”, за която се е разбрало от изтекли документи на Националната агенция по сигурност на САЩ и после е дискутирана на няколко конференции за сигурност. Целта са конкретни модели на Dell сървъри с определени версии на BIOS и операционни системи Windows 2000 и XP. Изследователите предполагат, че успешно инсталира rootkit програмата би имала възможност да се намеси в стъпките на процеса по стартиране на компютъра и да включи в ядрото на операционната система злонамерен модул. Друга програма от същите изтекли документи е “JETPLOW”, която пък е насочена към firewall продукти на компанията Cisco. От тях виждаме, че програмата е предназначена за инсталиране на постоянна задна вратичка, която да сработи с друга програма, вероятно за подслушване на трафика през защитната стена.

Около 2005г. някои от най-големите производители на лаптопи Dell, Lenovo, HP, Acer са слагали в своите устройства софтуера “Computrace” на компанията “Absolute Software”, който дава на потребителите начин за откриване и заключване от разстояние в случай на кражба. Софтуерът който има модул, който се съхранява в паметта, където се намира и BIOS програмата, както и модул в слоя на ядрото на ОС, който . При евентуална кражба сигнал за кражба след стартиране на компютъра модулът в ядрото инсталира и изпълнява програма, която е видима в процесите на потребителя и осъществява комуникацията с отдалечен сървър за

предприемане на последващи действия. Изследователи по сигурността са провели инспекция на инсталатор за по-нова версия на BIOS софтуера на лаптоп от един от производителите и са успели да открият имената и системните пътища на модулите, които трябва да осъществят комуникация със сървъра, като след това правят анализ на поведението на другите части на програмата. Те заключват, че начина по който функционира тази програма е на практика същият като добре изработен firmware rootkit и повдигат въпроса, какво би се случило ако хакери успеят да подменят по някакъв начин изпълнимите файлове, за да отправят заявки към друг сървър например.

Оказва се, че такова нещо се е случило със програмата “LoJack”, който се явява наследник на “Computrace” при системи с UEFI стартиращ софтуер. “LoJack” се предлага отново от “Absolute Software” изпълнява същата функция и работи на подобен принцип, както и предшественика си. През 2018г. изследователи от ESET разкриват, че в някои от атаките на руска хакерска група “Fancy Bear” е използвана модифицирана версия на продукта на “Computrace”. Злонамерения софтуер наречен “LoJax” използва без промяна модула в UEFI firmware и модула в ядрото, за да се заобиколи изискването в Windows 10 всички драйвери в слоя на ядрото да имат валиден цифров сертификат, одобрен от Microsoft. Променени модулите, които трябва да отправят заявки към сървъра за действия при кражба, като хакерите са намерили начин да променят URL адреса към свои сървъри и да изтеглят друг злонамерен софтуер.

## 8. Как да се предпазваме от заразяване с rootkit

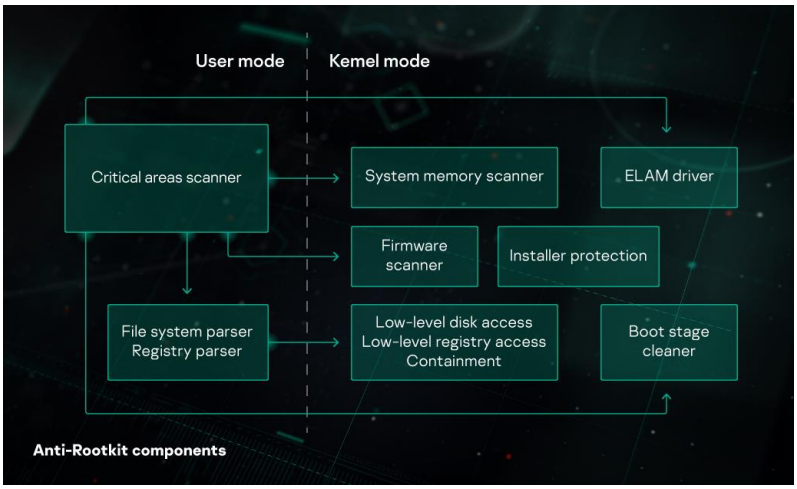
На първо място както при всички други malware програми е нужно да се обърне внимание на потребителите. Все по-широката употреба на компютърни системи, расте и броят на потребителите, които не са технически грамотните са най-честата цел на хакерите. Нещата, които трябва да станат навик на всеки потребител са да не се теглят и отварят прикачени файлове от имейли с непознат подател, да не се последват съмнителни линкове към уеб страници и тегленето на софтуер на софтуер да става единствено и само от официалните сайтове на производителите или от предназначените за това приложения при смартфоните. По този начин до голяма степен трябва да бъде премахната възможността за инсталиране на програма, която всъщност е троянски кон и цели да причини щети на системата.

С оглед на това, че във всеки софтуер може да има уязвимости, които хакерите да използват за осъществяване на атака, то е необходимо потребителите редовно да обновяват версиите на операционната си система и приложенията, които използват, както и за използват антивирусен софтуер. Трябва да се обмисли и идеята за инвестиция в допълнителни външни носители, на които редовно да бъдат правени резервни копия на системата.

Препоръчително е използването на технологии, които налагат допълнителни нива на сигурност като като новият стандарт за firmware софтуер UEFI предлага опцията “Secure boot”, която изисква наличие на валиден цифров сертификат за firmware софтуера на периферните устройства, софтуера за стартиране(bootloader) и ядрото на операционната система. От края на 2016 всички следващи версии на ОС Windows 10 налагат задължителното наличие на цифров сертификат на всички системни драйвери.

## 9. Решения за откриване и отстраняване на rootkit

Софтуерни решения, които засичат и премахват rootkit програми започват да се появяват около 2006г. Още тогава производителите на антивирусен софтуер осъзнават, че е нужно техните продукти да използват техники, подобни на rootkit, за да успяват да ги засичат. Дотогава процесите на антивирусния софтуер се изпълняват като нормален потребителски процес, но по този начин не може да се засичат заплахи, които работят на нивото на ядрото на операционната система.




*Фигура 3. Архитектура на Kaspersky Anti-Rootkit*

Промяната, която настъпва включва усложнение на антивирусните софтуери, която се състои във включване на специални модули, които се изпълняват в слоя на ядрото на ОС и по този начин им се предоставя достъп до структурите на

процесите, за да може да открият rootkit програми, които се опитват да скрият своето присъствие. Важен компонент е т.нар. ELAM (Early Launch AntiMalware) драйвер, който позволява модулът на антивирусната програма да бъде зареден от програмата за стартиране (bootloader) и да бъде функциониращ преди или заедно със стартирането на ядрото на ОС. Това позволява извършването на сканиране за rootkit програми в ранните етапи на стартиране на системата, с цел тяхното засичане преди те да предприели някакви действия за скриването си.

За справяне с rootkit във firmware и bootkit програми, антивирусните програми добавят модули, които могат да правят сканирания и на системния firmware софтуер, както и секторите от диска със стартиращите програми. Сканиранията за rootkit програми разчитат не само на сигнатури на вече известни представители, но и чрез използване на евристични методи, получени от обучението на модел с техниките на машинното самообучение. Тези технологии са в постоянен процес на развитие и е възможно да допуснат грешки, затова в повечето случаи решението какво действие да се предприеме се оставя на потребителя.

Повечето големи производители на антивирусен софтуер предлагат продукти за справяне с rootkit програми. “Kaspersky TDSS killer” е инструмент, който може да бъде изтеглен безплатно и предлага сканирания за rootkit програми в ядрото, програмата за стартиране на ОС и firmware. Програмата се предлага за голям брой от Windows операционни системи, включително и по-стари версии като 32-битови Windows XP и Windows Vista. Инструментът няма нужда от инсталиране, а се състои от един изпълним файл, който има възможност да бъде изпълнен и от конзолата. За да се осъществи сканиране по време на стартирането обаче е необходимо да се избере специална опция, която ще рестартира машината, инсталирайки нужните ELAM драйвери след което ще започне сканирането.

McAfee и AVG също имат безплатни инструменти за засичане на rootkit, като забелязахме единствено Avast да предлагат към безплатната си версия на антивирусен софтуер вградена функционалност за извършване на сканиране при стартиране. Това става от графичния интерфейс на програмата, където преди започване на стартирането има опция за изтегляне на най-новите открити дефиниции на вируси от базата данни на Avast, възможност за настройка на „чувствителността“ на сканирането спрямо неизвестни злонамерен програми и действия при намирането им.

## 10. Заключение

Заплахите от rootkit програми продължават да бъдат актуални и днес.

Атаките с rootkit продължават да се развиват и да представляват сериозна заплаха за потребителите и днес. Продължават да се измислят примери за rootkit програми, които се възползват от уязвимости в технологиите и причиняват огромни щети. За щастие производителите на операционни системи и антивирусни програми са разпознали опасността и продължават да подобряват сигурността на системите си. Необходими са повече усилия в обучението на крайните потребители за запознаване и прилагане на практики за изграждането на навици, които да не злонамерен софтуер да попадне в системите им.

## 11. Използвана литература

[1] “What Is a Rootkit and How to Remove It?”, Carly Burdova, 11.08.2021,

линк: https://www.avast.com/c-rootkit

[2] “What is Rootkit – Definition and Explanation”,

линк: https://www.kaspersky.com/resource-center/definitions/what-is-rootkit

[3] “What is a Rootkit?”, линк: https://www.fortinet.com/resources/cyberglossary/rootkit

[4] “Rootkit evolution”, Alisa Shevchenko, 28.08.2008,

линк: https://securelist.com/rootkit-evolution/36222/

[5] https://www.welivesecurity.com/2013/03/25/carberp-the-never-ending-story/

[6]https://web.archive.org/web/20101214100124/http://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf

[7] https://levvvel.com/what-is-kernel-level-anti-cheat-software/

[8] https://levvvel.com/games-with-kernel-level-anti-cheat-software/

[9] https://support.esea.net/hc/en-us/articles/360037065354-How-does-the-ESEA-Anti-Cheat-work-

[10] https://blog.invisiblethings.org/2006/06/22/introducing-blue-pill.html

[11] https://blog.invisiblethings.org/2007/08/03/virtualization-detection-vs-blue-pill.html

[12] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2008/08/20084218/BH-US-06-Rutkowska.pdf

[13] https://link.springer.com/chapter/10.1007/978-3-319-50011-9_29#Sec14

[14] https://www.blackhat.com/docs/asia-17/materials/asia-17-Matrosov-The-UEFI-Firmware-Rootkits-Myths-And-Reality.pdf

[15] https://www.webroot.com/blog/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/

[16] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/bioskits-join-ranks-of-stealth-malware/

[17] https://www.zdnet.com/article/fancy-bear-lojax-campaign-reveals-first-documented-use-of-uefi-rootkit-in-the-wild/

[18] https://www.netscout.com/blog/asert/lojack-becomes-double-agent

[19] https://docs.microsoft.com/en-us/windows-hardware/drivers/install/elam-driver-requirements

[20] https://www.kaspersky.com/enterprise-security/wiki-section/products/anti-rootkit-and-remediation-technology

[21] https://www.mcafee.com/enterprise/en-us/downloads/free-tools/how-to-use-rootkitremover.html

[22] https://www.avast.com/c-malware-removal-tool

[23] https://support.avast.com/en-in/article/Antivirus-Boot-time-Scan

[24] https://www.tomshardware.com/news/purism-heads-rootkit-tampering-protection,34128.html

[25] “Rootkits: Subverting the Windows Kernel”, Greg Hoglund, Jamie Butler

[26] “Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats”, Alex Matrosov, Eugene Rodionov

[27] източник за Фигура 1. https://www.ssla.co.uk/linux-operating-system/

[28] източник за Фигура 2. https://itoperationswiki.blogspot.com/2013/12/protection-rings-and-types-of.html

[30] източник за Фигура 3. https://www.kaspersky.com/enterprise-security/wiki-section/products/anti-rootkit-and-remediation-technology