GOCE DELCEV UNIVERSITY, SHTIP, NORTH MACEDONIA

FACULTY OF ELECTRICAL ENGINEERING

ETIMA 2021

FIRST INTERNATIONAL CONFERENCE

19-21 OCTOBER, 2021

TECHNICAL SCIENCES APPLIED IN ECONOMY, EDUCATION AND INDUSTRY

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ” - ШТИП
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

UNIVERSITY „GOCE DELCHEV” - SHTIP
FACULTY OF ELECTRICAL ENGINEERING

ПРВА МЕЃУНАРОДНА КОНФЕРЕНЦИЈА
FIRST INTERNATIONAL CONFERENCE

ЕТИМА / ETIMA 2021

ЗБОРНИК НА ТРУДОВИ
CONFERENCE PROCEEDINGS

19-21 Октомври 2021| 19-21 October 2021

Главен и одговорен уредник / Editor in Chief
Проф.д-р Сашо Гелев
Prof.d-r Saso Gelev

Јазично уредување / Language Editor
Весна Ристова (Македонски) / Vesna Ristova (Macedonian)

Техничко уредување / Technical Editing
Доц.д-р Далибор Серафимовски / d-r Dalibor Serafimovski

Издавач / Publisher
Универзитет „Гоце Делчев" - Штип / University Goce Delchev - Stip
Електротехнички факултет / Faculty of Electrical Engineering

Адреса на организационен комитет / Adress of the organizational committee
Универзитет „Гоце Делчев" – Штип / University Goce Delchev - Stip
Електротехнички факултет / Faculty of Electrical Engineering
Адреса: ул. „Крсте Мисирков" бр. 10-А / Adress: Krste Misirkov, 10 - A
Пош. фах 201, Штип - 2000, С.Македонија / PO BOX 201, Stip 2000, North Macedonia
E-mail: conf.etf@ugd.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

62-049.8(062)
004-049.8(062)

МЕЃУНАРОДНА конференција ЕТИМА (1 ; 2021)
Зборник на трудови [Електронски извор] / Прва меѓународна конференција ЕТИМА 2021, 19-21 Октомври 2021 = Conference proceedings / First international conferece ETIMA 2021, 19-21 October 2021 ; [главен и одговорен уредник Сашо Гелев]. - Штип: Универзитет "Гоце Делчев", Електротехнички факултет = Shtip: University "Goce Delchev", Faculty of Electrical Engineering, 2021

Начин на пристапување (URL): https://js.ugd.edu.mk/index.php/etima. - Текст во PDF формат, содржи 358 стр.илустр. - Наслов преземен од екранот. - Опис на изворот на ден 15.10.2021. - Трудови на мак. и англ. јазик. - Библиографија кон трудовите

ISBN 978-608-244-823-7

1. Напор. ств. насл.
а) Електротехника -- Примена -- Собири б) Машинство -- Примена -- Собири
в) Автоматика -- Примена -- Собири г) Информатика -- Примена -- Собири

COBISS.MK-ID 55209989

Прва меѓународна конференција ЕТИМА
19-21 Октомври 2021
First International Conference ETIMA
19-21 October 2021

ОРГАНИЗАЦИОНЕН ОДБОР
ORGANIZING COMMITTEE

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Маја Кукушева Панева / Maja Kukuseva Paneva
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Весна Конзулова / Vesna Konzulova
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Прва меѓународна конференција ЕТИМА
19-21 Октомври 2021
First International Conference ETIMA
19-21 October 2021

ПРОГРАМСКИ И НАУЧЕН ОДБОР
SCIENTIFIC COMMITTEE

Со Ногучи / So Noguchi
Висока школа за информатички науки и технологии
Универзитет Хокаидо, Јапонија
Graduate School of Information Science and Technology
Hokkaido University, Japan

Дионис Гашпаровски / Dionýz Gašparovský
Факултет за електротехника и информациони технологии,
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Антон Белан / Anton Beláň
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Георги Иванов Георгиев / Georgi Ivanov Georgiev,
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Ивелина Стефанова Балабанова / Ivelina Stefanova Balabanova,
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Бојан Димитров Карапенев / Boyan Dimitrov Karapenev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Влатко Чингоски / Vlatko Cingoski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Божо Крстајиќ / Bozo Krstajic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Милован Радуловиќ / Milovan Radulovic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Гоце Стефанов / Goce Stefanov
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Мирјана Периќ / Mirjana Peric
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Ана Вучковиќ / Ana Vuckovic
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Мирослава Фаркаш Смиткова / Miroslava Farkas Smitková
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Петер Јанига / Peter Janiga
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Јана Радичова / Jana Raditschová,
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Александар Туџаров / Aleksandar Tudzarov
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Владимир Талевски / Vladimir Talevski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

PREFACE

The Faculty of Electrical Engineering at University Goce Delcev (UGD), has organized the International Conference ***Electrical Engineering, Informatics, Machinery and Automation - Technical Sciences applied in Economy, Education and Industry-ETIMA*.**
ETIMA has a goal to gather the scientists, professors, experts and professionals from the field of technical sciences in one place as a forum for exchange of ideas, to strengthen the multidisciplinary research and cooperation and to promote the achievements of technology and its impact on every aspect of living. We hope that this conference will continue to be a venue for presenting the latest research results and developments on the field of technology.
Conference ETIMA was held as online conference where contributed more than sixty colleagues, from six different countries with forty papers.
We would like to express our gratitude to all the colleagues, who contributed to the success of ETIMA'21 by presenting the results of their current research activities and by launching the new ideas through many fruitful discussions.
We invite you and your colleagues also to attend ETIMA Conference in the future. One should believe that next time we will have opportunity to meet each other and exchange ideas, scientific knowledge and useful information in direct contact, as well as to enjoy the social events together.

The Organizing Committee of the Conference

ПРЕДГОВОР

Меѓународната конференција ***Електротехника, Технологија, Информатика, Машинство и Автоматика-технички науки во служба на економија, образование и индустрија-ЕТИМА*** е организирана од страна на Електротехничкиот факултет при Универзитетот Гоце Делчев.
ЕТИМА има за цел да ги собере на едно место научниците, професорите, експертите и професионалците од полето на техничките науки и да представува форум за размена на идеи, да го зајканува мултидисциплинарното истражување и соработка и да ги промовира технолошките достигнувања и нивното влијание врз секој аспект од живеењето. Се надеваме дека оваа конференција ќе продолжи да биде настан на кој ќе се презентираат најновите резултати од истражувањата и развојот на полето на технологијата.
Конференцијата ЕТИМА се одржа online и на неа дадоа свој допринос повеќе од шеесет автори од шест различни земји со четириесет труда.
Сакаме да ја искажеме нашата благодарност до сите колеги кои допринесоа за успехот на ЕТИМА'21 со презентирање на резултати од нивните тековни истражувања и со лансирање на нови идеи преку многу плодни дискусии.

Ве покануваме Вие и Вашите колеги да земете учество на ЕТИМА и во иднина. Веруваме дека следниот пат ќе имаме можност да се сретнеме, да разменime идеи, знаење и корисни информации во директен контакт, но исто така да уживаме заедно и во друштвените настани.

Организационен одбор на конференцијата

Содржина / Table of Contents

UDC: 004.491:004.492.056.5

ROOTKITS – CYBER SECURITY CHALLENGES AND MECHANISMS FOR PROTECTION

Goce Stevanoski,[1] Monika Kachurova,[2] Dimitar Bogatinov,[3]

[1]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, *goce.stevanoski@ugd.edu.mk*
[2]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, *monikakacurova@hotmail.com*
[3]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, *dimitar.bogatinov@ugd.edu.mk*

Abstract

A rootkit is a collection of computer software, typically malicious, that has the intention to infiltrate the operating system (OS) or database, avoiding detection, resist removal and maintain privileged access to the system. Many rootkits are designed to attack the "root", or kernel, of the OS and therefore work without disclosing their presence to the computer owner.
A rootkit is one of the most dangerous malware programs because it allows any program to gain access to different levels of the operating system. Rootkit's detection is difficult because a rootkit may be able to subvert the software that is intended to find it, and usually the only effective way to remove it is to perform a clean reinstallation of the operating system. Because rootkits can hijack or subvert security software, making it likely that this type of malware could live on your computer for a long time causing significant damage, with that positioning as one of the biggest concerns for IT administrators.
This paper aims to review the types of rootkits, their attack methods, as well as to describe the detection and prevention methods against this type of malware.

Key words: Rootkit, Backdoor, prevention, security

Вовед и преглед на литература

Огромниот број на податоци во дигиталниот свет претставува неисцрпно богатство на информации интересни за многу светски актери како што се владини агенции, невладини организации и различни криминални групации. Нивниот мотив постојано продуцира нови начини како да се искористи сајбер просторот за добивање на свежи и навремени доверливи податоци за предметот на интерес. Тоа е порив кој нема да исчезне и во иднина.

Ваквата состојба предизвикува постојан развој на различни вектори за напад на компјутерските мрежи и системи. Во множеството на сајбер закани како единствени по карактеристиките на софистицираност се јавува класа на малициозни софтвери наречена руткитови. Главна цел на руткитовите е да остане што подолго неоткриен во нападнатите системи, овозможи пристап на напаѓачите и сокрие докази за преземените активностите. На повеќето руткитови им се потребни привилегии на административно ниво за да се инсталираат во системот. Тоа најчесто се остварува со искористување на

различни ранливости на системот кои може да овозможат највисок пристап на администраторски права (ring 0). Целосна контрола врз системот значи дека постоечкиот софтвер во системот може да се модифицира, брише и деактивира, тука вклучувајќи го и софтверот кој инаку би можел да се користи за откривање или бришење на истиот.

Детекцијата на нови руткит софтвери во последните 10 години е во опаѓање. Причини за тоа се: сложеноста за да се развие ваков тип на софтвер, па напаѓачите развиваат поедноставни решенија и преземените мерки на развојните компании за отстранување на можностите за инсталација на руткит софтвери директно во дизајнот на системската архитекура. Но последните детекции на овој тип на софтвер, во 2018 на LoJax и во 2020 на MosaicRegressor, покажаа дека неоткривањето на руткитовите во „дивината“ на сајбер просторот се должи ѝ на софистицираноста на напаѓачите при развој на руткит софтверите.

Појавата на LoJax во 2018 година, како прв детектиран UEFI руткит ја потврди веќе започнатата дебата за безбедноста на компјутерските системи од ваков тип на напади. Истражувањата на ASERT и ESET покажаа дека LoJax руткит се користел од страна на групата Sednit на владини компјутерски системи на Балканот и во Централна и Источна Европа. Lojax е предвесник на новиот UEFI руткит софтвер детектиран во 2020 година од страна на Касперски а наречен MosaicRegressor. Овој руткит се наоѓал во компјутерски системи на дипломатски и невладини организации во Азија, Африка и Европа во периодот од 2017 до 2019 година. Истражувањата на собраните податоци и употребен јазик во MosaicRegressor покажале дека доминира кинескиот јазик а се таргетирани организации кои на различни начини биле поврзани со Северна Кореја.

Овие примери покажуваат дека руткитовите софтверите не се изумрени или во опаѓање истите стануваат пософистицирани во нивото присуство и делување а тоа придонесува за потешко детектирање на истите.

Опис на руткитовите и начин на функционирање

Како се појавувале руткит софтверите така нивата дефиниција се менувала. Повеќето дефиниции се однесуваат на тоа дека руткит е злонамерен софтвер, или колекција на злонамерни софтвери, во компјутерските системи, но не го опфаќаат целиот дијапазон на негово единствено делување. Поради тоа во трудот ќе ја прифатиме дефиницијата на (Bill Blunden) дека „Руткит софтвер воспоставува интерфејс за далечински пристап на нападнат систем со кој се овозможува да се манипулира системот и да се собираат податоци на начин на кој е тешко да се открие“.

Терминот руткит е комбинација на "root" (традиционалното име на привилегираниот корисник на оперативните системи слични на Unix) и зборот "kit" (кој се однесува на софтверските компоненти кои ја спроведуваат алатката). Овој термин има негативни конотации поради неговата употреба како софтвер за малициозни активности. Првично, руткитовите претставувале легитимна колекција на алатки што овозможувала административен пристап до компјутер или мрежа. Денес, руткит софтверите се поврзуваат со малициозните видови на софтвери кои обезбедуваат привилигиран пристап на највисоко ниво во компјутерските системи, притоа криејќи го своето постоење и дејствие. Напаѓачите користат руткит за да се сокријат сè додека не одлучат да го нападнат системот. Нападите вклучуваат активности за деактивација на анти-малициозен софтвер и антивирусен софтвер, оштетување на инсталирани апликации, собирање на чувствителни информации и информации за однесувањето на корисникот, започнување на DDoS напади и слично. Со цел отстранување на закана од руткитовите, од витално значење е да се разбере како истите се кријат и како се детектираат во еден систем.

За да се откријат руткитовите и да се заштитат системите од истите, треба да се објасни нивното функционирање. Во понатамошниот текст во чекори е прикажано како тие работат.

Чекор 1: Инфекција на таргетираниот систем

Првиот чекор на напад со руткит е инсталирањето на руткитот во таргетираниот систем. Притоа, се користи еден од следните методи за инсталирање на малициозен софтвер:

- Phishing – напад со испраќање на електронски пораки кои го наведуваат корисникот да преземе документ или да пристапи кон линк кој инсталира руткит во позадина без негово знаење.
- Преземање на лажни софтвери/апликации: Навидум легитимен софтвер кој претставува апликација која го намамува корисникот да преземе руткит.
- Drive by Downloads: Во некои случаи, самата посета на веб страница со слаба веб-безбедност може да инсталира руткит во системот.
- Malvertising: Напаѓачите дизајнираат реклами кои содржат малициозен софтвер за да инсталираат руткит кога ќе се кликне на нив.
- Baiting: Напаѓачот остава УСБ со инсталиран руткит на јавно место. Ако некоја жртва го поврзе со неговиот компјутер, руткитот ќе биде инсталиран.
- Tailgating/ Evil maid attacks: Напаѓачот сам инсталира руткит софтвер на компјутери кои што се без надзор.
- Exploit Kits: Напаѓачите ги користат овие комплети за скенирање на системи/ апликации/ IoT уреди за пронаоѓање на ранливости во системите и за инјектирање на руткитовите.

Чекор 2: Тајни активности

Откако ќе се инсталираат, руткитовите остануваат скриени во системот без знаење на корисникот. Руткитовите ги избегнуваат антивирусните програми, анти – малициозните софтвери и други софтвери за безбедност, бидејќи се подигнуваат во исто време, пред или после подигнувањето на системот. Исто така, руткитовите манипулираат со размена на податоци за време на системските процеси за да го сочуваат неговото постоење.

Чекор 3: Креирање на задна врата

Руткит создава задна врата за обезбедување на напаѓачот со привилегиран пристап до компјутерот и/или мрежата.

<u>Можни последици од напад со руткит</u>

Употребата на руткитовите често се држи во тајност, а со нивна употреба се инсталираат други малициозни софтвери во системот. Руткитовите работат во позадина на системот и често се поддршка на малициозниот софтвер кој се инсталира преку деинсталирање на антивирусната програма, повторна инсталација на малициозниот софтвер и слично.[1] Можни последици од напади со руткитовите се:

Крадење на чувствителни податоци: Руткитовите им овозможува на хакерите да инсталираат дополнителни малициозни софтвери кои крадат чувствителни кориснички информации, како што се броеви на кредитни картички, кориснички лозинки и слично.

Инфекција со малициозен софтвер: Напаѓачите користат руткитовите за да инсталираат малициозен софтвер на компјутерите и системите без да бидат откриени. Руткитовите го кријат малициозниот софтвер од кој било постоечки антивирус, честопати деактивирајќи го безбедносниот софтвер без корисничко знаење. Како резултат на деактивацијата, руткитовите им овозможуваат на напаѓачите да инјектираат штетни датотеки на нападнатиот систем.

Отстранување на датотека: Руткитовите овозможуваат пристап до сите датотеки и команди на оперативниот систем. Напаѓачите кои користат руткитовите можат лесно да ги избришат директориумите на Linux и Windows, клучевите од регистарите и датотеките.

Прислушување: Сајбер криминалците користат руткитови за искористување на необезбедени мрежи и пресретнување на лични кориснички информации и комуникации, како што се е – пошта и пораки разменети преку разговор.

Далечинско управување: Напаѓачите користат руткитови со далечински пристап за промена на системаската конфигурација. Тогаш напаѓачите можат да ги променат отворените TCP порти во внатрешноста на firewall – от или да ги променат скриптите за стартување на системот.

Видови на руткитови

Руткитовите може да се класифицираат според местото на нивното инјектирање. Подолу се прикажани видовите на руткитови, согласно тежината на откривање и отстранување до најсофистицирани и многу потешки за откривање и отстранување.[2]

Апликациски руткитови

Едноставните руткитови работат во режим на корисник. Таквите руткитовите модифицираат процеси, мрежни врски, датотеки, настани и системски услуги. Притоа можат да инфицираат стандардни апликации како Microsoft Office, Notepad, или Paint. Тоа е единствениот вид на руткит што може да се открие со обична антивирусна апликација. Руткитовите во корисничкиот режим се извршуваат во ring 3, заедно со други апликации како корисник, наместо системски процеси на ниско ниво. Тие имаат голем број на можни инсталациски вектори за пресретнување и менување на стандардното однесување на програмските интерфејси (API) на апликацијата.

Некои инјектираат динамички поврзана екстензија (како што е .DLL датотека во Windows или екстензија .dylib на Mac OS X) во други процеси и со тоа можат да навлезат во било кој целен процес за да ја измамат; други со доволно привилегии едноставно за да се пребрише меморијата на целната апликација. Механизмите за инјектирање вклучуваат:

Употреба на проширувања на апликација обезбедена од добавувачи. На пример, Windows Explorer има јавни интерфејси кои им овозможуваат на трети страни да ја прошират својата функционалност.

- Следење на пораките.
- Debuggers.
- Експлоатација на безбедносни слабости.

- Функционирање на најчесто користените API-ја, на пример, за да се скрие процес или датотека што работи во податочниот систем.

Јадрени руткитови

Руткитовите кои работат во јадрото, исто така познати како руткитовите во режим на кернел, можат да го модифицираат целиот оперативен систем. Руткитовите на јадрото се извршуваат со највисоките привилегии на оперативниот систем (Ring 0) со додавање на код или замена на делови од јадрото на оперативниот систем, вклучувајќи ги и Кернелот и соодветните двигатели на уредот. Повеќето оперативни системи ги поддржуваат драјверите за уредот на режимот на јадрото, кои ги извршуваат со истите привилегии како самиот оперативен систем. Оваа класа на руткит има неограничен безбедносен пристап, но е потешко да се напише. Комплексноста прави грешки и сите грешки во кодот што работат на ниво на кернелот може сериозно да влијаат на стабилноста на системот, што доведува до откривање на руткит. Roots може да ги модифицира структурите на податоци во кернелот на Windows користејќи метод познат како манипулација на директен кернел (DKOM). Овој метод може да се користи за да се сокријат процеси. Roots на кернелот исто така може да ја закачи табелата за системска дескрипторска услуга (SSDT) или да ги модифицира портите помеѓу корисничкиот режим и режимот на кернелот, со цел да се скрие самата себе. Честопати, руткит создава скриен, шифриран датотечен систем во кој може да скрие друг малициозен софтвер или оригинални копии на датотеки.

Bootkits

Модификацијата руткит која се вика bootkit може да го инфицира кодот за стартување како Master Boot Record (MBR), записник за гласовно запишување (VBR) или секторот за подигнување, и на тој начин може да се користи за напад на системи за шифрирање со целосен диск.

Hypervisor level (Ниво на хипервизори)

Руткитовите се создадени како Тип II Хипервизори како доказ за концептот. Со искористување на функциите за виртуелизација на хардвер како што се Intel VT или AMD-V, овој тип на руткит работи во Ring-1 и го хостира целниот оперативен систем како виртуелна машина, со што му овозможува на Руткит да интервенира со хардверски повици направени од оригиналниот оперативен систем, За разлика од нормалните хипервизори, тие не мора да се вчитаат пред оперативниот систем, но можат да се вчитаат во оперативен систем пред да го промовираат во виртуелна машина.

Firmware and hardware (Основен софтвер хардвер)

Руткит во основниот софтвер го користи истиот за кај уредот или платформата да создаде постојана слика на малициозен софтвер во хардверот, како што е рутер, мрежна картичка, хард диск или системски BIOS. Руткит-от се крие во основниот софтвер, бидејќи истиот обично не го проверува интегритетот на кодот. Технологијата Intel Active Management, дел од Intel vPro, имплементира управување надвор, давајќи им на администраторите далечна администрација, далечинско управување и далечинска контрола на компјутери без вклучување на процесор или BIOS, дури и кога системот е исклучен. Далечинската администрација вклучува далечинско вклучување и исклучување, далечинско ресетирање, пренасочено подигнување, пренасочување на конзолата, пристап до подигнување на BIOS-те, програмирање за филтрирање за влезните и излезни мрежни сообраќаи, проверка на присуството на агентот, алармирање, пристап до информации за системот, информации за хардверските ресурси, постојани

дневници за настани и други информации кои се зачувани во меморијата. Хардверските руткитови вградени во чипсетот можат да помогнат во враќањето на украдени компјутери, да ги отстранат податоците или да ги направат бескорисни, но исто така претставуваат и загриженост за приватноста и безбедноста на незабележливо шпионирање и пренасочување од страна на раководството или напаѓачите кои би можеле да добијат контрола.

Начини за заштита од руткитовите

Руткит нападите се опасни и штетни, но тие го инфицираат системот или компјутерот само доколку на било кој начин се стартува малициозниот софтвер што го носи руткит. Во понатамошниот текст се наведени чекори што треба да се следат за да се спречи инфекцијата со руткит. [3]

Скенирање на системите: Руткит скенирањата со помош на софтверски програми обично се ефикасни во откривањето и отстранувањето на руткит апликации. Сепак, тие се неефикасни против другите видови на напади.

Скенирањата на ниво на јадро можат да детектираат малициозен код само кога руткит е неактивен. Ова значи дека мора да се запрат сите процеси на системот и да се стартува компјутерот во безбедносен режим за ефикасно скенирање на системот. Потребно е да се направи резервна копија од податоците, а потоа повторно да се инсталира целиот систем.

Избегнување на фишинг напади: Фишинг е вид на напад од социјален инженеринг во кој што напаѓачите користат е – пошта за да ги измамат корисниците да кликнат на малициозен линк или да превземат инфектиран прилог. Инфектираните прилози можат да бидат Word или Excel документи, апликација или програма или инфектирана слика.

Ажурирање на софтвер: Тековните ажурирања на софтверот се од суштинско значење за безбедност или спречување на напаѓачите да инјектираат малициозен софтвер. Сите програми и оперативниот систем треба да бидат ажурирани и на тој начин може да се избегне напад на руткит кој ги користи ранливостите.

Користење на антивирус од следната генерација: Авторите на малициозниот софтвер секогаш се обидуваат да бидат чекор пред индустријата за сајбер безбедност. За спротиставување на неговиот напредок, треба да се користат антивирусни програми кои ги користат модерните безбедносни техники. Притоа, може да се одреди потеклото на руткитот врз основа на неговото однесување, да се открие малициозен софтвер и да се изврши блокирање од инфицирање на системот.

Следење на мрежниот сообраќај: Техниките за следење на мрежниот сообраќај ги анализираат мрежните пакети со цел да се идентификува потенцијален малициозен мрежен сообраќај. Анализата на мрежата исто така може побрзо да ги ублажи заканите додека ги изолира мрежните сегменти кои се под напад за да се спречи ширењето на нападот.

Континуирано образование на корисниците: Напаѓачите ја користат најслабата алка во сајбер безбедноста – човечката компонента – за да постигнат системска инфекција и инсталација на руткис. Најдобар начин да се спречи инфекцијата со руткит е преку континуирано образование на корисниците, особено оние со административни привилегии. Тие треба да разберат како да ги идентификуваат обидите за фишинг, важноста од превземање само на легитимен софтвер, а не со кликнување на сомнителни датотеки кои го идентификуваат потенцијално малициозниот мрежен сообраќај.

Заклучок

Руткит е една од најопасните малициозни програми, поради тоа што дозволува која и да е програма да добие пристап до различни нивоа од оперативниот систем. Сè додека постојат експлоатации на софтвер, руткитовите ќе ги користат овие експлоатирања. Тие работат заедно. Сепак, дури и ако таквите експлоатации не се можни, руткитовите сепак ќе постојат.

Во следните неколку децении, напредокот на технологиите за виртуелна машина ќе нанесе огромен удар врз оние кои се потпираат на далечинска експлоатација. Ова не значи дека експлоатациите ќе исчезнат. Новиот свет на експлоатација ќе се заснова на логички грешки во програмите наместо на архитектурните недостатоци.

Со или без далечинска експлоатација, руткит-ите ќе опстојуваат. Руткитовите може да се сместат во системите во многу фази, од развој до инјектирање. Сè додека има луѓе, луѓето ќе сакаат да дознаваат информации за други луѓе. Ова значи дека руткитовите секогаш ќе имаат место во нашата технологија. Програмите и технолошките субверзии се безвременски.

Руткит најчесто се внесуваат на крајот од процесот на напад. Затоа и се нарекуваат post-exploit алатки.

Користена литература

[1] A. Todd, J. Benson, G. Peterson, T. Franz, M. Stevens, and R. Raines, "Analysis of tools for detecting rootkits and hidden processes," in Proceedings of the IFIP International Conference on Digital Forensics, P. Craiger and S. Shenoi, Eds., Orlando, FL, 2007, pp. 89–105.

[2] J. A. Dawson, J. T. McDonald, J. Shropshire, T. R. Andel, P. Luckett, and L. Hively, "Rootkit detection through phase-space analysis of power voltage measurements," in Proceedings of the International Conference on Malicious and Unwanted Software (MALWARE), Oct. 2017, pp. 19– 27.

[3] L. Zhang, S. Shetty, P. Liu, and J. Jing, ''RootkitDet: Practical end-to-end defense against kernel rootkits in a cloud environment,'' in Proc. 19th Eur. Symp. Res. Comput. Secur., 2014, pp. 475–493.

[4] J. Joy, A. John, and J. Joy "Rootkit Detection Mechanism: A Survey" in Chapter in Communications in Computer and Information Science · January 2011 pp. 367-373

[5] Arati Baliga, Liviu Iftode :" Automated Containment of rootkits Attacks" 2018, pp.2-5

[6] Hyde, D. (2009). A Survey on the Security of Virtual Machines. St. Louis, MO: Washington University in St. Louis. Retrieved 9.2.2020 from https://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec.pdf

[7] Jana, A. P. (2019). Keysniffer [Software]. Retrieved 8.12.2019 from ***https://github.com/jarun/keysniffer***

[8] Kim, S., Park, J., Lee, K., You, I., & Yim, K. (2012). A Brief Survey on rootkit Techniques in Malicious Codes. Journal of Internet Services and Information Security (JISIS), 2(3/4), pp. 134-147.

[9] Kleiman, I., Gao, J., Khan, I. & Song, D. (2019). Honey Pot Bears rootkit [Software]. Retrieved 28.1.2020 from ***https://github.com/shortland/Honey-Pot-Bears-Руткит***

[10] Lehti, R., & Virolainen, P. (2019). AIDE - Advanced Intrusion Detection Environment [Software]. Retrieved 31.1.2020 from https://github.com/aide/aide