УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 11.05.2021. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Саве Милутиновића под насловом „Анализа рансомвер малициозног софтвера и његова модификација ради избегавања детекције“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Сава Милутиновић је рођен 5.4.1997. године у Београду. Завршио је Основну школу „20. Октобар“ у Београду и Девету београдску гимназију у Београду као вуковац. Електротехнички факултет уписао је 2016. године. Дипломирао је на одсеку за Рачунарску технику и информатику 2020. године са просечном оценом 9,24. Дипломски рад одбранио је у септембру 2020. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство уписао је у октобру 2020. године. Положио је све испите са просечном оценом 8,60. Запослен је у струци на позицији софтвер инжењер 2.

2. Извештај о студијском истраживачком раду

Кандидат Сава Милутиновић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на анализу и методе детекције *рансомвер* (енг. *Ransomware*) напада. Истражене и анализиране су врсте рансомвер малвера, као и методе детекције и заштите које користе антивирусни софтвери. У складу са овим истраживањем имплементиране су нове функционалности рансомвера са циљем заобилажења заштите коју пружа антивирусни софтвер, а са циљем обезбеђивања робусније заштите од ове врсте напада.

3. Опис мастер рада

Мастер рад обухвата 37 страна, са укупно 10 слика, 2 табеле и 28 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Такође је уведен појам рансомвера и описани су његов основни механизам рада и заступљеност рансомвер напада у свету.

У другом поглављу је дат детаљан опис рада рансомвера, подела на категорије, где је за сваку категорију дат опис механизма рада, примери напада, као и основне карактеристике сваке категорије рансомвера. Дат је и кратак историјат развоја рансомвера као и опис значајних рансомвер напада.

У трећем поглављу је дат опис метода детекције малвера од стране антивирусног софтвера. За сваку методу детекције је описан механизам рада, предности и слабости методе, као и начини заобилажења кључних мејханизама. Анализа механизама рада антивирусних софтвера је урађена кроз анализу једног софтвера отвореног кода, као и патената комерцијалних антивирусних софтвера.

У четвртом поглављу је описан *RaasNet* програм за прављење *Demonware* рансомвера, који представља основу над којом су рађене модификације реализоване у раду. Описане су и карактеристике *Python* програмског језика и *PyInstaller* библиотеке које су релевантне за овај рансомвер. Такође је дата детаљна анализа кода, начина употребе, корисничког интерфејса и механизма рада програма и рансомвера.

У петом поглављу су приказани начини модификовања рансомвера, где је за метрику успешности узет број детекција користећи *VirusTotal* веб сервис и успешност заобилажења

детекције од стране *Windows Defender* антивирусног софтвера при извршавању на виртуелној машини. Првобитно је урађена анализа перформанси оригиналног рансомвера и идентификација дела кода који доприноси детекцији од стране антивирусног софтвера. Урађене су модификације претходно идентификованог кода за комуникацију са сервером и шифровање података. Такође је урађено сакривање кода кроз шифровање изворног кода. Модификације су анализиране самостално и комбиновано.

Шесто поглавље је закључак у оквиру кога су сумирани резултати анализе и модификације рансомвера. Уочени су недостаци у модерном антивирусном софтверу и технологија на којој се ради како би се побољшао њихов рад у будућности. Такође, наведени су недостаци рада у анализи комерцијалних сигурносних система који се користе у привреди као и заобилажења детекције на нивоу машинског кода.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Саве Милутиновића се бави анализом и модификацијом рансомвера, са циљем разумевања механизама детекције од стране антивирусних алата у корисничким уређајима. Успешно су реализоване модификације *Demonware* рансомвера које успешно заобилазе детекцију у окружењу за тестирање и имају значајно мањи број детекција на *VirusTotal* веб сервису. У оквиру рада је приказан програм који служи за прављење разних врста рансомвера, што је једна од најпопуларнијих метода за зараду у сајбер криминалу у скорије време. Такође је дата детаљна анализа антивирусног софтвера и неких од метода који они користе за детекцију малвера.

Основни доприноси рада су: 1) детаљна анализа механизама рада рансомвера и антивирусних алата који детектују рансомвер, 2) имплементација модификација рансомвера за сакривање комуникације са сервером путем интернета, сакривањем изворног кода шифровањем и сакривање шифровања модатака користећи мање познате алгоритме; 3) Тестирање успешности антивирусних софтвера при детекцији различитих врста рансомвера.

5. Закључак и предлог

Кандидат Сава Милутиновић је у свом мастер успешно анализирао рањивости у антивирусном софтверу и применио уочене мане при имплементацији модификација рансомвера које могу да заобиђу неке од метода детекције модерног антивирусног софтвера. Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.

На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Саве Милутиновића под насловом „Анализа рансомвер малициозног софтвера и његова модификација и циљу заобилажења одбране“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 11.09.2023. године

Чланови комисије:

Др Павле Вулетић, ванредни професор

Др Жарко Станисављевић, ванредни професор