Prof. dr hab. inż. Tadeusz Niedziela Warszawa 19.06.2024 r.

Recenzja rozprawy doktorskiej

mgr inż. Michała Gleta

pt. Uniwersalny zestaw wskaźników do wykrywania ataków ransomware

1. Podstawa opracowania recenzji

Podstawą wykonania recenzji jest pismo Dziekana Wydziału Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie dr hab. inż. Jerzego Pejaśa, prof. ZUT z dnia 22.06.2024 r. o wyznaczeniu w dniu 21.05.2024 r. przez Radę Dyscypliny Informatyka techniczna i telekomunikacja na recenzenta pracy doktorskiej mgr inż. Michała Gleta na temat: „Uniwersalny zestaw wskaźników do wykrywania ataków ransomware".

Recenzowana rozprawa doktorska jest z obszaru nauk technicznych (dyscyplina naukowa Informatyka techniczna i telekomunikacja). Rozprawa została wykonana na Wydziale Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego pod kierunkiem naukowym Promotora prof. zw. dr hab. dr h. c mult. Brunona Hołysta i Promotora pomocniczego dr inż. Piotra Bora.

Recenzję sporządzono na podstawie dostarczonej dokumentacji tj. papierowej wersji rozprawy doktorskiej oraz jej zapisu w wersji elektronicznej zamieszczonej na płycie CD.

2. Treść i zakres rozprawy doktorskiej

Opiniowana rozprawa doktorska zawiera 293 stron. Składa się z: 11 ponumerowanych rozdziałów (z których w ostatnim jest bibliografia, literatura uzupełniająca, spis rysunków oraz spis listingów kodów źródłowych), streszczenia (w wersji polskiej i angielskiej). Układ pracy nie budzi zastrzeżeń.

Dokonany przez Doktoranta przegląd literatury oraz przeprowadzona analiza stanu problemu pozwoliła na określenie w rozdziale pierwszym: przedmiotu badań i celu badań, hipotez badawczych, zakresu badań, metod badawczych oraz ustalenie aktualnego stanu badań.

Przedmiotem badań w rozprawie doktorskiej jest szeroko rozumiane bezpieczeństwo danych w kontekście ataków z oprogramowaniem złośliwym typu ransomware. Badania mają charakter teoretyczny polegające na wyjaśnieniu istoty działania oprogramowania ransomware oraz ustaleniu metod wykrywania jego aktywności (wskaźników).

Celem badań jest opracowanie metody, umożliwiającej skuteczne wykrywanie ataków z wykorzystaniem oprogramowania typu ransomware na wczesnym etapie jego aktywności dla zwiększenia szerokorozumianego bezpieczeństwa (państwa, społeczeństwa oraz jednostek). Dodatkowym nie mniej ważnym celem jest opracowanie wskaźników wykrywania aktywności nowych, nieznanych, wersji krypto wirusów.

Celem poznawczym badań, jest analiza funkcjonowania oprogramowania ransomware oraz analiza metod wykrywania jego aktywności.

Głównym problemem badawczym jest odpowiedź na pytanie: W jaki sposób zwiększyć poziom bezpieczeństwa: państwa, społeczeństwa oraz obywateli w kontekście ataków z wykorzystaniem oprogramowania typu ransomware?

Doktorant sformułował główną hipotezę badawczą i szczegółowe hipotezy badawcze .

Główna hipoteza badawcza

Opracowane autorskie wskaźniki wykrywania ataków typu ransomware zwiększą poziom bezpieczeństwa danych w ujęciu bezpieczeństwa jednostki, społeczeństwa oraz państwa.

Szczegółowe hipotezy badawcze

A. Cechy charakterystyczne wyodrębnione na podstawie analizy wybranych próbek oprogramowania ransomware umożliwią utworzenie zestawu wskaźników wykrywających aktywność w systemie operacyjnym wirusa typu ransomware.
B. *Wykorzystanie funkcji LSH/LPH umożliwi wykrycie aktywności złośliwego oprogramowania typu ransomware.*
C. Wykorzystanie mechanizmu pułapek typu honeypot umożliwi wykrycie aktywności złośliwego oprogramowania typu ransomware.

Sformułowany przedmiot i cel badań oraz hipotezy badawcze (główna i szczegółowe) są spójne i logiczne.

W związku z ustalonym przedmiotem i celem badań, problemami badawczymi oraz hipotezami badawczymi Doktorant określił szeroki zakres badań oraz przyjął założenie, że wykorzystanie zostanie metoda projektowania systemów informatycznych, polegająca na ustalaniu oraz teoretycznej weryfikacji założeń koncepcji przed jej implementacją co pozwoli zmniejszyć ryzyko niepowodzenia oraz błędów podczas praktycznej realizacji koncepcji.

Problem ochrony przed atakami z wykorzystaniem oprogramowania ransomware jest obecnie aktualny i ważny zarówno z punktu widzenia naukowego jak i praktycznego (szeroko rozumianego cyberbezpieczeństwa).

Złośliwe oprogramowanie może być wykorzystywane do różnych celów (kradzieży danych, niszczenia danych, uszkodzenia systemu operacyjnego, podsłuchiwania komunikacji, ataków na komputery oraz wielu szkodliwych oraz nielegalnych działań). Cyberprzestępcy ciągle rozwijają nowe rodzaje złośliwego oprogramowania, stąd ważne jest, aby być świadomym zagrożeń i zachować ostrożność podczas korzystania z zasobów. Oprogramowanie ransomware ciągle zyskuje na złożoności i różnorodności. Ewoluuje, staje się bardziej zawansowane i jest niezwykle popularne w świecie cyberprzestępczości. Żądane okupy przez przestępców stają się coraz wyższe a ataki ukierunkowane są na sektory krytycznej infrastruktury, duże korporacje czy organizacje.

W rozdziale drugim Doktorant opisał: podstawowe pojęcia związane z oprogramowaniem ransomware: definicje i klasyfikacje oprogramowania ransomware, definicje oprogramowania ransomware, fazy oprogramowania ransomware, fazy ataku oprogramowania ransomware, sposoby rozprzestrzeniania, ransomwareas a service, rys historyczny oprogramowania ransomware oraz statystyki ataków ransomware.

W rozdziale trzecim Doktorant przeanalizował działanie oprogramowania ransomware rodziny Avaddon z punktu widzenia: zaatakowanego użytkownika, sposobu instalacji, powodowanych szkód, sposobu odzyskania danych, analizy

statystycznej (analizy importowanych bibliotek zewnętrznych, analizy wykorzystywanych funkcji z Windows API, deasemblacji, dekompilacji), analizy dynamicznej (analizy stanu systemu po przeprowadzeniu ataku, analizy stanu dysku po przeprowadzonym ataku, analizy wywołań istotnych funkcji API systemu Windows), audytu kodu źródłowego (funkcji main, mechanizmu szyfrowania danych – tworzenia kontekstu oraz kluczy kryptograficznych, mechanizmu szyfrowania danych – szyfrowania zawartości pliku, mechanizmu szyfrowania danych – szyfrowania klucza AES kluczem publicznym RSA, analizy funkcji API systemu Windows używanych przez Avaddon), technicznej analizy budowy, sposobu działania i sposobu rozprzestrzeniania.

Rozdział czwarty dotyczy wywoływania funkcji API udostępnianych przez system operacyjny, które stanowi ważną część oprogramowania ransomware. W związku z powyższym dla zrealizowania podstawowych celów rozprawy Doktorant przeprowadził szereg badań (wykonywania operacji kryptograficznych – CryptoAPI, wykonywania operacji na plikach i folderach – FileAPI, wykonywania operacji sieciowych – NetworkAPI, wykonywania operacji związanych z obsługą wątków oraz procesów – ProcessThreadAPI, wykonywania operacji związanych z ustawieniami systemu operacyjnego – SystemSettingsAPI, wykonywania nietypowych operacji – UnusualAPI). Doktorant przeprowadził badania wykorzystując wiele wersji oprogramowania ransomware (AvosLocker, BlackMatter, Cuba, Dharma, DoejoCrypt, Epsilon, HDLocke, Jormungad). Badania cech charakterystycznych oprogramowania ransomware w kontekście wywoływanych funkcji API systemu operacyjnego Windows prowadzone były w jednolitym środowisku testowym. Każda próbka ransomware testowana była na tej samej instancji stacji testowej. Wyniki badań poszczególnych próbek ransomware podzielone zostały na cztery kategorie ze względu na częstość wywołań oraz na trzy kategorie ze względu na istotność (funkcje API niebezpieczne, funkcje API potencjalnie niebezpieczne oraz funkcje ogólnego przeznaczenia).

W rozdziale piątym Doktorant przeanalizował ważne pułapki typu honeypot, które udają słabe lub niewłaściwie zabezpieczone zasoby (serwer, routery, bazy danych lub inne komputery struktury IT). W ogólnym przypadku to zasób komputerowy, który ma przyciągać cyberataki. Innymi słowy to przynęty na cyberprzestępców. Atakujący próbujący wykryć słabe punkty w systemach, są przyciągani do honeypot'a. Doktorant słusznie uważa, że pułapki typu honeypot mogą stanowić jeden z mechanizmów wczesnego wykrywania aktywności oprogramowania ransomware. Zatem można je z powodzeniem zastosować do wykrywania trwającego ataku oprogramowania ransomware w pojedynczym systemie komputerowym na rzeczywiście działającym zasobie (decoy files). Specjalnie spreparowane pliki lub zestawy plików są umieszczane w systemie komputerowym celem zwabienia potencjalnych atakujących a także identyfikacji prób naruszenia bezpieczeństwa. Doktorant stwierdza, że wykorzystanie plików decoy files w połączeniu z honeypot'ami może stanowić skuteczny mechanizm wykrywania ataków oprogramowania ransomware.

Rozdział szósty dotyczy badań losowości danych. Wykorzystanie mechanizmów badania poziomu losowości danych umożliwia skuteczne wykrycie aktywności złośliwego oprogramowania. Doktorant założył, że entropie Shannon'a można wykorzystać do weryfikacji zmiany poziomu losowości pomiędzy danymi odczytywanymi a zapisywanymi. Im zwrócona wartość będzie mniejsza, tym analizowane dane będą charakteryzowały się mniejszym poziomem losowości.

Badania entropii Shannon'a Doktorant przeprowadził z wykorzystaniem szerokiej wersji oprogramowania ransomware (Maoloa, UnlockYourFiles, BlackKingdom, Ryuk, DarkSide, WannaCry, REvil, JigsawLocker). Dodatkowo przeanalizował wartości entropii Shannon'a dla plików audio, wideo, obrazów oraz dokumentów przed oraz po atakach przykładowych wersji oprogramowania ransomware. Na potrzeby mechanizmu detekcji aktywnego ataku oprogramowania ransomware Doktorant przebadał dane odczytywane oraz zapisywane na dysku (pliki) stosując test Mauera jako „poprawny sposób pomiaru jakości kluczy używanych w algorytmach kryptograficznych". Badania zostały przeprowadzone z szeroką wersją oprogramowania ransomware (Maoloa, UnlockYourFiles, BlackKingdom, Ryuk, DarkSide, WannaCry, REvil, JigsawLocker). Uzyskane wyniki badań przedstawił w formie tabel wartości testu Mauera dla plików testowych przed oraz po atakach wykonanych wersji oprogramowania ransomware. Kolejnym testem losowości był test monobitowy, który zastosował Doktorant dla plików testowych (niezaszyfrowanych i zaszyfrowanych) przed oraz po atakach wybranych wersji oprogramowania ransomware. Wynikiem tego testu było ustalenie, czy analizowane dane binarne są zgodne z oczekiwanym rozkładem losowym. Uważam, że niezwykle cenne są prezentowane w tym rozdziale wyniki badań wartości testu Maurea, entropii Shannon'a i testu monolitowego porównujące czasy wykonania dla plików niezaszyfrowanych i zaszyfrowanych oraz częściowo zaszyfrowanych. Prezentowane w rozprawie oryginalne wyniki badań Doktoranta wyraźnie ilustrują możliwości oceny zmian zachodzące w plikach oraz efektywności stosowanych testów: testu Maurea, entropii Shannon'a i testu monobitowego.

Rozdział siódmy dotyczy dwóch technik kategoryzacji danych LSH (Locality-Sensitive Hashing) oraz LPH (Locality-Preserving Hashing) stosowanych w analizie danych zwłaszcza w kontekście przetwarzania i organizacji dużych zbiorów danych oraz w zadaniu wyszukiwania podobnych elementów w danych. Doktorant zastosował techniki obliczania skrótów w analizie danych. Z punktu widzenia bezpieczeństwa są to niekryptograficzne funkcje skrótu. Doktorant słusznie uważa, że monitorowanie poziomu zmian w danych można wykorzystać we wskaźnikach wczesnej detekcji oprogramowania ransomware

Rozdział ósmy dotyczy analizy dostępnych metod (metody analizy struktur, metody analizy zachowania, metody heurystycznej modelowania, metody bazującej na uczeniu maszynowym oraz sztucznej inteligencji) wykrywania złośliwego oprogramowania. Doktorant ustalił główne zalety oraz wady wykrywania złośliwego oprogramowania powyższych metod.

W rozdziale dziewiątym Doktorant prezentuje oryginalne autorskie opracowane wskaźniki wykrywania aktywności oprogramowania ransomware. Podstawowym celem wskaźników do monitorowania wywołań funkcji API jest uzyskanie informacji z jakich funkcji API systemu dany proces korzysta w określonym momencie. W wyniku przeprowadzonych analiz i badań Autor zaproponował wysokopoziomowe wskaźniki wykrywania złośliwego oprogramowania. Dla każdego wskaźnika ustalił podstawowe atrybuty/nazwy wskaźnika, bazowy mechanizm, idee działania, poziom weryfikacji pozytywnej, poziom weryfikacji negatywnej oraz poziom ostrzegawczy. Na potrzeby wczesnej detekcji oprogramowania typu ransomware zaproponował dziewięć wskaźników (wskaźnik wykorzystania API kryptograficznego, wskaźnik wykorzystania API plikowego, wskaźnik wykorzystania API do obsługi wątków oraz procesów, wskaźnik wykorzystania funkcji API do modyfikacji ustawień systemowych, wskaźnik wykorzystania nietypowego API, wskaźnik zmian losowości

danych, wskaźnik zmian klasy abstrakcji, wskaźnik dostępu do pułapek honeypot, wskaźnik zmian pułapek honeypot), których zadaniem jest ciągła analiza procesów, zasobów oraz stanu systemu. Zadaniem dużej części wskaźników jest monitorowanie wykorzystania różnego rodzaju funkcji API udostępnianych przez system Windows.

Opisał techniki wstrzykiwania kodu na potrzeby monitorowania wykorzystania API (wstrzykiwanie DLL za pomocą funkcji CreateRemoteThread, wstrzykiwanie DLL za pomocą funkcji SetWindowsHookEx, wstrzykiwanie DLL za pomocą funkcji AppInt DLLs, Portable Executable Injection), modyfikacje wpisów w tabele adresów importowanych funkcji IAT, wykrywanie powstawania nowego procesu w systemie Windows. Dokonał specyfikacji technicznej wskaźników (wskaźnika wykorzystania API kryptograficznego, wskaźnika wykorzystania API plikowego, wskaźnika wykorzystania API do obsługi wątków oraz procesów, wskaźnika wykorzystania API do modyfikacji ustawień systemowych, wskaźnika wykorzystania nietypowego API) oraz specyfikacji technicznej wskaźnika zmian poziomu losowości danych (wskaźnika zmian abstrakcji, wskaźnika dostępu do pułapek honeypot, wskaźnika zmian pułapek honeypot).

Autor rozprawy opracował prototypową implementację wskaźników z wykorzystaniem języka C/C++. Na potrzeby mechanizmu wykrywania nowego procesu w systemie Windows, oraz potrzeby wskaźników utworzył filtr sterowników wysokiego poziomu, który został umieszczony nad sterownikiem systemu plików. Na potrzeby prototypowej implementacji wskaźników monitorowania API wykorzystał mechanizm EasyHook. Mechanizm ten zastosował na potrzeby tworzenia API Hook'ów. W tym rozdziale wykazał się dużą swobodą operowania nowoczesnymi narzędziami informatycznymi.

Korzystając z opracowanych prototypowych implementacji wskaźników detekcji aktywności oprogramowania ransomware, Autor rozprawy przeprowadził testy skuteczności ich działania. Testy przeprowadzone zostały w kontrolowanym środowisku symulującym rzeczywisty system komputerowy. Testy skuteczności zaimplementowanych wskaźników Doktorant wykonał korzystając z szerokiego oprogramowania ransomware (Maoloa, Ryuk, DarkSide, WannaCry, REvil, Conti, Maze, LockBit, Sodinokibi, Cuba, Nefilim, AvosLocker, HelloKitty, Dharma, MedusaLocker, Chao, GlobeImposter, Petya, LockyNetWalker, LockerGogaKeyPass). Duża liczba zastosowanych wskaźników to nowe nieużywane dotychczas wersje.

Testy przeprowadzone przez Doktoranta na opracowanych prototypowych implementacjach wskaźników, zarówno dla próbek stosowanych w trakcie badań wstępnych, jak również na nieznanych wersjach oprogramowania ransomware wykazały wysoki poziom wykrycia aktywnego ataku ransomware przez zaproponowane wskaźniki. Godnym uwagi jest fakt, iż wysoki (96%) poziom wykrycia został osiągnięty nawet bez udziału sześciu wskaźników odpowiedzialnych za monitorowanie wywołań wybranych funkcji API systemu Windows. Kolejnym ważnym testem było oszacowanie ogólnego spadku wydajności systemu operacyjnego po wyłączeniu zaimplementowanego mechanizmu wykrywania aktywności oprogramowania ransomware. Uzyskane duże różnice w wydajności wirtualnych maszyn wskazują na konieczność przeprowadzenia kolejnych dalszych badań na fizycznym środowisku testowym.

Doktorant dokonał ważnej weryfikacji jaki wpływ na normalne działanie oprogramowania dodatkowego ma opracowany system wykrywania aktywności ransomware z wyłączonym: mechanizmem monitorowania aktywności dyskowych,

mechanizmem obsługi pułapek honeypot oraz mechanizmem wywołań API systemu Windows. Uzyskane wyniki wskazują, na konieczność opracowania mechanizmu ograniczającego liczbę alarmów typu „false positive".

Autor w rozprawie udowodnił bardzo wysoki poziom detekcji zaproponowanych prototypowych implementacji wskaźników, które mogą być wykorzystane do zbudowania skutecznego systemu detekcji oraz zatrzymania ataku ransomware.

W rozdziale dziesiątym Autor dokonał zwięzłej weryfikacji hipotez badawczych dotyczących wskaźników detekcji aktywności złośliwego oprogramowania na podstawie przeprowadzonych badań opracowanych prototypowych implementacji wskaźników. Doktorant potwierdził prawdziwość hipotez szczegółowych dotyczących wskaźników detekcji aktywności złośliwego oprogramowania, na podstawie wyników eksperymentalnych otrzymanych podczas przeprowadzonych testów zaproponowanych implementacji wskaźników z wykorzystaniem wielu (23) próbek oprogramowania ransoware. Tym samym potwierdził empirycznie główną hipotezę badawczą *„Opracowane autorskie wskaźniki wykrywania ataków typu ransomware zwiększą poziom bezpieczeństwa danych w ujęciu bezpieczeństwa jednostki, społeczeństwa oraz państwa"*.

Rozdział jedenasty to podsumowanie rozprawy doktorskiej.

3. Ocena merytoryczna rozprawy doktorskiej

Recenzowana rozprawa doktorska „Uniwersalny zestaw wskaźników do wykrywania ataków ransomware" prezentuje dużą wiedzę teoretyczną oraz praktyczną mgr inż. Michała Gleta w dyscyplinie naukowej Informatyka techniczna i telekomunikacja Jej zawartość merytoryczna potwierdza wysokie umiejętność Autora do samodzielnego prowadzenia badań naukowych.

Doktorant wybrał tematykę związaną ze złośliwym oprogramowaniem oraz jego przeciwdziałaniem. Tematyka jest obecnie niezwykle aktualna i bardzo ważna ze społecznego punktu widzenia. Zgodnie z przytoczonymi w rozprawie danymi statystycznymi oraz eksperckimi prognozami, oprogramowanie ransomware stanowiło, stanowi i przez kolejne lata będzie stanowić poważne zagrożenie dla szeroko pojętego bezpieczeństwa teleinformatycznego. Głównym wynikiem rozprawy jest specyfikacja wskaźników detekcyjnych, których zadaniem jest monitorowanie procesów w systemie Windows oraz weryfikacja, czy nie są to procesy oprogramowania ransomware. Na potrzeby weryfikacji poprawności działania zaproponowanych wskaźników, Autor opracował ich prototypowe implementacje oraz zaprezentował otrzymane wyniki testów. Dzięki takiemu podejściu, powstała rozprawa, która z jednej strony prezentuje oryginalne autorskie propozycje w sposób teoretyczny, uzasadniając ich wybór oraz skuteczność, a następnie weryfikuje ich rzeczywiste działanie. W tym miejscu należy pochwalić Autora za przygotowanie rozprawy zawierającej w sobie elementy czysto naukowe oraz czysto praktyczne. Potwierdza to wysokie umiejętności Doktoranta z zakresu prowadzenia badań naukowych wraz z wysokimi umiejętnościami stricte inżynierskimi. Zaproponowane wskaźniki wymagają wykorzystania wielu różnych, niskopoziomowych mechanizmów systemu Windows oraz technik programowania. Jest to wiedza bardzo specjalistyczna, na ogół nie znana powszechnie nawet wśród wykwalifikowanych inżynierów informatyki. Zrozumienie działania oraz wykorzystanie tych mechanizmów do stworzenia systemu bezpieczeństwa chroniącego przed atakami ransomware, niewątpliwie stanowi duże osiągnięcie Doktoranta. Przedmiot przeprowadzonych przez Autora badań oraz przedmiot dysertacji stanowi oryginalne rozwiązanie

problemu naukowego, a uzyskane wyniki mogą znaleźć szerokie zastosowanie w sferze mechanizmów bezpieczeństwa teleinformatycznego. Tym samym, otrzymane w rozprawie wyniki z pewnością znajdą zastosowanie zarówno w sferze gospodarczej jak i społecznej.

Bardzo pozytywnie oceniam ilość oraz jakość przeprowadzonych oraz opisanych w rozprawie badań naukowych. W pierwszej części badania związane są bezpośrednio z oprogramowaniem ransomware oraz jego analizą. Następnie, przeprowadzane są wstępne badania potwierdzające słuszność zaproponowanych przez Doktoranta metod detekcji. Na potrzeby tych badań wykorzystane zostały liczne wersje złośliwego oprogramowania. Rozprawa kończy się badaniami skuteczności oraz efektowności działania prototypowych implementacji wskaźników. Na potrzeby tych badań również wykorzystane zostały liczne wersje złośliwego oprogramowania, częściowo inne niż uprzednio. Tym samym, zweryfikowana została niejako skuteczność wskaźników w wykrywaniu nieznanych wcześniej zagrożeń. Wszystkie uzyskane wyniki badań przedstawione zostały w bardzo czytelny i jasny sposób. Zazwyczaj występowały w formie tabelarycznej, z wyraźnym zaznaczeniem innym kolorem istotnych danych oraz wyników.

Doktorant w sposób swobodny i racjonalny stosował zaawansowane narzędzia informatyczne a uzyskane wyniki badań świadczą o wysokich umiejętnościach planowania i rozwiązywania złożonych problemów naukowych. Prezentowane w rozprawie wyniki stanowią kompendium wiedzy na temat wykrywania ataków przez złośliwe oprogramowania.

W opinii recenzenta rozprawa doktorska pt. Uniwersalny zestaw wskaźników do wykrywania ataków ransomware nosi wszelkie znamiona oryginalności twórczej.

4. Uwagi ogólne i szczegółowe

Pomimo bardzo pozytywnego doboru tematyki oraz treści rozprawy doktorskiej mgr inż. Michała Gleta, uwagę należy zwrócić również na małoistotne, aczkolwiek negatywne aspekty. Składają się na nie: zbyt duża objętość (pomijając mało istotne dla ostatecznego wyniku pracy elementy, można było uzyskać taką samą jakościowo rozprawę przy mniejszej, przyjaźniejszej dla czytelnika, objętności) oraz niepotrzebny wstęp związany z podstawowymi pojęciami z zakresu informatyki ogólnej.

Zawarte w recenzji uwagi nie wpływają na wysoką wartość merytoryczną rozprawy. Praca nie wymaga w związku z tym zmian ani uzupełnień.

Bardzo wysoko oceniam warsztat naukowy mgr inż. Michała Gleta. Liczba publikacji naukowych jak ich jakość oraz ilość udziałów w konferencjach, jest czymś rzadko spotykanym na tym etapie rozwoju kariery naukowej.

5. Wniosek końcowy

Recenzowana rozprawa doktorska dotyczy aktualnego problemu badawczego i ma charakter teoretyczny. Stanowi oryginalne rozwiązanie wykrywania ataków złośliwego oprogramowania.

Mając na uwadze kompleksową ocenę zawartości rozprawy doktorskiej mgr inż. Michała Gleta pt. „Uniwersalny zestaw wskaźników do wykrywania ataków ransomware" **stwierdzam jednoznacznie**, że praca spełnia wymagania stawiane rozprawą doktorskim.

Przedłożoną do recenzji rozprawę doktorska oceniam bardzo pozytywnie. Na szczególną uwagę zasługują otrzymane oryginalne wyniki badawcze. Uważam, że

Doktorant wykazał się samodzielnością oraz wysokimi umiejętnościami rozwiązywania problemów naukowych.

Praca doktorska stanowi oryginalne rozwiązanie problemu naukowego, dotyczącego dyscypliny naukowej: Informatyka techniczna i telekomunikacja.

Stwierdzam, że recenzowana rozprawa doktorska spełnia wymagania obowiązujących przepisów w odniesieniu do prac doktorskich zawarte w art. 187 ust. 1 i ust. 2 Ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. 2023 poz. 742, ze zm.). **Stwierdzam również, że sformułowane hipotezy rozprawy zostały udowodnione, a cel pracy został osiągnięty**.

Wnioskuję o przyjęcie rozprawy i dopuszczenie jej do dalszego procedowania oraz publicznej obrony.

Po zapoznaniu się z zawartością rozprawy doktorskiej mgr inż. Michała Gleta pt. „Uniwersalny zestaw wskaźników do wykrywania ataków ransomware" oraz zasadami wyróżniania rozpraw doktorskich na Wydziale Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie, składam wniosek o jej wyróżnienie.

Uzasadnienie: W ocenie recenzenta rozprawa doktorska pt. „Uniwersalny zestaw wskaźników do wykrywania ataków ransomware" reprezentuje wyjątkowo wysoki poziom naukowy w stosunku do wymagań ustawowych. Autor rozwiązał problem badawczy z wykorzystaniem najnowszych narzędzi informatycznych. Zaproponował autorskie oraz nowatorskie techniki wykrywania ataków oprogramowania ransomware, bazujące na oryginalnych metodach detekcji. Wykorzystane przez Doktoranta prymitywy, takie jak np. funkcje LSH i LPH, stanowią nietypowe oraz oryginalne podejście do problemu wykrywania oprogramowania malware. Uzyskane wyniki badań opublikowane zostały głównie w wysoko punktowanych zagranicznych czasopismach naukowych (wykaz poniżej). Zaproponowane w rozprawie doktorskiej metody badawcze stanowią istotny wkład w rozwój dyscypliny Informatyka techniczna i telekomunikacja. Uzyskane przez Autora wyniki mogą być z powodzeniem wykorzystane zarówno w praktyce jak i w procesie dydaktycznym oraz w tworzeniu szkoły naukowej w zakresie cyberbezpieczeństwa.

Niedziela

.....

prof. dr hab. inż. Tadeusz Niedziela

Wykaz publikacji bezpośrednio związanych z rozprawą doktorską

1. M. Glet, K. Kaczyński, Ransomware and Honeypots, 38th IBIMA Conference, Seville, Spain, 11.2021, (70 pkt);
2. M. Glet, K. Kaczyński, POSTER: Ransomware Detection Mechanism – Current State of the Project. In: , et al. Applied Cryptography and Network Security Workshops. ACNS 2022. Lecture Notes in Computer Science, vol 13285. Springer, 06.2022, (70 pkt);
3. Bajera, J., Glet, M., (2023). Ransomware Attack on the QNAP Device – The Case Study, 41th IBIMA Conference, Seville, Spain, 06.2023, (70 pkt);
4. Glet, M., Kaczyński, K., POSTER: Ransomware Detection Mechanism – Project Status at the beginning of 2023. In: , et al. Applied Cryptography and Network Security Workshops. ACNS 2023. Lecture Notes in Computer Science, Springer, 06.2023, (70 pkt);
5. Kukuła, K., Glet, M., (2024), The usage of the Post Thread Message mechanism for non-standard inter-process communication in the Windows operating system – The Case Study, 43rd IBIMA Conference, Seville, Spain, (w trakcie publikacji), (70 pkt);
6. Bajera, J., Glet, M., (2024), Detection of cryptographic functions within binary executable ransomware files – The Case Study, 43rd IBIMA Conference, Seville, Spain, (w trakcie publikacji), (70 pkt);
7. CRYPTXXX V3 – ANALIZA UŻYTEGO MECHANIZMU SZYFROWANIA, Biuletyn WAT, Vol. LXV, Nr 4/2016, (7 pkt).

Wykaz publikacji pośrednio związanych z rozprawą doktorską

1. M. Glet, Analiza metod projektowania funkcji skrótu oraz możliwości zastosowania w projekcie przekształceń trójkątnych, praca zbiorowa: Brunon Hołyst, Jacek Pomykała, „Podpis elektroniczny i biometryczne metody identyfikacji", Wyd. Wyższa Szkoła Menedżerska, Warszawa 2010, ISBN 978-83-7520-042-3, str. 149-164, (pkt. 3);
2. M. Glet, Projekt funkcji skrótu bazującej na konstrukcji MCM i przekształceniach trójkątnych, Biuletyn WAT, Vol. LX, Nr 4, 2011, pp. 399-411, (9 pkt);
3. M. Glet, Implementacja ataku strukturalnego na sieci SAN, Praca zbiorowa Brunon Hołyst, Jacek Pomykała, Cyberprzestępczość i ochrona informacji. Wyższa Szkoła Menedżerska, Warszawa, ISBN 978-83-7520-076-8; 2012, 233-244;
4. J. Dmitruk, M. Glet, PDF Encryption oparty o certyfikaty X.509 – teoretyczny poziom bezpieczeństwa, Biuletyn WAT, Tom 66, Zeszyt 4, 2017, (pkt. 8);
5. M. Glet, Security Analysis of Signal Data Storage Mechanisms in iOS Version, International Journal on Information Technologies and Security, Vol. 11, No 4 (2019), ISSN: 1313-8251, (20 pkt);
6. M. Glet, K. Kaczyński, Acces Logs – Underestimated Privacy Risks, International Journal of Electronics and Communications, Vol. 66, No. 3 (2020), DOI: 10.24425/ijet.2020.131892, pp. 405-410, (40 pkt);
7. M. Glet, K. Kaczyński, Authentication of Physical Objects with Dot-Based 2D Code, 22nd International Conference on Information Security and Assurance, 16-17.09.2020, Lizbona, Portugalia, Materiały konferencyjne - International Journal of Computer and Information Engineering Vol:14, No:8, 2020, pp. 293-299, (20 pkt);
8. M. Glet, K. Kaczyński, Secret Sharing Scheme for Creating Multiple Secure Storage Dimensions for Mobile Applications, International Journal on Information Technologies and Security, Vol. 12, No 4 (2020), ISSN: 1313-8251, pp. 83-102, (20 pkt);
9. M. Glet, K. Kaczyński, Digital signature corruption – macOS case study, 36th IBIMA Conference, Granada, Spain, 4-5.11.2020, (70 pkt);
10. M. Glet, K. Kaczyński, Signal, SHA1 and certificate pinning, 37th IBIMA Conference, Cordoba, Spain, 30-31.05.2021, (70 pkt);
11. M. Glet, K. Kaczyński, Secure data storage scheme for Android applications, 37th IBIMA Conference, Cordoba, Spain, 30-31.05.2021, (70 pkt);
12. M. Glet, K. Kaczyński, Secure decentralized file storage framework build on IPFS, 38th IBIMA Conference, Seville, Spain, 11.2021, (70 pkt);
13. Glet, M., Kaczyński, K. (2022). NFT-BASED User Authentication Scheme For Mobile APPS, 39th IBIMA Conference, Seville, Spain, 05.2022, (70 pkt);
14. Glet, M., Kaczyński, K., Zielski P., (2023). Hiding Data In Printed Documents, 41th IBIMA Conference, Seville, Spain, 06.2023, (70 pkt);
15. Glet, M., Kaczyński, K., Zielski P., (2023). Watermarking Scheme For Physical Documents, 41th IBIMA Conference, Seville, Spain, 06.2023, (70 pkt);

16. Glet, M., Kaczyński, K., POSTER: One Time Chat – a toy end-to-end encrypted web messaging service. In: , et al. Applied Cryptography and Network Security Workshops. ACNS 2024. Lecture Notes in Computer Science, Springer, (w trakcie publikacji), (70 pkt).