dr hab. inż. Piotr Bilski

Instytut Radioelektroniki i Technik Multimedialnych

Wydział Elektroniki i Technik Informacyjnych

Politechnika Warszawska

Warszawa, dn. 20.06.24

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA ZACHODNIOPOMORSKIEGO UNIWERSYTETU TECHNOLOGICZNEGO W SZCZECINIE

Tytuł rozprawy: Uniwersalny zestaw wskaźników do wykrywania ataków ransomware

Autor rozprawy: mgr inż. Michał Glet

Promotor: prof. zw. dr hab. dr h.c. mult. Brunon Hołyst

Promotor pomocniczy: dr inż. Piotr Bora

1. **Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

Tematem rozprawy doktorskiej jest analiza szkodliwego oprogramowania komputerowego typu ransomware, a w szczególności poszukiwanie skutecznej metody jego detekcji. W efekcie atak przy użyciu takiego programu mógłby zostać zidentyfikowany (również w trakcie trwania procesu), a następnie udaremniony. Jest to tematyka aktualna w ramach informatyki śledczej, a jej znaczenie dla gospodarki oraz bezpieczeństwa państwa rośnie ze względu na rozwój systemów informatycznych w ogóle, a równolegle z nimi – metod atakowania zdalnego systemów komputerowych. Oprogramowanie ransomware jest poważnym problemem ze względu na łatwe i szybkie rozprzestrzenianie się oraz aspekt socjotechniczny (np. phishing) wykorzystywany podczas ładowania i uruchamiania ładunku, co sprawia, że klasyczne systemy typu zapory ogniowe, czy programy antywirusowe nie są w stanie zapobiec atakowi. Autor postanowił przeanalizować znane oprogramowanie typu ransomware w celu zidentyfikowania najważniejszych cech jego struktury oraz sposobów przeprowadzania ataku. W efekcie można byłoby opisać typowy wektor ataku, co znacząco ułatwiłoby obronę przed podobnymi zagrożeniami.

Praca ma charakter teoretyczny, tzn. analizowane są rzeczywiste programy typu malware, jednak efekty tej analizy nie posłużyły do stworzenia systemu detekcji wykorzystywanego w praktyce, a raczej demonstracji właściwości oprogramowania oraz propozycji implementacji oprogramowania obronnego, którego wersja eksperymentalna (działająca w ściśle kontrolowanych warunkach na zwirtualizowanym systemie komputerowym) została zweryfikowana na potrzeby pracy. Autor przeprowadził dość dokładną analizę wybranych rodzajów oprogramowania (zakładam, że korzystał z dostępnych programów) w celu zaproponowania zestawu cech (sygnatur), na podstawie których można byłoby przeprowadzać analizę. Obejmują one zarówno analizę statyczną, jak i dynamiczną, co zwiększa potencjalną użyteczność metody. Można sobie wyobrazić, że na podstawie tej rozprawy powstanie system wyspecjalizowany do wykrywania szkodliwego oprogramowania o ściśle określonej charakterystyce (która może nawet wykraczać poza profil ransomware).

Rozprawa składa się z jedenastu rozdziałów (wliczając w to wstęp oraz podsumowanie). Krytyczne dla jej znaczenia i sensu są rozdziały III-IX (używam numeracji jak w oryginalne), w których opisano szczegóły funkcjonowania oprogramowania ransomware z punktu widzenia działania programu pod kontrolą systemu operacyjnego MS Windows. Opis ten jest szczegółowy, jego zrozumienie wymaga

wiedzy z zakresu systemów operacyjnych oraz programowania systemowego. W rozdziale III przedstawiono szczegóły działania oraz zasady analizy programu Avaddon, jak rozumiem, w celu demonstracji sposobu postępowania odnośnie innych analizowanych obiektów. Rozdział IV zawiera kategoryzację wywołań systemowych systemu operacyjnego MS Windows. W rozdziale V opisano istotę tworzenia pułapek dla programów ransomware w postaci makiet systemu operacyjnego i plików wystawionych w celu przyciągnięcia uwagi atakującego. Rozdziały VI i VII przedstawiają metody analizy plików w celu wykrycia faktu, że doszło do ataku. Rozdziały VIII i IX zawierają opis metod wykrywania obecności złośliwego oprogramowania oraz propozycje Autora odnośnie wskaźników determinujących obecność szkodliwego programu. Rozdziały te są miejscami zbyt obszerne (np. rozdział VIII można było sprowadzić do krótkiego opisu podejścia zastosowanego przez Autora), jednak pozwalają na zorientowanie się, co jest istotą przedstawionego projektu.

W rozprawie sformułowano jedną zasadniczą tezę badawczą oraz cztery szczegółowe (choć w punkcie I.3 zasugerowano, że jest ich pięć). Dotyczą one możliwości zwiększenia bezpieczeństwa systemów komputerowych poprzez analizę oprogramowania uruchamianego pod kontrolą systemu operacyjnego. W szczególności Autor ma na myśli operowanie na przygotowanym przez siebie zestawie wskaźników służących do opisu struktury oraz zachowania programu (poprzez analizę wywoływanie funkcji systemowych, wykorzystywanie określonych bibliotek dołączanych dynamicznie, atakowanie określonych typów plików, wreszcie analizę losowości przetwarzanych danych). Tezy te są skonstruowane poprawnie, jednak moim zdaniem zbyt ogólne. Przede wszystkim, o ile zachowanie oprogramowania malware zapewne wygląda podobnie dla różnych systemów operacyjnych, o tyle Autor udowodnił słuszność swojego postepowania tylko dla systemu operacyjnego MS Windows. Jego wybór jako pola do eksperymentów jest zrozumiały – jest to najpopularniejszy system dla komputerów osobistych (zarówno typu desktop, jak i laptop/notebook), z pominięciem systemów kieszonkowych typu smartfon. Niemniej udział innych systemów w rynku (choć mniejszy), jest niezerowy (chodzi tu głównie o systemy macOS, dystrybucje Linuksa, w znacznie mniejszym stopniu „klasyczne" wersje UNIXa typu AIX, Solaris lub HP-UX, wreszcie Amiga OS). Sposób analizy oprogramowania przedstawiony w rozprawie jest zaś ściśle związany z architekturą systemów MS Windows (konkretnie – Windows 10). W przypadku systemów typu UNIX-like przynajmniej część wskaźników opracowana przez Autora nie będzie mogła być wykorzystana (np. ze względu na zupełnie inną strukturę jądra oraz wywołania systemowe). Z tego powodu uważam, że w tezach powinna być zawarta informacja, że badania zostały ograniczone do konkretnego rodzaju komputerów (architektura x86) i systemów operacyjnych. Podobnie ma się sprawa z tytułem rozprawy, w której znajduje się słowo „uniwersalny". Właśnie ze względu na analizę bardzo konkretnych funkcji systemu MS Windows 10 zestaw ten nie może być uznany za uniwersalny (chyba, żeby rozumieć to jako „pozwalający wykrywać oprogramowanie ransomware dowolnego typu", ale to wymagałoby z kolei istotnego komentarza).

2. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle /świadczący o dostatecznej wiedzy autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Rozprawa zawiera 144 źródła literatury podstawowej oraz 22 uzupełniającej. Te drugie są dość luźno powiązane z tematyką pracy i faktycznie mogą stanowić rozszerzenie wiedzy tu zaprezentowanej. Jeśli chodzi o literaturę podstawową, to pomimo dużej liczby pozycji, w większości przypadków odnoszą się one do dokumentacji technicznej wywołań systemowych, a także tekstów na portalach internetowych. Dodatkowo, Wikipedia pomimo dużej popularności nadal w świecie naukowym nie jest traktowana na podobnym poziomie, jak np. czasopisma z grupy IEEE Transactions… . Udało mi się z przedstawionej listy źródeł wyłowić 17 następujących, typowych dla rozpraw doktorskich: [29], [66], [75], [76], [78], [84], [85], [88], [91], [92],[93], [95], [97], [98], [100], [102], [103]. Na liście występują również odniesienia do projektów programistycznych (np. [34], [87], czy [128]), co w przypadku pracy w dyscyplinie informatycznej jest poprawne. Z kolei w opracowaniu zabrakło odniesień do pewnych źródeł, które dotyczą zagadnień podobnych do przedstawianych w rozprawie, np.:

[1] Subash Poudyal, Kishor Datta Gupta, Sajib Sen, “PEFile Analysis: A Static Approach To Ransomware Analysis,” The International Fournal of Forensic Compter Science (2019), No. 1, pp. 34-39.
[2] K. P. Subedi, D. R. Budhathoki and D. Dasgupta, "Forensic Analysis of Ransomware Families Using Static and Dynamic Analysis," 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2018, pp. 180-185, doi: 10.1109/SPW.2018.00033.
[3] Chen, Q., Islam, S.R., Haswell, H., Bridges, R.A. (2019). Automated Ransomware Behavior Analysis: Pattern Extraction and Early Detection. In: Liu, F., Xu, J., Xu, S., Yung, M. (eds) Science of Cyber Security. SciSec 2019. Lecture Notes in Computer Science(), vol 11933. Springer, Cham. https://doi.org/10.1007/978-3-030-34637-9_15
[4] M. M. Hasan and M. M. Rahman, "RansHunt: A support vector machines based ransomware analysis framework with integrated feature set," 2017 20th International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2017, pp. 1-7, doi: 10.1109/ICCITECHN.2017.8281835.

Analiza baz artykułów naukowych i pozycji konferencyjnych pozwala znaleźć znacznie więcej podobnych opracowań, jednak z rozprawy nie wynika, czy Autor o nich wie oraz czy brał je pod uwagę podczas swoich badań.

Należy podkreślić, że w ramach rozprawy doktorskiej, oprócz przedstawienia własnego rozwiązania, zadaniem Autora jest pokazanie aktualnego stanu wiedzy w określonej dziedzinie. Oprócz wykazania się wiedzą ekspercką, powinien on również podkreślić innowacyjność własnego rozwiązania w kontekście innych, konkurencyjnych systemów. W tym sensie lista publikacji jest znacząca i zawiera istotne źródła (szczególnie te dotyczące szczegółów technicznych), jednak nie pozwala jednoznacznie ocenić oryginalności proponowanego rozwiązania. W zakresie wiedzy naukowej obarczona jest ona zatem niedostatkami, które powinny zostać uzupełnione w przyszłości.

Innym mankamentem opracowania jest całkowity brak odniesienia się do własnych publikacji, co również jest dobrą praktyką w przypadku rozpraw doktorskich. Na podstawie analizy Bazy Wiedzy Wojskowej Akademii Technicznej zlokalizowałem 13 pozycji autorskich, z czego najistotniejsze są dwa artykuły w czasopismach z listy MNiSW oraz cztery publikacje na konferencjach międzynarodowych (te ostatnie związane są ściśle z tematem rozprawy). Zachęcam Autora do cytowania również swoich prac w publikacjach, ponieważ pozwala to ocenić, na ile przedstawiony projekt został zaprezentowany światu naukowemu.

Podsumowując, przegląd literatury jest zdecydowanie niekompletny i choć zawiera istotne dla dziedziny publikacje naukowe oraz źródła techniczne (np. odniesienia do systemu dokumentacji firmy Microsoft), należałoby go uzupełnić (m.in. publikacjami przytoczonymi przeze mnie powyżej).

3. Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Rozprawa doktorska ukierunkowana jest na metodykę wykrywania ataku dokonywanego przez oprogramowanie typu ransomware. Autor skupia się na konkretnym aspekcie jego działania, tj. operacji prowadzących do szyfrowania wybranych plików. Pod uwagę brane są wywołania systemowe, cele szyfrowania (tj. typy plików) oraz konkretne efekty operacji modyfikacji danych. Podstawowymi metodami analizy jest tu inżynieria odwrotna, wymagająca zdekomponowania kodu maszynowego do kodu źródłowego (pod uwagę brane były języki asembler, C oraz C++, które istotnie są głównymi narzędziami tworzenia programów systemowych dla systemu MS Windows). Dzięki temu możliwe jest wyekstrahowanie funkcji systemowych wykorzystywanych przez ransomware. Z drugiej strony analiza post factum plików szyfrowanych przez szkodliwe oprogramowanie może pozwolić odróżnić „standardowe” operacje na danych od tych niewłaściwych, prowadzących do masowego zaszyfrowania dużej liczby plików (w domyśle – w celu zmuszenia użytkownika systemu do skontaktowania się z przestępcą). Na podstawie tej analizy zaproponowane zostały cechy (nazywane przez Autora wskaźnikami), których ewaluacja ilościowa może pomóc w detekcji ataku typu ransomware lub stwierdzenia, że do takowego doszło.

Autor do realizacji postawionych przed sobą celów wykorzystał aparat matematyczny oraz narzędzia informatyczne. W tym pierwszym przypadku wykorzystane zostały dwa zestawy algorytmów dotyczących, odpowiednio, losowości danych oraz kategoryzacji danych. Oba służą do analizy post mortem, tzn. już zrealizowaniu ataku i polegają na określeniu stopnia zmian wprowadzonych w wyniku zaszyfrowania danych w szeregu popularnych plików (m.in. **docx**, **txt**, **csv**, czy **mp4**). Propozycja wykorzystania Entropii, testu Maurera, czy testu monobitowego do oceny zmian wprowadzonych w plikach (domyślnie – odgadnięcia, czy modyfikacje zostały wprowadzone przez oprogramowanie ransomware, czy też jakieś inne, nieszkodliwe) jest ciekawy (choć stosowany wcześniej, np. w Davies SR, Macfarlane R, Buchanan WJ. Comparison of Entropy Calculation Methods for Ransomware Encrypted File Identification. Entropy (Basel). 2022 Oct 21;24(10):1503. doi: 10.3390/e24101503, czy Arroyo, Jan Carlo & Sison, Ariel & Medina, Ruji & Delima, Allemar Jhone. (2022). A Cryptographic Test of Randomness, Entropy, and Brute Force Attack on the Modified Playfair Algorithm with the Novel Dynamic Matrix. 12. 73-83. 10.46338/ijetae0622_11). Jak rozumiem, głównym wkładem Autora jest tutaj porównanie różnych podejść oraz weryfikacja ich przydatności do detekcji ataku.

Drugi aspekt pracy to analiza działania programów ransomware od strony programowania systemowego. Aby dokonać zniszczeń, szkodliwe oprogramowanie musi wykonać szereg operacji dyskowych oraz realizujących operację szyfrowania. W tym celu wywoływane są konkretne funkcje systemowe, które umożliwiają modyfikację zawartości plików. Analiza zachowania szkodliwego oprogramowania jest bardziej uniwersalna od analizy jego struktury, ponieważ umożliwia wykrycie programów polimorficznych modyfikujących w trakcie działania swój kod. Jest to technika powszechnie stosowana w oprogramowaniu (np. antywirusowym) chroniącym system. Inną możliwością mogłoby być zastosowanie metod sztucznej inteligencji w trybie detekcji heurystycznej (na zasadzie wykrywania anomalii), jednak jest to temat na odrębną ścieżkę badań. Autor proponuje połączyć analizę zachowania oprogramowania z zestawem pułapek, które ułatwiają analizę skutków działania monitorowanego oprogramowania (takich jak przynęty, tj. decoy files). Jest to interesujące podejście, które warto było zweryfikować.

4. Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?

Na podstawie lektury rozprawy można określić następujące istotne osiągnięcia Autora oraz jego oryginalny wkład do dziedziny techniki:

- Zaproponowanie unikatowego zestawu wskaźników pozwalających na monitorowanie zachowania każdego oprogramowania działającego pod kontrolą systemu operacyjnego MS Windows. Zestaw ten zawiera parametry znane wcześniej, jednak po raz pierwszy zostały one zebrane jednym podejściu, co pozwala na możliwie pełną analizę oprogramowania podejrzanego o wykonywanie szkodliwych operacji. Wskaźniki te obejmują zarówno analizę zachowania oprogramowania (wywołania systemowe), jak i efektów jego działania w postaci listy plików poddanych działaniu programu i szczegółów ich modyfikacji).
- Weryfikacja zaproponowanej metodyki analizy na zestawie 23 programów typu ransomware, które zostały uruchomione w kontrolowanych warunkach (wewnątrz zwirtualizowanego systemu komputerowego). Lista przetestowanych programów nie jest oczywiście pełna, jednak dostatecznie liczna, aby można było na tej podstawie wyciągać ogólniejsze wnioski. Autor stworzył oprogramowanie służące do analizy wywołań systemowych oraz wykorzystał narzędzia analityczne, co zapewniło stosunkowo wysoką skuteczność zaproponowanej metodyki, pozwalając rozważyć jej zastosowanie w praktyce. Oprócz analizy dokładności detekcji sprawdzono również narzut obliczeniowy, jaki związany jest z działaniem takiego dodatkowego modułu ochronnego. Jest on znaczący, jednak nie na tyle duży, aby eliminować możliwość wykorzystania obok powszechnie używanego oprogramowania ochronnego.

5. Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy?

Jednym z istotnych mankamentów rozprawy jest jej długość. Opracowanie zajmuje 293 strony i jest zdecydowanie zbyt rozległe w stosunku do przedstawianej treści. Pewne fragmenty pracy są wręcz nieistotne i nie powinny znaleźć się w tekście na poziomie doktorskim (czego przykładem jest wprowadzanie definicji danych, systemu komputerowego, systemu teleinformatycznego, czy pliku – są to pojęcia tak podstawowe dla dyscypliny informatyka, że po prostu szkoda na nie miejsca i czasu). Pracę spokojnie można skrócić mniej więcej o połowę, np. pomijając większą część znaczną część rozdziału I i II. Ponadto w pracy znajduje się bardzo duża liczba rozległych tabel, z których tylko część jest istotna. Dobrym przykładem jest tabela w punkcie III.5.2, zawierająca funkcje systemu MS Windows wykorzystywane przez program Avaddon. Nie bardzo rozumiem sens umieszczania długiej listy funkcji systemowych, z których tylko część jest skomentowana. Większość takiej treści można byłoby przedstawić w formie zwięzłego tekstu, tabelę ograniczając tylko do krytycznych funkcji systemowych). Poza tym algorytmy przedstawione w punktach VII.1.1 oraz VII.1.2 mają pewne części wspólne, których nie trzeba powtarzać, oszczędzając w ten sposób kolejną stronę (w tym celu należałoby jednak numerować równania). Opisy testów z rozdziału VI są momentami niejasne.. W przypadku Entropii nie wyjaśniono dokładnie, jak jej definicja ma się do obliczanych wartości dla zaszyfrowanego bajtu (tutaj przydałby się przykład obliczeniowy).

Opracowanie obarczone jest szeregiem usterek redakcyjnych, z których najistotniejsze to:

a. Brak numeracji równań, co uniemożliwia np. odnoszenie się do nich z różnych fragmentów tekstu. Dodatkowo pewne symbole użyte są w nich niewłaściwie, np. symbol „*” nie oznacza mnożenia, a splot (należałoby użyć symbolu kropki: „·”).
b. Brak numeracji i tytułów dla tabel, do których również można byłoby się odnosić w tekście.
c. Używanie określeń slangowych, które mogą być zastąpione polskimi odpowiednikami, np. „hook’i” to „uchwyty”.
d. Drobne usterki typu literówki (np. „ziemną” na str. 162 lub „niewyrycia” na str. 183) nie utrudniają zasadniczo zrozumienia tekstu, jednak czasami odwracają uwagę od istoty rzeczy.

Pomimo tych drobnych niedociągnięć, pracę czyta się dobrze i nie ma większych problemów ze zrozumieniem treści.

6. Uwagi krytyczne

Treść zawarta w pracy jest zrozumiała i pozwala docenić wysiłek Autora włożony w badania nad oprogramowaniem typu ransomware oraz podjęcie próby zbudowania wiedzy na temat jego zachowania, co może przyczynić się do zwiększenia bezpieczeństwa w systemach teleinformatycznych. Niemniej lektura poszczególnych rozdziałów rodzi szereg pytań i wątpliwości, z których najistotniejsze przedstawiam poniżej.

- Stworzone oprogramowanie działa pod kontrolą systemu operacyjnego MS Windows 10 (z tekstu wynika, że jest to wersja 64-bitowa). Systemy tego typu potrafią obsługiwać obecnie kod 64- oraz 32-bitowy. Autor (być może ze względu na brak czasu) pominął inne systemy, np. wcześniejsze wersje typu Windows 7 lub Windows 8, ale również systemy serwerowe typu MS Windows Server 2018. Z tego względu trudno ocenić, w jakim stopniu zastosowana technika będzie uniwersalna, szczególnie że firma Microsoft dość intensywnie modyfikuje nie tylko jądro pomiędzy kolejnymi wersjami systemu, ale również wywołaniami systemowymi (zawartość plików DLL).
- Ta uwaga powiązana jest z poprzednią. W literaturze analizowane są osobno programy typu malware dla platform mobilnych (tj. dla systemów iOS oraz Android). W jaki sposób wnioski przedstawione w rozprawie mają się do takich systemów?
- Rozdział III zawiera analizę oprogramowania Avaddon, jednak nie jest wyjaśnione, jaką rolę pełni ten fragment. Czy chodzi o zademonstrowanie działania typowego programu typu

ransomware oraz technik jego analizy, która potem została wykorzystana do analizy innych przypadków? Wątpliwość jest o tyle zasadna, że w dalszej części tekstu analizowane jest inne oprogramowanie tego typu, natomiast do Avaddon się już nie wraca.

- Jednym ze wskaźników jest zwracanie uwagi na wykorzystanie mniej popularnych wywołań systemowych (na zasadzie detekcji anomalii). Autor nie wyjaśnia jednak, co rozumie przesz to pojęcie oraz na jakiej podstawie ocenia, czy dane wywołanie systemowe jest typowe, czy nie. Jest to o tyle istotne, że określenie „nietypowych" wywołań jest miękkie i prawdopodobnie wymaga szerokiej analizy statystycznej nie tylko programów typu ransomware, ale także wszystkich innych, uruchamianych w systemie.
- Wiele z przedstawionych wskaźników (rozdział IX.6) zawiera wymaganie przekroczenia poziomu wartości progowej (w celu podjęcia decyzji, że jest to malware lub przynajmniej przyjęcia ostrzeżenia, że program jest podejrzany i powinien zostać objęty obserwacją). Autor nie podaje jednak, jakie są wartości progowe przyjęte przez niego i wykorzystane podczas eksperymentów. Domyślać się należy, że wartości progowe mają istotne znaczenie dla możliwości detekcji (lub nie) konkretnego programu ransomware, zaś ich dobór stanowi osobne zagadnienie badawcze.
- W dziedzinie, w której porusza się Autor powszechne jest obecnie stosowanie metod sztucznej inteligencji. Odnosi się on na poziomie ogólnym do tego zagadnienia, wspominając o podobnych podejściach. Rodzi to pytanie, jak ma się zaproponowane podejście do metod sztucznej inteligencji (szczególnie działających w warunkach niepewności danych, np. maszyn wektorów nośnych)?
- W rozdziale VIII Autor przedstawia różne techniki wykrywania programów typu ransomware, rozróżniając podejścia heurystyczne oraz wykorzystujące sztuczną inteligencję. Czy obie te grupy istotnie są na tyle różne, że uzasadnia to traktowanie ich osobno? Większość znanych mi podejść heurystycznych wykorzystuje (w jakiś sposób) algorytmy sztucznej inteligencji.
- Autor zaproponował szereg różnorodnych wskaźników do wykrywania programów ransomware. Powstaje jednak pytanie, wszystkie są one niezbędne? Na podstawie analizy zależności pomiędzy parametrami być może udałoby się zlokalizować cechy nadmiarowe, a przez to niepotrzebne. Jest to o tyle istotne, że oprogramowanie wykorzystane przez Autora podczas eksperymentów jest znacząco obciążające dla systemu komputerowego i można byłoby spróbować je zminimalizować np. poprzez zmniejszenie ilości przetwarzanych danych.
- Program typu ransomware atakuje określone rodzaje plików. Jak wynika z analizy, celem są najpopularniejsze typy określonych plików tekstowych, graficznych, dźwiękowych itp. Czy jedną z metod obrony przed takim intruzem może być wykorzystywanie wyłącznie miej typowych standardów (np. **odt** zamiast **docx**)?

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Przedstawiona rozprawa doktorska jest interesującym opracowaniem na temat konkretnego rodzaju szkodliwego oprogramowania, tj. ransomware. Oprócz ogólnego opisu i technicznej charakterystyki tego typu aplikacji Autor przedstawił konkretną propozycję budowy systemu detekcji tego typu zagrożeń. Nie jest to implementacja na poziomie prototypu, lecz kilka osobnych podejść, które w praktyce mogą zostać zintegrowane w postaci jednego, spójnego programu. Pomimo pewnych (zauważalnych) mankamentów treść pracy zawiera wskazanie oryginalnych rozwiązań w zakresie zapewnienia bezpieczeństwa i odporności na ataki programów typu ransomware. Techniki zaproponowane w postaci wskaźników dotyczących zachowania oprogramowania oraz efektów jego działania są zrozumiałe, a ich przydatność – udowodniona eksperymentalnie, choć należy podkreślić, że dotyczy to jednego, konkretnego systemu operacyjnego oraz wybranego zestawu programów.

Ogólny poziom pracy, pomimo wymienionych niedostatków jest akceptowalny. Na podstawie dostarczonego tekstu można zatem uznać, że Autor wykazał się wymaganą wiedzą oraz

kompetencjami dla osób posiadających stopień doktora nauk technicznych. Z wymienionych powodów oceniam, że opiniowana praca doktorska Pana mgr. inż. Michała Gleta spełnia wymagania stawiane rozprawom doktorskim, określonym w artykule 187 ust. 1 i ust. 2 Ustawy z dnia 20 lipca 2018 roku Prawo o Szkolnictwie Wyższym i Nauce (Dz.U. z 2018 poz. 1668 z późn. zm.) i wnoszę o dopuszczenie jej do publicznej obrony.