dr hab. inż. Jerzy Kosiński, prof. AMW
Wydział Dowodzenia i Operacji Morskich
Akademia Marynarki Wojennej w Gdyni

Szczytno, dn. 20 czerwca 2024 roku

RECENZJA

rozprawy doktorskiej mgra Michała Gleta pt.:

UNIWERSALNY ZESTAW WSKAŹNIKÓW DO WYKRYWANIA ATAKÓW RANSOMWARE

przygotowanej pod kierunkiem naukowym prof. dr. hab. Brunona Hołysta

Podstawą napisania recenzji jest Uchwała z dnia 21 maja 2024 r. Rady Dyscypliny Informatyka techniczna i telekomunikacja Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie w sprawie powołania recenzentów w przewodzie doktorskim Pana mgra Tomasza Kulczyk Michała Gleta

1. Ocena wstępna

Obserwując statystyki cyberprzestępczości przedstawiane przez organa ścigania (np. Europol, IC3 FBI) lub firmy informatyczne (np. Sophos) można wyraźnie zauważyć, że w ostatnich latach dominującym cyberzagrożeniem jest ransomware. Szczególnie dobrze jest to widoczne, kiedy bierze się pod uwagę straty wynikające z tych ataków. Zapłacone kwoty okupów, pamiętając o zaleceniach lub zakazach ich płacenia, nie są jedynym kosztem ponoszonym przez ofiary. Znacznie większe są koszty utraty możliwości działania i przywrócenia stanu sprzed ataku. Do tego dochodzą niewymierne koszty społeczne, w tym te najdotkliwsze – utraty życia ludzkiego (atak na szpital w Stutgarcie). Zmiany w sposobie realizacji tych ataków, z jednej strony ataki ukierunkowane na wybrane, wypłacalne ofiary, a z drugiej ataki typu

Ransomware as a Servis, sprawiają, że przestępcy widzą swoje „biznesowe" korzyści i potencjalną bezkarność. Niestety, również te zmiany sprawiają, że ofiary mają mniejsze możliwości obrony przed atakiem.

Biorąc powyższe pod uwagę, należy uznać, że opracowanie zestawu wskaźników wykrywania ataków ransomware, prawie zupełnie nie analizowane pod względem naukowym, stanowi także duże wyzwanie pod względem praktycznym. Określenie wskaźników może być wykorzystane, poprzez lepsze zrozumienie funkcjonalności ransomware, zarówno do poprawy bezpieczeństwa użytkowników, jak i do ograniczenia zagrożenia ransomwarem.

W powyższym kontekście, rozprawa Pana mgra Michała Gleta powinna być postrzegana bardzo pozytywnie. Autor rozprawy za przedmiot swoich badań przyjął: bezpieczeństwo danych w kontekście ataków z wykorzystaniem oprogramowania typu ransomware, przekładające się na bezpieczeństwo w ujęciu jednostki, społeczeństwa, jaki i państwa (s.18).

Tak sformułowany przedmiot badania świadczy dobrze o świadomości Doktoranta problematycznych kwestii dotyczących aktualnych cyberzagrożeń w kontekście podnoszenia poziomu bezpieczeństwa państwa i obywateli.

Główny problem badawczy rozprawy zawarty jest w pytaniu:

w jaki sposób zwiększyć poziom bezpieczeństwa państwa, społeczeństwa oraz jednostki w kontekście ataków z wykorzystaniem oprogramowania typu ransomware? (str. 19).

Autor dysertacji rozbudował główny problem badawczy tworząc 5 problemów szczegółowych:

1. *Jakie cechy charakterystyczne posiada oprogramowanie typu ransomware?*
2. *Jaki wpływ mają najczęściej używane mechanizmy bezpieczeństwa na wykrywanie aktywności oprogramowania typu ransomware?*
3. *Jaki wpływ ma oprogramowanie typu ransomware na systemy tworzenia kopii bezpieczeństwa?*
4. *Jak można wykrywać, bazując na określonych wcześniej cechach charakterystycznych, aktywność oprogramowania typu ransomware?*
5. *Z jakich komponentów ma się składać i w jaki sposób ma działać mechanizm bezpieczeństwa umożliwiający wczesne wykrywanie ataków z wykorzystaniem oprogramowania ransomware?*

Na podstawie dotychczasowej wiedzy i wstępnej obserwacji Autor dysertacji sformułował główną hipotezę w postaci:

Opracowane autorskie wskaźniki wykrywania ataków typu ransomware zwiększą poziom bezpieczeństwa danych w ujęciu bezpieczeństwa jednostki, społeczeństwa oraz państwa (s.19)

oraz 4 hipotezy szczegółowe:

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

aktywności złośliwego oprogramowania typu ransomware.

4. Wykorzystanie mechanizmów badania poziomu losowości danych umożliwi wykrycie aktywności złośliwego oprogramowania typu ransomware.

Hipotezy 1 (pomijając zapisaną potoczą niezręczność – wirus ransomware) i 2 odpowiadają problemom badawczym 1 i 2. Hipotezy 3 i 4 odpowiadają problemom 4 i 5. Brak hipotezy dla problemu szczegółowego 3. Doktorant w pracy nie odniósł się do tego problemu – i słusznie, gdyż jest to źle sformułowany problem (za to identycznie dwukrotnie zwraca uwagę na wagę kopii zapasowej s.43 i 47).

W celu weryfikacji przedstawionych hipotez Doktorant wykorzystał kilka metod badawczych: badanie dokumentów, analiza i krytyka piśmiennictwa, formalno-dogmatyczna, dedukcja, wnioskowanie. Wykorzystał również metody projektowania systemów informatycznych.

Wszystkie hipotezy robocze zostały pozytywnie zweryfikowane, co Doktorant jawnie potwierdził w rozdziale X, ale także we podsumowaniach rozdziałów V, VI, VII, IX.

Celem badania było stworzenie autorskiej koncepcji mechanizmu, umożliwiającego wykrywanie ataków z wykorzystaniem oprogramowania typu ransomware (s.18).

W sensie pragmatycznym do celu badań należało:

1. Opracowanie, na podstawie przeprowadzonych analiz próbek oprogramowania ransomware, wskaźników detekcyjnych ransomware.

2. Umożliwienie wykrywania aktywności nowych, wcześniej nieznanych, wersji ransomware.

Zarówno postawione problemy badawcze, jak i sformułowane hipotezy badawcze są adekwatne do tematu, przyjętego celu pracy i przedmiotu badań.

Przyjęty w pracy schemat postępowania badawczego odpowiednio kierunkował wysiłek Doktoranta na realizację celu pracy.

W kontekście całości pracy należy zwrócić uwagę na praktyczne wykorzystanie metod typowych dla projektowania systemów informatycznych.

Praca została napisana językiem poprawnym z niewielką ilością błędów (głównie stylistyczne – interpunkcja, wszystkie wyliczenia z dużej litery), chociaż zdarzają się również pojedyncze zapisy nieprecyzyjne (np. ładunkiem jest wersja binarna wirusa (s.15), wiper jako odmiana ransomware (s.41); bezpieczeństwo, ataki, incydenty cybernetyczne; phishing i obok socjotechnika (s.50)). Brak numeracji i tytułów tabel, uniemożliwiający precyzyjne wskazanie i powodujący nadużywanie określeń powyżej/poniżej.

Rozdziały i podrozdziały, ich tematyka i następstwo, tworzą logiczną całość.

Niemniej jednak recenzowana rozprawa stanowi istotny wkład w rozwój badań w obszarach informatyki technicznej i nauk społecznych.

2. Zawartość rozprawy

Dysertacja Pana mgra Michała Gleta liczy ogółem 268 stron tekstu, 10 stron bibliografii z netografią (144 poz., w tym 24 poz. Wikipedia, 25 poz. Malpedia) oraz 22 pozycjami literatury uzupełniającej, spis rysunków i kodów źródłowych. Wykorzystana w pracy literatura przedmiotu, nie jest zbyt

obszerna, co więcej, wskazane w bibliografii źródła często mają charakter wtórny (24 razy przywołana Wikipedia).

Podstawowy tekst rozprawy składa się z jedenastu rozdziałów, przy czym pierwszy rozdział jest rozdziałem metodycznym, a dwa ostatnie należy traktować jak podsumowanie pracy. W ośmiu rozdziałach merytorycznych Doktorant zawarł treści odpowiadające szczegółowym problemom badawczym.

W pierwszym rozdziale pt. Uzasadnienie wyboru tematu badań (ss.12-22) Autor opisał przedmiot i cele badań. Sformułował problem badawczy (główny i 5 szczegółowych) i hipotezy robocze (1 główna i 4 szczegółowe). Bardzo ogólnie przedstawił zakres badań, wykorzystane metody i techniki badawcze oraz aktualny stan badań. W zakończeniu wskazał ograniczenie badawcze wynikające z brakiem wiarygodnych opracowań naukowych z podejmowanegozakresu.

W drugim rozdziale pt. Oprogramowanie ransomware (ss.23-76) Doktorant opisuje podstawowe pojęcia wykorzystywane w pracy. Przedstawia definicję i klasyfikację malware. Zwraca uwagę na rozprzestrzenianie się ransomware i fazy jego ataku. Opisuje rys historyczny, statystyki i zagrożenia wynikające z wykorzystania ransomware, także w formule Ransomware as a service. Do tego rozdział można mieć kilka zastrzeżeń, o których wyjaśnienie prosiłbym w czasie obrony:

1. Przedstawione na s.49 fazy ataku wychodzą poza atak – dlaczego nie wykorzystano standardowych w takich opisach Cyber Kill Chain, Mitre ATT&CK lub modelu diamentowego?
2. Jakie były źródła statystyk z rozdz. II.8.6?

3. Czy zalecenie zawarte w 3 ostatnich zdaniach na stronie 54 znajdują potwierdzenie w działaniach cyberprzestępców, np. grupy Conti?

W trzecim rozdziale pt. Analiza ransomware Avaddon (ss.76-114) opisana została wykonana analiza statyczna i dynamiczna tego narzędzia, wzbogacona o analizę kodu, co pozwoliło na opisanie budowy i sposobu działania (w tym rozprzestrzeniania) ransomware.

W czwartym rozdziale pt. Wywołania funkcji API (ss.115-140) Doktorant opisał zbadane wykorzystywanie, przez badane typy ransomware (9), wywołań funkcji API systemu Windows. Pozwoliło to na podział funkcji API na kategorie o zróżnicowanej częstości wywołań i istotności. Niestety w pracy zabrakło wskazania funkcji API ze względu na istotność. Proszę o uzupełnienie na obronie tego braku, przynajmniej w kategorii funkcje API niebezpieczne (domyślnie są to funkcje wskazane w rozdziale IX).

W rozdziale piątym pt. Pułapki typu honeypot (ss.141-151) Doktorant p możliwość wykorzystania mechanizmu honeypot z decoy files do wykrywania ataku ransomware.

W rozdziale szóstym pt. Badanie losowości danych (ss.152-170) Autor wskazał możliwości oceny zmian zachodzących w pliku za pomocą testu Mauera, entropii Shanona oraz testu monobitowego. Zaprezentował także wyniki wykorzystania tych testów w kontekście pełnego i częściowego szyfrowania różnych plików przez 8 typów ransomware.

W rozdziale siódmym pt. Kategoryzacja danych (ss.171-182) Doktorant opisał możliwości technik LSH i LPH używanych w analizie danych do wyszukiwania podobnych elementów. Zaprezentował także wyniki

wykorzystania 4 algorytmów sprawdzania podobieństw między sekwencjami danych na różnych typach plików.

W rozdziale ósmym pt. Wybrane metody wykrywania złośliwego oprogramowania (ss.183-189) Doktorant opisał pięć metod (analizy sygnatur, analizy zachowania, heurystyczne, modelowania, bazujące na uczeniu maszynowym oraz sztucznej inteligencji) wykrywania złośliwego oprogramowania.

Rozdział dziewiąty pt. Autorskie wskaźniki wykrywania aktywności Ransomware (ss.189-273) jest opisem dziewięciu zaproponowanych przez Doktoranta wskaźników wraz z propozycją metod technicznych ich implementacji. Opis jest uzupełniony wynikami testów działania zaproponowanych wskaźników, ich efektywności oraz reakcji typu „false positive". Po lekturze tego rozdziału nasuwa się pytanie: jaki jest poziom wykrycia aktywnego ataku ransomware z wykorzystaniem zaproponowanych wskaźników, zmierzony tylko dla 14 typów ransomware, które nie były analizowane podczas realizacji prac nad wskaźnikami?

W rozdziale X pt. Weryfikacja hipotez badawczych (ss.274-276) Doktorant w sposób bezpośredni odniósł się do weryfikacji, na podstawie przeprowadzonych testów, postawionych hipotez badawczych.

W rozdziale XI pt. Podsumowanie (ss.277-279) Doktorant podsumował całość rozprawy podkreślając, że osiągnięto założony cel. Jednocześnie zaproponował dalsze działania.

Całość pracy jest przedstawiona interesującym i zrozumiałym językiem. Przeprowadzone badania i przedstawione wnioski świadczą o dojrzałości naukowej kandydata do stopnia doktora.

3. Ocena merytoryczna dysertacji

Doktorant poddał wnikliwej analizie problem badawczy, odpowiadając na postawione pytania i weryfikując założone hipotezy. Określenie problemu badawczego, opis celów i uwarunkowań danego problemu zawarte w rozdziałach 2-8, zostały przedstawione na tyle szczegółowo, aby można było odpowiednio zaplanować badanie. Należy stwierdzić, że układ rozdziałów i podrozdziałów jest logicznie uzasadniony i hierarchicznie uporządkowany, tytuły i podtytuły dokładnie określają zakres merytoryczny i odpowiadają zawartej w nich treści. Treści kolejnych rozdziałów i podrozdziałów wynikają z postawionych problemów badawczych i poprzedzających je rozważań. W pracy udokumentowano przeprowadzone przez Doktoranta badania, zarówno nad koncepcją wskaźników, jak i nad weryfikacją ich poprawności.

W nawiązaniu do rozważań szczegółowych warto podkreślić, że recenzowana praca jest oryginalnym rozwiązaniem problemu naukowego i stanowi cenną inspirację do dalszej naukowej dyskusji, w jaki sposób poprawić skuteczność wykrywania ataków ransomware, a tym samym bezpieczeństwo jednostki, społeczeństwa, jaki i państwa.

W pracy występują incydentalne błędy redakcyjne, które nie obniżają wartości recenzowanej pracy.

Reasumując: uznaję, że dysertacja pt.: „Uniwersalny zestaw wskaźników do wykrywania ataków ransomware” s**pełnia wszystkie wymogi formalne i merytoryczne** określone w art. 187 Ustawy z dnia 20 lipca 2018 r., Prawo o szkolnictwie wyższym i nauce i **wnioskuję o dopuszczenie Pana mgra Michała Gleta do publicznej obrony doktoratu**.

PODPIS ZAUFANY
JERZY
KOSIŃSKI
20.06.2024 17:07:53 [GMT+2]
Dokument podpisany elektronicznie
podpisem zaufanym