dr inż. Krzysztof Cabaj
Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych
Instytut Informatyki

Analiza i przeciwdziałanie atakom sieciowym ze szczególnym uwzględnieniem złośliwego oprogramowania

Autoreferat

1 Dane osobowe i przebieg zatrudnienia w jednostkach naukowych

1.1 Imię i Nazwisko

Krzysztof Cabaj

1.2 Posiadane dyplomy, stopnie naukowe - z podaniem nazwy, miejsca i roku ich uzyskania

2010 – doktor nauk technicznych w dziedzinie informatyki, Wydział Elektroniki i Technik Informacyjnych, Politechniki Warszawskiej

2004 – mgr inż. informatyki, Wydział Elektroniki i Technik Informacyjnych, Politechniki Warszawskiej

1.3 Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych

od 01.2010 - adiunkt w Instytucie Informatyki, Wydział Elektroniki i Technik Informacyjnych, Politechniki Warszawskiej

od 03.2009 do 12.2009 - asystent w Instytucie Informatyki, Wydział Elektroniki i Technik Informacyjnych, Politechniki Warszawskiej

2 Tytuł osiągnięcia naukowego

Jako osiągnięcie naukowe uzyskane po otrzymaniu stopnia doktora, stanowiące znaczny wkład autora w rozwój dyscypliny naukowej, wskazuję cykl publikacji powiązanych tematycznie zatytułowany "***Analiza i przeciwdziałanie atakom sieciowym ze szczególnym uwzględnieniem złośliwego oprogramowania***". W skład osiągnięcia wchodzą publikacje [C1- C10]. Każda publikacja jest scharakteryzowana poprzez liczbę punktów MNiSW wg zasad punktacji obowiązujących do roku 2018. Przy publikacjach z listy JCR podana jest wartość współczynnika IF w momencie publikacji.

3 Wykaz publikacji stanowiących osiągnięcie naukowe

Lista publikacji ułożona jest zgodnie z kolejnością występowania w dalszej części opisu.

[C1] Cabaj Krzysztof, Denis Marek, Buda Michał: Management and Analytical Software for Data Gathered from HoneyPot System, w: Information Systems in Management, WULS Press Warsaw, vol. 2, nr 3, 2013, ss. **5 punktów MNiSW**

Moim wkładem było opracowanie koncepcji systemu typu HoneyPot (system WebHP) oraz systemów analizy danych uzyskanych z systemów HoneyPot (systemy Miner i HPMS), nadzór nad implementacją, analiza i opracowanie uzyskanych danych oraz przygotowanie tekstu artykułu. Mój udział szacuję na 70%.

[C2] Cabaj Krzysztof, Gawkowski Piotr: HoneyPot systems in practice, w: Przegląd Elektrotechniczny, SigmaNOT, vol. 91, nr 2, 2015, ss. 63-67, DOI:10.15199/48.2015.02.16, **14 punktów MNiSW**

Moim wkładem było opracowanie koncepcji rozwoju systemów HoneyPot WebHP oraz HeartBleadHP, nadzór nad ich implementacją, analiza i opracowanie pozyskanych z tych systemów danych oraz przygotowanie tekstu artykułu. Mój udział szacuję na 80%.

[C3] Cabaj Krzysztof, Grochowski Konrad, Gawkowski Piotr: Practical Problems of Internet Threats Analyses, w: Theory and Engineering of Complex Systems and Dependability. Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX / Zamojski Wojciech [i in.] (red.), Advances in Intelligent Systems and Computing, vol. 365, 2015, Springer International Publishing, ISBN 978-3-319-19215-4, ss. 87-96, DOI:10.1007/978-3-319-19216-1_9, **15 punktów MNiSW**

Moim wkładem było wykrycie aktywności związanej z propagacją rodziny robaków wykorzystujących podatność Shellshock, obserwowanej w danych uzyskanych z systemu WebHP, wstępna analiza zagrożenia, analiza i opracowanie uzyskanych danych oraz przygotowanie fragmentów tekstu artykułu. Mój udział szacuję na 70%.

[C4] Buda Michał, Cabaj Krzysztof: Metody eksploracji danych w analizie ruchu obserwowanego przez system HoneyPot, w: Studia Bezpieczeństwa Narodowego, vol. 4, nr 6, 2014, ss. 325-339, **6 punktów MNiSW**

Moim wkładem było opracowanie koncepcji wykorzystania algorytmów eksploracji danych wykrywających zbiory częste do analizy logów z systemu WebHP, nadzór nad implementacją modułu systemu HPMS realizującego zaproponowane algorytmy, analiza danych i finalne opracowanie wyników oraz przygotowanie tekstu artykułu. Mój udział szacuję na 80%.

[C5] Cabaj Krzysztof, Gawkowski Piotr, Grochowski Konrad [i in.] : Network activity analysis of CryptoWall ransomware, w: Przegląd Elektrotechniczny, Sigma NOT, vol. 91, nr 11, 2015, ss. 201-204, DOI:10.15199, **14 punktów MNiSW**

Moim wkładem było opracowanie koncepcji systemu dynamicznej analizy złośliwego oprogramowania o nazwie Maltester, nadzór nad jego implementacją, wstępna analiza sposobu działania próbek złośliwego oprogramowania rodziny CryptowWall, analiza i opracowanie uzyskanych danych oraz przygotowanie tekstu artykułu. Mój udział szacuję na 60%.

[C6] Cabaj Krzysztof, Gawkowski Piotr, Grochowski Konrad, Amadeusz Kosik: Developing malware evaluation infrastructure, w: Proceedings of the 2016 Federated Conference on Computer Science and Information Systems / Ganzha Maria, Maciaszek Leszek A., Paprzycki Marcin (red.

), Annals of Computer Science and Information Systems, vol.8, 2016, IEEE, ISBN 978-83-60810-90-3, ss. 981-898, **15 punktów MNiSW**

Moim wkładem był nadzór merytoryczny nad opracowaniem koncepcji systemu dynamicznej analizy MESS, dalsze analizy sposobu działania próbek złośliwego oprogramowania rodziny CryptowWall, analiza aktywności serwerów proxy wykorzystywanych przez atakujących, analiza i opracowanie uzyskanych danych oraz przygotowanie tekstu artykułu. Mój udział szacuję na 60%.

[C7] Cabaj Krzysztof: Management System for Dynamic Analysis of Malicious Software, w: Information Systems in Management, vol. 5, nr 4, 2016, ss. 473-480, **5 punktów MNiSW**

[C8] Cabaj Krzysztof, Mazurczyk Wojciech: Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall, w: IEEE Network, vol. 30, nr 6, 2016, ss. 14-20, DOI:10.1109/MNET.2016.1600110NM, **45 punktów MNiSW, IF=7,23**

Moim wkładem było opracowanie metody blokowania komunikacji pomiędzy ofiarą a serwerami sterującymi (Command and Control - C&C), implementacja aplikacji SDN, która ją realizowała, wykonanie dynamicznej analizy zebranych próbek złośliwego oprogramowania rodziny CryptoWall na potrzeby eksperymentów oraz przygotowanie fragmentów tekstu artykułu. Mój udział szacuję na 80%.

[C9] Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech: Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics, w: Computers & Electrical Engineering, vol. online 27 October 2017, 2017, ss. 1-16, DOI:10.1016/j.compeleceng.2017.10.012, **20 punktów MNiSW, IF=1,57**

Moim wkładem było opracowanie metod wykrywania komunikacji do serwerów sterujących C&C wykorzystywanych przez złośliwe oprogramowanie, implementacja programu dokonującego detekcji, wykonanie eksperymentów oraz przygotowanie fragmentów tekstu artykułu. Mój udział szacuję na 50%.

[C10] Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech, Piotr Nowakowski, Piotr Żórawski: Network Threats Mitigation Using Software-Defined Networking for the 5G Internet of Radio Light System, w: Security and Communication Networks, vol. 2019, 2019, ss. 1-22, DOI:10.1155/2019/4930908 , **20 punktów MNiSW, IF = 0,904**

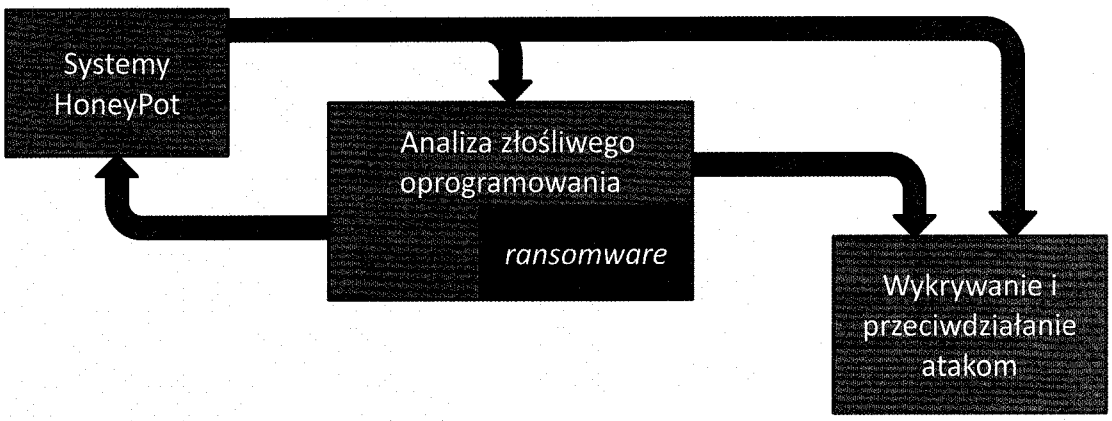
Moim wkładem było opracowanie koncepcji detekcji skanowań i ich blokowania, nadzór nad implementacją, opracowanie koncepcji eksperymentów oraz przygotowanie tekstu artykułu. Mój udział szacuję na 40%.

3.1 Opis osiągnięcia naukowego

Badania związane z analizą zagrożeń sieciowych, w tym złośliwego kodu, są zbliżone do działań podejmowanych w ramach tzw. *białego wywiadu*, czy szeroko rozumianych procedur OSINT (ang. *Open-source Inteligence*). Osoby zajmujące się analizą nie mają bezpośredniego dostępu do atakujących i tylko na podstawie ogólnie dostępnych danych i informacji mogą prowadzić swoje analizy. Stąd nawet tak podstawowa cecha badanej próbki jak nazwa rodziny

złośliwego oprogramowania, do której należy nie jest w żaden sposób uzgadniana. W efekcie skutkuje to wprowadzaniem dodatkowych nieścisłości, ponieważ to same zagrożenie jest znane pod różnymi określeniami. Dużym problemem jest także zdobycie aktualnych próbek złośliwego oprogramowania, czy plików zawierających ruchu sieciowy generowany w ramach przeprowadzania nowych ataków. W większości przypadków jest to bardzo czasochłonny proces, będący integralną częścią prowadzonych analiz. Dodatkowo, w ramach tego typu badań. obserwujemy tak zwany wyścig zbrojeń (ang. *arms race*). Atakujący bardzo dokładnie śledzą szeroko publikowane wyniki analiz i na ich podstawie modyfikują swoje działania tak, aby uniemożliwić lub choćby poważnie utrudnić prace zmierzające do poznania nowych zagrożeń i opracowania nowych metod obrony. W związku z tym, mimo opracowanych wcześniej metodologii prowadzenia analiz, muszą być one stale modyfikowane, aby uwzględnić aktualny sposób działania atakujących.

Przedstawione osiągnięcie naukowe dotyczy tematyki bezpieczeństwa komputerowego i jest podsumowaniem moich prac prowadzonych od 2013 do 2018 roku. W tym czasie prowadziłem badania naukowe w trzech głównych nurtach dotyczących: ***(i)* systemów HoneyPot, *(ii)* analizy złośliwego oprogramowania** oraz ***(iii)* wykrywania i przeciwdziałania atakom sieciowym**. Prowadzone badania były ściśle skorelowane, a wyniki z jednego obszaru wpływały na dalsze prace prowadzone w innych obszarach. Przykładowo, dane, próbki złośliwego oprogramowania, uzyskane w ramach obsługi wdrożonych systemów HoneyPot podlegały analizie, a następnie na ich podstawie modyfikowałem systemy HoneyPot w celu reakcji na taktykę stosowaną w nowych zagrożeniach. Dodatkowo, w ramach prowadzonych przeze mnie prac związanych z analizą złośliwego oprogramowania, należy wyróżnić istotny podobszar związany z badaniem zagrożeń typu ransomware. Rysunek 1 przedstawia graficznie obszary prowadzonych przeze mnie badań naukowych wraz z występującymi między nimi powiązaniami.



Rysunek 1 Obszary naukowe wchodzące w skład osiągnięcia wraz z wzajemnymi relacjami.

1. *Systemy HoneyPot*

Głównym problemem badawczym w tym obszarze był brak ogólnie dostępnych, a także aktualnych danych dotyczących ataków sieciowych. Pierwsze moje prace dotyczące analizy ataków sieciowych wiązały się z uruchomieniem w sieci Instytutu Informatyki różnych systemów HoneyPot, między innymi systemów Nepenthes i Dionae. Zebrane w ten sposób dane podlegały analizie. W toku tych prac przeanalizowane zostały dokładnie metody rozprzestrzeniania się kilku zagrożeń, między innymi robaków, których celem były urządzenia firm Synology i QNAP oraz

masowe włamania wykorzystujące błąd w aplikacji do systemu PhpMyAdmin. Wraz ze zdobywaniem większej wiedzy na temat charakteru ataków, odpowiadałem za przygotowanie kolejnych systemów pozwalających na zbieranie coraz pełniejszego spektrum danych - systemy WebHP i HPMS (ang. HoneyPot Management System), kończąc na próbkach złośliwego oprogramowania. Wyniki badań zostały opublikowane w artykułach [C1-C7].

2. *Analiza złośliwego oprogramowania*

Dalsze moje prace polegały na analizie sposobu działania próbek złośliwego oprogramowania zebranych w nadzorowanych przeze mnie systemach HoneyPot. Ze względu na czas potrzebny na analizę pojedynczej próbki oraz stosowane techniki zaciemiania kodu i mechanizmy przeciwdziałania analizie odwrotnej skupiłem się na dynamicznych metodach analizy, które polegają na uruchomieniu jej w kontrolowanym środowisku. W ramach prac dyplomowych prowadzonych w Instytucie Informatyki, pod moją opieką i z moją pomocą powstały systemy Maltester i MESS (ang. Malware Evaluation Support System). Systemy te umożliwiły przeprowadzanie dalszych, pogłębionych analiz nowych zagrożeń. W ramach badań dotyczących analizy złośliwego oprogramowania, należy wyróżnić dość znaczny wkład prac związanych z analizą zagrożeń klasy *ransomware.* W ramach prowadzonych prac związanych z analizą powłamaniową, jednej z wydziałowych maszyn uzyskałem próbkę złośliwego oprogramowania. Pobraną podczas tego procesu próbkę przeanalizowałem z wykorzystaniem wdrożonych przeze mnie w Instytucie Informatyki systemów do dynamicznej analizy złośliwego oprogramowania. Ciekawe zachowanie sieciowe skłoniło mnie do dalszych prac, w ramach których przez ponad rok analizowałem różne zagrożenia rodzin CryptoWall i Locky. W rezultacie tych badań, informacje na temat wykrytych podczas analizy adresów IP, które były wykorzystywane podczas ataków przekazane zostały funkcjonariuszom Komendy Głównej Policji oraz Europolu. Dodatkowo, w marcu 2016 zostałem zaproszony na spotkanie w siedzibie Europolu, podczas którego prezentowałem wyniki przeprowadzonych przeze mnie analiz zagrożenia rodziny CryptoWall funkcjonariuszom różnych służb, zarówno Europolu jak i FBI. Wyniki prowadzonych badań zostały opublikowane w artykułach [C5, C6, C7, C8, C9].

3. *Wykrywanie i przeciwdziałanie atakom.*

Podczas analizy zagrożeń typu ransomware zaobserwowałem, że w przypadku braku odpowiedzi od serwerów atakującego, dysk ofiary nie zostaje zaszyfrowany. Skłoniło mnie to do zaprojektowania systemów wykrywania faktu infekcji oraz blokowania niebezpiecznej komunikacji w celu ochrony danych, znajdujących się na zainfekowanych maszynach. Proponowane rozwiązania wykorzystywały nowatorskie podejście do sterowania sieciami komputerowymi - SDN (ang. Software-Defined Networking) i zrealizowane były jako tak zwane aplikacje SDN. Wyniki badań zostały opublikowane w publikacjach [C8, C9, C10].

Szczegółowy opis badanych przeze mnie problemów, dotyczących różnych aspektów bezpieczeństwa systemów komputerowych zamieszczono w kolejnych podrozdziałach.

3.1.1 Systemy HoneyPot

Już w VI wieku przed narodzeniem Chrystusa słynny chiński generał Sun Tzu pisał: "Jeśli znasz siebie i swego wroga, przetrwasz pomyślnie sto bitew". Wychodząc z tego założenia, od wielu lat osoby zajmujące się tematyką bezpieczeństwa systemów komputerowych w celu poznania sposobu działania atakujących uruchamiają systemy typu HoneyPot. Zgodnie z definicją zaproponowaną przez Lanca Spitznera w książce [1], "system HoneyPot jest zasobem informacyjnym, którego wartość polega na nielegalnym wykorzystaniu". Wdrożenie tego typu systemu ułatwia dokonanie włamania atakującemu, a jednocześnie pozwala na poznanie sposobu działania atakujących w celu przygotowania odpowiednich środków zaradczych. Jest to bardzo elastyczne narzędzie i ze względu na charakter zbieranych danych może być zbudowane jako oprogramowanie symulujące wybrane usługi sieciowe, w pełni funkcjonalny system komputerowy posiadający błędy, cała podsieć takich systemów, a nawet rekord w bazie danych lub niewidoczny adres e-mail zamieszczony na stronie internetowej. Ze względu na dużą elastyczność, należy dobrać odpowiedni system HoneyPot, aby uzyskać interesujące dane minimalizując jednocześnie ryzyko dla organizacji, w której będzie on działał. Oczywiście, wraz ze wzrostem ryzyka, na jakie się godzimy, jesteśmy w stanie uzyskać dokładniejsze dane dotyczące działań atakującego w przechwyconym systemie. Jednak do realizacji części badań wystarczyć mogą dużo prostsze systemy, które minimalizują ryzyko prawdziwego udanego ataku. W związku z tym, moje badania wykorzystywały systemy klasy niskiego poziomu interakcji (ang. *low interaction*), które poprzez symulowanie podatności sprowadzają ryzyko do akceptowalnego poziomu, bliskiego zeru.

W ramach pierwszych badań, związanych ze zbieraniem danych dotyczących rzeczywistej aktywności ataków sieciowych, wdrożyłem w sieci Instytutu Informatyki szereg ogólnie znanych i dostępnych na zasadzie otwartego kodu systemów: Nepenthes [2] oraz jego następcę: system Dionaea [3]. W związku z potrzebą zapewnienia bezpieczeństwa innym użytkownikom sieci, w celu zwiększenia ich odporności na ataki, zostały one przeze mnie dostosowane do uruchomienia na aktualnie mało popularnej architekturze procesorów rodziny PA-RISC. Dodatkowo, wdrożenie wymagało rekonfiguracji infrastruktury sieciowej a także opracowania odpowiednich polityk bezpieczeństwa dla wydziałowej zapory ogniowej. Systemy te są nazywane systemami niskiego poziomu interakcji, czyli jedynie symulowały podatne usługi. Takie rozwiązanie jest dobrym kompromisem pomiędzy uzyskanymi danymi dotyczącymi przebiegu ataku, a minimalizacją ryzyka udanego włamania się do maszyny uruchomionej w sieci uczelnianej.

Wstępne wyniki (opisane w pracach [C1, C2]) uzyskane w ramach prowadzonych badań pozwoliły zidentyfikować niedoskonałości tych systemów. Główną niedoskonałością systemów HoneyPot typu open source było uproszczone symulowanie witryny udostępnianej za pomocą protokołu HTTP. Było to o tyle istotną wadą, że nie pozwalało na zbieranie danych dotyczących interesujących mnie ataków, skierowanych na aplikacje Webowe. W efekcie, pozwalało to atakującym na szybkie wykrycie faktu połączenia z systemem HoneyPot. Dodatkowo, w sytuacji ataku przeprowadzonego automatycznie przez złośliwe oprogramowanie, nie dochodziło do wysłania najistotniejszych danych zawierających szczegóły ataku - wysłania eksploit-a. Należy zaznaczyć, że mimo swoich braków są one nadal używane i dostarczają interesujących danych dotyczących aktywności oraz zainteresowań atakujących.

W związku z wykryciem niedoskonałości dostępnych systemów HonePot, w ramach dalszych prac, rozpocząłem rozwój autorskiego systemu, dedykowanego zbieraniu danych dotyczących skanowań i ataków na serwery wykorzystujące protokół HTTP. W ramach prowadzonych przeze mnie prac dyplomowych zaimplementowano i wdrożono pod moim kierownictwem w sieci Instytutu Informatyki systemy WebHP i HPMS. Pierwszy z wymienionych systemów - WebHP - został zaimplementowany jako skrypt w języku PHP działający pod kontrolą serwera Apache ze specjalnie przygotowaną konfiguracją. W ramach tej konfiguracji, jakiekolwiek zapytanie do nieistniejącej strony przekazywane jest do skryptu, który loguje szczegóły połączenia w bazie danych. System HPMS służy do wizualizacji oraz analizy informacji znajdujących się w bazie danych uzupełnianej przez sensory systemu WebHP. Opis systemów WebHP i HPMS oraz wstępne analizy uzyskanych za ich pomocą danych zostały przedstawione w publikacji [C1].

W ramach dalszych badań tego nurtu, prowadziłem obserwacje i analizy uzyskanych danych oraz uruchamiałem specjalizowane systemy w reakcji na pojawiające się nowe zagrożenia. Jednym z przykładów jest system HeartBleedHP służący do analizy prób wykradania kluczy kryptograficznych, którego uruchomiłem pod koniec kwietnia 2014 roku w sieci Instytutu Informatyki. Wykorzystywał on ujawnioną w tym czasie podatność w implementacji biblioteki OpenSSL umieszczoną w katalogu CVE (ang. *Common Vulnerabilities and Exposures*) pod numerem CVE-2014-6271 [4]. System ten został zaimplementowany w trakcie prowadzonych przeze mnie projektów studenckich realizowanych w ramach przedmiotu Bezpieczeństwo Systemów i Sieci, którego jestem koordynatorem. Kilka miesięcy działania ujawniły skanowania w poszukiwaniu podatnych serwerów, jak i pojedyncze próby wykradania kluczy [C2]. Ponadto, prowadziłem prace związane z opracowaniem metodologii uruchamiania nowych "sond", systemów HoneyPot będących w stanie zbierać dane dotyczące specyficznych aplikacji lub ataków, na podstawie danych zarejestrowanych w innych systemach HoneyPot. W ramach tych prac, po wykryciu zwiększonej aktywności zaobserwowanej przez system Dionaea na określonym porcie i wstępnym potwierdzeniu, że wykorzystywany jest protokół HTTP, uruchomiane były dodatkowe sondy systemu WebHP. Analiza zarejestrowanego ruchu pozwoliła potwierdzić, że jest to atak skierowany na urządzenia NAS (ang. *Network-attached Storage*) firmy Synology, a celem atakujących jest uruchomienie oprogramowania "kopiącego" kryptowalutę Bitcoin. Wyniki tych prac zostały dokładnie omówione w publikacji [C2].

W ramach dalszych prac badawczych rozwijane były techniki zbierania danych. Zdobyte doświadczenia, które pozwoliły dokonać rekonfiguracji działających systemów, w taki sposób, aby umożliwić zbieranie danych poświęconych robakowi rozprzestrzeniającemu się na urządzenia firmy QNAP z wykorzystaniem błędu Shellshock [5]. Główny wniosek z tych prac dotyczył faktu, że środowisko systemu HoneyPot musi być w pełni zgodne z oryginalnym, symulowanym system. Zgodność trzeba zachować nawet, jeśli skutkuje to pracą łamiącą reguły opisane w protokole. Przykładowo, robak atakujący urządzenia firmy QNAP wysyłał nagłówek z prośbą o kompresję danych, jednak spodziewał się danych nieskompresowanych, a co gorsza w sytuacji otrzymania poprawnych (skompresowanych) danych nie działał prawidłowo. Szczegółowe omówienie uzyskanych wyników zostało omówione w publikacji [C3].

Podczas wszystkich prac związanych z analizą wyników działania wdrożonych systemów HoneyPot, dużym problemem był uzyskany w rezultacie ich funkcjonowania wolumen danych. Większość opisanych powyżej badań była dokonywana manualnie, co wiązało się z dużym obciążeniem czasowym. W związku z tym postanowiłem wrócić do wątku badań z okresu

doktoratu i zastosować metody eksploracji danych w celu ułatwienia pracy analityka. W ramach tych badań wykorzystane zostały metody wykrywające zbiory częste (ang. *frequent sets*) [6]. Pierwszym etapem prac było przekształcenie danych zbieranych przez system WebHP do postaci dogodnej do dalszej analizy. W ramach tego procesu każde połączenie zalogowane przez system WebHP zostało przekształcone do postaci zbioru zawierającego elementy reprezentujące jego poszczególne cechy- przykładowo, adres atakującego, użyty URL czy nazwę przeglądarki. Na tak przygotowanych danych uruchamiany był proces wykrywania zbiorów częstych. W efekcie prowadzonych prac potwierdzono, że wykryte zbiory częste pozwalają wykryć pewne powtarzalne zachowania świadczące o zorganizowanej działalności i określić ich charakter. Dodatkowo, automatyczne działania pozwoliły zredukować liczbę danych, z którymi musi zapoznać się analityk. Przykładowo, w ramach prowadzonych badań w okresie od pierwszego marca do końca kwietnia 2014 roku, system WebHP zarejestrował ponad 25 tysięcy połączeń skierowanych do wdrożonego systemu HoneyPot. W efekcie użycia zaproponowanej metody uzyskano 1050 wzorców, co znacznie zredukowało liczbę danych, które następnie wymagały manualnej analizy. Wyniki tych prac zostały dokładnie omówione w publikacji [C4].

3.1.2 Analiza złośliwego oprogramowania

Jednym z wyników działania systemów HoneyPot jest możliwość pozyskania rzeczywistych próbek złośliwego oprogramowania. Bez dokładniej analizy, nie niosą one jednak dodatkowej informacji dotyczącej obserwowanych ataków. Dopiero pełne ich zbadanie jest bardzo wartościowe, ponieważ ujawnia dużo szczegółów dotyczących sposobu działania atakujących w kolejnych etapach ataku, kiedy już uzyskają dostęp do maszyny ofiary. Jednak analiza tego typu programów jest czasochłonna oraz, co gorsze, związana z dużym ryzykiem, jeśli podczas nieumiejętnego obchodzenia się z próbką złośliwego oprogramowania dojdzie do jej nieumyślnego uruchomienia na maszynie osoby przeprowadzającej analizę. Głównym problemem badawczym w tym obszarze jest zapewnienie, aby analiza złośliwej próbki nie doprowadziła do infekcji systemu używanego przez osobę ją badającą. Ponadto, ważne jest, aby uniemożliwić próbce wykrycia faktu przeprowadzania jej analizy.

W literaturze znane są dwa główne podejścia do analizy złośliwego oprogramowania - statyczna i dynamiczna. Analiza statyczna polega na manualnej analizie programu instrukcja po instrukcji i aż do odtworzenia pełnego działania programu. Głównym narzędziem podczas tego procesu są disassemblery i debugery, z których najczęściej wykorzystywanym przez osoby związane z bezpieczeństwem jest program Ida Pro [7]. Metoda ta pozwala uzyskać informacje o wszystkich funkcjach analizowanego programu, także tych, które mogę zostać uruchomione w konkretnych, trudnych do przewidzenia momentach działania programu, np. o określonej dacie i godzinie, kiedy użytkownik wykona określoną czynność, itp. Niestety, statyczna analiza kodu posiada podstawową wadę: jest to czas potrzebny na jej wykonanie oraz konieczność zaangażowania osoby o odpowiednio wysokich kwalifikacjach praktycznie w trakcie trwania całego procesu badawczego. Drugie podejście - analiza dynamiczna - polega na uruchomieniu próbki w kontrolowanym środowisku i obserwację jej zachowania. Takie podejście jest dużo szybsze i można je z powodzeniem skalować, wykorzystując do analizy wiele maszyn jednocześnie. Oczywiście, także i ta metoda posiada kilka wad. Najważniejsza związana jest

z faktem, że dynamiczna analiza może nie ujawnić wszystkich funkcji realizowanych przez badany program.

W toku dalszych prac skupiłem się na wykorzystaniu i rozwoju metod wykorzystujących dynamiczną analizę złośliwego oprogramowania. W efekcie prowadzonych badań opracowałem koncepcję systemu umożliwiającego automatyczne przeprowadzanie analizy podejrzanego programu wykonywalnego. W efekcie działania takiego systemu, otrzymywałem, miedzy innymi, informacje o pobranych z Internetu programach, uruchomionych procesach oraz całej aktywności sieciowej. Mimo istnienia podobnych systemów, przykładowo Cuckoo Sandbox [8], zdecydowałem się na rozwój własnego rozwiązania. Motywacją była realizacja systemu, który w przeciwieństwie do ogólnie znanych rozwiązań będzie trudno rozróżnialny od maszyny zwykłego użytkownika. Zaprojektowany system wykorzystuje dostępne na zasadach otwartego kodu środowisko wirtualizacyjne Xen [9] zarządzające maszynami wirtualnymi, na których uruchamiane są próbki złośliwego oprogramowania. Maszyny wirtualne wykorzystywane podczas analizy posiadały dodatkowe moduły pozwalające na zbieranie informacji dotyczących uruchamianych podczas analizy procesów oraz zmian na dysku twardym. Z kolei system zarządzania środowiskiem Maltester zapewniał uruchomienie każdej analizy na "czystej" maszynie, a także zapewniał bezpieczeństwo innych urządzeń. System został zaimplementowany i wdrożony w sieci Instytutu Informatyki w ramach prowadzonych przeze mnie prac dyplomowych. Opis systemu Maltester oraz wyniki analiz próbek złośliwego oprogramowania rodziny CryptoWall z jego wykorzystaniem zostały przedstawione w publikacji [C5] (więcej szczegółów na temat badań związanych z zagrożeniami typu ransomware umieszczono w kolejnym podrozdziale).

W ramach dalszych prac związanych z tą tematyką pełniłem nadzór merytoryczny nad opracowaniem koncepcji kolejnego systemu dynamicznej analizy wdrożonego w sieci Instytutu Informatyki. Ogólne założenia, co do funkcjonowania takiego systemu bazowały na rozwiązaniach znanych z systemu Maltester, jednak korzystał on z innego zarządcy maszyn wirtualnych, tj. Microsoft Hyper-V. Wybór tego środowiska wirtualizacji podyktowany był jego małą popularnością w środowisku osób zajmujących się analizą złośliwego oprogramowania, co w moich założeniach miało znacząco utrudnić wykrycie przez badaną próbkę faktu prowadzenia jej analizy. System taki, o nazwie MESS. został zrealizowany w ramach prowadzonych w Instytucie Informatyki prac dyplomowych. Opis systemu MESS oraz wyniki dalszych analiz próbek złośliwego oprogramowania rodziny CryptoWall z jego wykorzystaniem przedstawiono w publikacji [C6].

Skuteczności działania systemów Maltester i MESS dowodzi fakt, że podczas analizy jednego z zagrożeń o nazwie Morto [10] w wymienionych systemach dynamicznej analizy pozyskane próbki uruchamiały się bez problemów, ujawniając swój sposób działania - w tym ruch sieciowy wykorzystujący metody steganograficzne. Poproszeni o pomoc specjaliści bezpieczeństwa, zajmujący się analizą tego typu danych komercyjnie, stwierdzili, że dostarczone próbki są uszkodzone i nie uruchamiają się w ich środowisku badawczym. Najprawdopodobniej powodem braku działania złośliwego oprogramowania było wykrycie przez próbkę komercyjnego środowiska do dynamicznej analizy, które powodowało celowe zakończenie się programu błędem, bez ujawniania rzeczywistej niebezpiecznej funkcjonalności.

Dość istotny podobszar w ramach prezentowanego nurtu badawczego dotyczy zagrożeń typu ransomware (zbitek angielskich słów "*ransom*" i "*software*") - złośliwe oprogramowanie, które

pierwotnie uniemożliwiało prawowitemu użytkownikowi korzystanie z komputera do momentu zapłaty okupu na rzecz przestępcy. Mimo tego, że pierwsze próby ataków tego typu sięgają końca lat 80 (program AIDS/PC Cyborg z 1989 [11]) ich popularność wzrosła w ciągu kilku ostatnich lat w związku z popularyzacją Internetu (ułatwiającego masowe infekcje) oraz rozwojem kryptowalut umożliwiających dokonanie praktycznie anonimowych wpłat okupu na rzecz przestępców. Dodatkowo, twórcy złośliwego oprogramowania zamiast blokować dostęp do komputera zaczęli szyfrować pliki użytkowników. Obecnie, co potwierdzają liczne raporty firm i instytucji zajmujących się cyberbezpieczeństwem jest to jedno z najpopularniejszych i najniebezpieczniejszych zagrożeń.

Rozpoczęcie moich badań związanych z analizą zagrożeń typu ransomware związane było z infekcją złośliwym oprogramowaniem tego typu jednego z komputerów w sieci Instytutu Informatyki. Poproszony zostałem o usunięcie zagrożenia oraz próbę odzyskania danych. Pozyskaną w ramach tych czynności próbkę złośliwego oprogramowanie przeanalizowałem z wykorzystaniem wcześniej opisanych własnych systemów dynamicznej analizy. Sposób działania tej próbki okazał się bardzo interesujący ze względu na rozbudowaną komunikację sieciową. W przeciwieństwie do większości wcześniej analizowanych próbek, które nawiązywały połączenie jedynie z jednym serwerem C&C (ang. *Command and Control*) atakującego, próbka ta próbowała nawiązać połączenia z szeregiem maszyn. Wstępna analiza komunikacji nie ujawniła dużej liczby nowych informacji w związku z faktem wykorzystaniem przez atakujących szyfrowania komunikacji. Wśród użytych do dalszej komunikacji maszyn znajdowały się także urządzenia zlokalizowane na terenie Polski. Po telefonicznym kontakcie z jednym z administratorów maszyny, okazało się, że jest on także ofiarą ataku i nic nie wiedział o dodatkowym oprogramowaniu działającym na administrowanej przez niego maszynie. Dodatkowo, udostępnił mi nielegalnie umieszczone na jego maszynie skrypty atakujących. Manualna analiza tak uzyskanych kodów źródłowych ujawniła wykorzystany algorytm szyfrowania oraz pozostałe szczegóły używanego protokołu. Pozwoliło to na odszyfrowanie komunikacji między maszyną ofiary a serwerami wykorzystywanymi przez atakujących do dystrybucji kluczy służących do szyfrowania dokumentów ofiary. Wyniki tych prac zostały przedstawione w publikacji [C5].

W ramach dalszych prac związanych z analizą tego typu zagrożeń opracowano metody wyszukiwania kolejnych próbek złośliwego oprogramowania w ogólnodostępnych serwisach internetowych, takich jak Malwr [12], Reverse.It [13], czy Hybrid Analysis [14]. Miało to istotne znaczenie, ponieważ atakujący często zmieniali serwery dystrybuujące klucze kryptograficzne, co miało utrudnić przerwanie ich działalności. W ramach tych prac przygotowałem dedykowany system ARTA współpracujący z systemami Maltester i WebHP, który umożliwiał automatyczne wykonania analizy serwerów wykorzystywanych w celu połączenia się z serwerami C&C. W efekcie, zastosowanie wdrożonego systemu przyspieszało czas analizy posiadanych próbek.

W wyniku prowadzonych prac przeanalizowane zostało 359 próbek złośliwego oprogramowania rodziny CryptoWall i ujawniono 2038 unikalnych adresów URL wykorzystujących 1945 unikalnych domen. Opis systemu ARTA oraz przeprowadzonych za jego pomocą badań zostały zamieszczone w publikacji [C7].

Uzyskane dane zostały przekazane funkcjonariuszom Wydziału do Walki z Cyberprzestępczością, Biura Służby Kryminalnej, Komendy Głównej Policji. Ponadto, wyniki okazały się na tyle interesujące, że zostałem zaproszony do ich zaprezentowania w trakcie

zaproszonego wykładu w siedzibie Europolu w Hadze przed reprezentantami międzynarodowych służb m.in. Federal Bureau of Investigation (FBI) oraz European Cyber Crime Centre (EC3) Europolu. Wygłoszona prezentacja miała tytuł "Dynamic analysis of CryptoWall network activity".

Kontynuacją wspomnianych powyżej badań było opracowanie metod służących do wykrywania faktu infekcji oraz próbom przeciwdziałania zaszyfrowania dysku ofiary. Szczegóły tych prac przedstawiono w kolejnym podrozdziale.

3.1.3 Wykrywanie i przeciwdziałanie atakom

Prowadzone wcześniej prace badawcze dotyczące zbierania próbek rzeczywistego złośliwego oprogramowania za pomocą systemów HoneyPot oraz ich późniejsza analiza w dedykowanych systemach pozwoliły na zdobycie wiedzy dotyczącej sposobu ich działania. Dodatkowo, w ramach prowadzonych analiz sposobu działania zagrożeń typu ransomware, zidentyfikowano ich słabe strony, umożliwiające wykrycie zagrożenia, a także przeciwdziałanie uruchomieniu jego destruktywnych funkcji. Ostatni z tematów badawczych, jakim się zajmowałem dotyczył wykorzystania tej wiedzy oraz skorzystania z możliwości jakie daje koncepcja SDN (ang. *Software Defined Networking)* do budowy systemów bezpieczeństwa reagujących na aktualnie pojawiające się w Internecie zagrożenia.

SDN jest relatywnie nowym paradygmatem budowy sieci komputerowych [15]. Zmienia on sposób zarządzania i sterowania przesyłaniem ruchu w sieciach, a dodatkowo umożliwia bardzo proste, programowe rozszerzanie ich funkcjonalności, np. o moduły monitorujące czy reagujące na wykryte zagrożenia. Aktualnie używane sieci, w środowisku SDN nazywane "starymi" (ang. *legacy networks*), można rozważać, jako system rozproszony. Każde urządzenie sieciowe samodzielnie podejmuje decyzję, w zależności od informacji odebranych od sąsiadujących urządzeń. Realizacja dodatkowych funkcji sieci wiąże się ze zmianami oprogramowania lub współpracą z każdym urządzeniem osobno. Co gorsza, urządzenia każdego producenta mogą używać własnych, często nie udostępnionych publicznie protokołów. Sieci oparte na SDN w przeciwieństwie do poprzednio opisanych mają centralny punkt służący do zarządzania siecią - kontroler SDN. Kontroler SDN podejmuje decyzję dotyczące sposobu sterowania i samodzielnie komunikuje się z podległymi przełącznikami SDN. Takie podejście było motywowane między innymi ograniczeniem kosztów nowych przełączników oraz zwiększeniem ich wydajności. Przy takich założeniach, przełączniki mają być relatywnie proste oraz tanie. Cała logika działania sieci jest zaszyta w kontrolerze SDN. Dużą zaletą tego podejścia jest możliwość prostego dodawania nowych funkcji do sieci, poprzez uruchomienie na kontrolerze tak zwanych aplikacji SDN. Tematyką sieci opartych na koncepcji SDN zainteresowałem się około 2014 roku, właśnie z powodu możliwości wykorzystania aplikacji SDN w celu realizacji nowych funkcji bezpieczeństwa.

Wykonana przeze mnie analiza działania próbek złośliwego oprogramowania rodziny CryptoWall wykazała, że jeśli żaden serwer z zaszytej w kodzie listy nie odpowiada, nie dochodzi do zaszyfrowania dysku ofiary. W związku z tym zaimplementowano i przebadano aplikacje SDN, które blokują ruch od potencjalnych ofiar do podanych adresów IP, reprezentujących serwery C&C atakującego. W ramach prowadzonych prac zaproponowano dwie wersje aplikacji. W pierwszej wersji cały ruch protokołu DNS jest kierowany do kontrolera SDN i na podstawie

weryfikacji używanej domeny odpowiedź jest przekazywana dalej lub blokowana. Druga wersja, bez zbędnej zwłoki przesyła dalej zapytanie DNS i równocześnie przesyła je do kontrolera w celu dalszej analizy. Takie rozwiązanie nie wpływa na opóźnienie komunikacji z większością domen, ponieważ są one bezpieczne i nie wymagając blokowania. Taki system będzie działał poprawnie o ile czas analizy i blokowania będzie mniejszy niż czas przekazania kluczy z serwera C&C. Przeprowadzone badania eksperymentalne prototypowego systemu wykazały, że czas reakcji nie przekracza 100ms.. Dodatkowo, podczas badań udowodniono, że czas przekazania klucza z serwera C&C jest dużo większy (od 3,76 do 27,38 s, średnio 9,28 s) niż czas reakcji zaproponowanego systemu, co gwarantuje jego poprawne działanie. Wyniki tych prac zostały przedstawione w publikacji [C8].

Główną wadą rozwiązań zaproponowanych w ramach wcześniej prowadzonych przeze mnie prac była konieczność posiadania aktualnej i stale rozszerzanej listy zawierającej adresy serwerów C&C. Takie rozwiązanie przy bardzo szybkiej zmianie adresów wykorzystywanych przez atakujących praktycznie je dyskwalifikuje. W ramach dalszych prac postanowiłem rozwiązać problem badawczy dotyczący możliwości wykrywania i przeciwdziałania atakom ransomware wykorzystując charakterystykę ruchu sieciowego - pewne wzorce zachowań. W ramach kolejnych prac związanych z analizą komunikacji próbek złośliwego oprogramowania typu ransomware rodzin CryptoWall i Locky, zbadałem rozmiary komunikatów wymienianych podczas uzyskania klucza szyfrującego. Wyniki tych prac wykazały, że w tym celu używane są komunikaty POST protokołu HTTP. Dalsze prace potwierdziły, że mimo intencjonalnego dodania pewnej losowości w komunikacji, rozmiary wiadomości w kolejnych fazach komunikacji są powtarzalne. Umożliwia to wykrywanie infekcji, bez potrzeby deszyfrowania całej komunikacji tylko na podstawie analizy rozmiarów wymienianych komunikatów. W toku prac zaproponowano i zweryfikowano mechanizm detekcji zainfekowanych maszyn, na podstawie klasyfikacji rozmiarów obserwowanych wiadomości. Zaimplementowane i eksperymentalnie zweryfikowane rozwiązanie uzyskiwało detekcję na poziomie 97–98% przy poziomie fałszywych alarmów na poziomie 1–2% lub 4–5% w zależności od zastosowanego wariantu oceny metody. Wyniki tych prac zostały przedstawione w publikacji [C9].

W ramach dalszych prac, wykorzystując doświadczenie z budowy systemów bezpieczeństwa w oparciu o koncepcję SDN, postanowiłem zastosować je do innych zagrożeń sieciowych. W ramach moich prac w projekcie IoRL (ang. *Internet of Radio Light*) zaproponowałem system wykrywający i blokujący aktywność atakujących związaną ze skanowaniem maszyn podłączonych do sieci. Wyniki tych prac zostały przedstawione w publikacji [C10].

3.1.4 Podsumowanie - wkład w dziedzinę

W ramach prowadzonych przez ostatnie kilka lat badań zajmowałem się kompleksowo problemem analizy i przeciwdziałaniu atakom z wykorzystaniem złośliwego oprogramowania. Za najważniejsze moje osiągniecie uważam opracowanie szeregu metod wykrywających i blokujących komunikację ofiar z serwerami C&C, w tym metodę wykorzystującą jedynie analizę rozmiarów nagłówków przesyłanych w ramach metody POST protokołu HTTP. Dodatkowo oceniam, że wniosłem istotny wkład w opracowanie metod oraz przeprowadzenie analiz zagrożeń klasy ransomware, ze szczególnym uwzględnieniem analizy infrastruktury używanej podczas ataków złośliwego oprogramowania rodzin CryptoWall i Locky. Oprócz omówienia wyników

w szeregu publikacji, także w czasopismach indeksowanych w JCR, zostały one przekazane Wydziałowi do Walki z Cyberprzestępczością, Komendy Głównej Policji oraz funkcjonariuszom Europolu. Uzyskane wyniki spotkały się z zainteresowaniem szerokiego grona odbiorców. Publikacja w czasopiśmie IEEE Networks od czasu publikacji (grudzień 2016), przez niecałe 2,5 roku była wielokrotnie cytowana (55 razy według bazy Google Scholar, i 18 razy według bazy WoS). Dodatkowo zostałem także zaproszony do przedstawienia uzyskanych wyników przez Europol oraz na konferencji branżowej Advanced Threat Summit. Co warte podkreślenia, w związku z brakiem uznanych zbiorów testowych wielokrotnie byłem proszony przez innych naukowców o udostępnienie zebranych próbek złośliwego oprogramowania rodzin CryptoWall i Locky. W tym czasie wykonałem także szereg recenzji artykułów dotyczących zagrożenia typu ransomware, między innymi przez takie czasopisma IEEE Communications Magazine (JCR), Cryptology (JCR) czy Journal of Information Security and Applications.

Poniżej znajduję się lista, pozostałych istotnych wyników uzyskanych w ramach prowadzonych przeze mnie prac:

- Opracowanie metodyki uruchamiania nowych „sond" HoneyPot na bazie analizy dotychczas zebranych danych,
- Zaprojektowanie i wdrożenie w sieci Instytutu Informatyki systemów HoneyPot: WebHP, HPMS, HeartBleed,
- Opracowanie koncepcji wykorzystania metod eksploracji danych do automatycznego wykrywania zagrożeń,
- Zebranie danych na potrzeby kolejnych badań,
- Opracowanie koncepcji działania, architektury oraz wdrożenie systemu dynamicznej analizy Maltester,
- Opracowanie metodyki umożliwiającej automatyczną identyfikację serwerów atakujących w środowisku dynamicznej analizy we współpracy z systemem HoneyPot – wdrożenie jako system ARTA,
- Przeprowadzenie analizy zagrożeń, między innymi złośliwego oprogramowania typu ransomware rodzin CryptoWall, Locky oraz robaków dedykowanych na urządzenia wbudowane firm Synology i QNAP,
- Opracowanie metody przeciwdziałania ransomware poprzez analizę aktywnych próbek złośliwego oprogramowania i blokowanie aktywnych adresów serwerów atakującego,
- Opracowanie koncepcji nowej metody detekcji ransomware opartej o analizę charakterystyki ruchu HTTP,
- Nadzór nad implementacją prototypów systemów wykorzystujących koncepcję sieci programowalnych (Software-Defined Networking) i eksperymentalną weryfikacją ich skuteczności.

3.2 Omówienie pozostałych osiągnięć naukowo-badawczych

Większość moich pozostałych osiągnięć naukowo-badawczych, niewchodzących do przedłożonego osiągnięcia naukowego, związane jest z pracą przy czternastu projektach, w tym

pełnienie roli kierownika w trzech z nich. Pełna lista projektów przedstawiona jest w załączniku "Wykaz opublikowanych prac", punkt II J.

W trakcie współpracy z pracownikami Instytutu Telekomunikacji, pod kierownictwem prof. Krzysztofa Szczypiorskiego w latach 2008 - 2012 brałem udział w badaniach związanych z technikami steganografii sieciowej. W ramach prac nad projektem TrustMAS sfinansowanym przez armię amerykańską i siły powietrzne (US Army and US Air Force) odpowiadałem za implementację symulatora ruchu sieciowego, który pozwalał na analizę koncepcji „rozproszonego rutera steganograficznego". Dodatkowo, byłem współautorem publikacji opisującej uzyskane wyniki [16]. W ramach dalszych prac związanych z tym obszarem wspomagałem badania dotyczące analizy nieprawidłowości występujących w rzeczywistym ruchu telefonii internetowej. Wyniki tych badań zostały opisane w artykule opublikowanym w czasopiśmie indeksowanym na liście JCR [17].

Do tematyki steganografii wróciłem ponownie w 2017 roku, kiedy zostałem kierownikiem projektu CoCoDe (ang. *Covert Communication Detection*) sfinansowanym przez AFOSR (ang. *Air Force Office of Science Research*). Celem trzyletniego projektu jest zbadanie możliwości wykrywania ruchu steganograficznego z wykorzystaniem metod eksploracji danych. Dodatkowo, w ramach prac, analizie poddane są rozproszone ukryte kanały sieciowe (ang. *Distributed Network Covert Channels*) oraz wpływ ich zastosowania na możliwość wykrycia wiadomości steganograficznych. Wstępne wyniki prac zostały przedstawione w publikacjach konferencyjnych [18, 19].

Wykorzystując zdobyte doświadczenie oraz wdrożone w sieci Instytutu Informatyki systemy dynamicznej analizy złośliwego oprogramowania rozpocząłem współpracę z naukowcami zaangażowanymi w inicjatywę CUIng (ang. *Criminal Use of Information Hiding*). W ramach tych prac zajmowaliśmy się analizą trendu polegającego na coraz częstszym wykorzystaniu przez złośliwe oprogramowanie metod steganografii sieciowej do ukrycia faktu komunikacji z serwerami C&C, do eksfiltracji poufnych danych bądź ściągnięcia kolejnych modułów złośliwego oprogramowania. Wyniki tych prac zostały opublikowane w czasopiśmie z indeksowanym na liście JCR [20].

Drugim szerokim zagadnieniem, jakim się zajmowałem, są prace związane z rozwijaniem nowoczesnych metod nauczania, w szczególności związanych z tematyką sieci komputerowych oraz aspektów bezpieczeństwa. W ramach pierwszych prac, których wyniki zostały opublikowane na konferencji [21], zajmowaliśmy się zdalnym dostępem do urządzeń sieciowych wykorzystywanych podczas nauki zagadnień sieciowych. Do tych prac wróciłem w roku 2017, kiedy zostałem po stronie Instytutu Informatyki kierownikiem projektu międzynarodowego IVLIS (ang. *International Virtual Lab on Information Security*) realizowanego wraz z partnerami z Niemiec i Włoch. Celem tego projektu jest przygotowanie zdalnego laboratorium, umożliwiającego realizację ćwiczeń wybranych zagadnień dotyczących bezpieczeństwa sieciowego bez potrzeby fizycznej obecności na uczelni. Aktualnie grupa studentów realizujących, prowadzony przeze mnie przedmiot "Bezpieczeństwo Systemów i Sieci", realizuje część ćwiczeń laboratoryjnych na prototypie tej platformy we współpracy ze studentami z Włoch i Niemiec.

W latach 2014-2017 uczestniczyłem w projekcie programu Erasmus+ ParIS (ang. *Strategic Partnership in Information Security*). W ramach projektu z partnerami z Luksemburga, Portugalii i Ukrainy opracowany został program wspólnych studiów magisterskich realizowanych na

różnych uczelniach związanych z tematyką bezpieczeństwa. Wyniki tych prac zostały opublikowane w czasopiśmie indeksowanym przez JCR [22].

W pozostałych projektach, w których brałem udział odpowiedzialny byłem za projekt oraz w wielu przypadkach implementację prototypowych systemów wykrywających różnego typu ataki. W większości sytuacji wykorzystywałem do tego celu metody eksploracji danych. Poniżej znajduje się lista najciekawszych, moim zdaniem, realizowanych projektów, wraz z listą publikacji opisujących wyniki prowadzonych prac.

- Efipsans (ang. *Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomic Networks and Services*), w ramach Europejskiego 7 programu ramowego (2008-2010).

Projekt oraz implementacja prototypu elementu decyzyjnego działającego w architekturze GANA (ang. *Generic Autonomic Network Architecture*), realizującego funkcjonalność samoobrony sieci. Zaproponowany i zrealizowany moduł, nazwany Node_Level_Security_Decision_Element, wykorzystywał zbiory częste do wykrywania ataków sieciowych, między innymi, ataków odmowy usługi (DDoS), rozsyłania SPAM-u przez zainfekowane maszyny oraz skanowań sieciowych [23].

- Inżynieria Internetu Przyszłości, w ramach programu operacyjnego innowacyjna gospodarka, POIG.01.01.02-00-045/09-00, (2010-2013).

Inżyniera Internetu Przyszłości (IIP) - projekt oraz implementacja prototypu agentów bezpieczeństwa warstwy drugiej systemu IIP: lokalnego agenta bezpieczeństwa (ang. Local Security Agent, LSA) oraz głównego agenta bezpieczeństwa (ang. Master Security Agent, MSA). W ramach projektu zaproponowałem i zrealizowałem wykrywanie ataków w danych z zapory ogniowej, rejestru nieudanych logowań do usługi SSH oraz logów z modułu HMAC systemu IIP z wykorzystaniem zbiorów częstych. Oprogramowanie zostało zintegrowane w ogólnopolskiej sieci PL-LAB między innymi na węzłach w Krakowie, Wrocławiu i Warszawie, a jego skuteczność zweryfikowane eksperymentalnie [24 - 29].

- SYNAT (System Nauki i Techniki) pt. „Utworzenie uniwersalnej, otwartej, repozytoryjnej platformy hostingowej i komunikacyjnej dla sieciowych zasobów wiedzy dla nauki, edukacji i otwartego społeczeństwa wiedzy" (2010-2013)

Propozycja oraz implementacja prototypowego modułu wykrywającego z wykorzystaniem wzorców eksploracji danych - zbiorów częstych i wzorców wyskakujących (ang. *Jumping Emerging Patterns*) uruchomienie podejrzanych pojedynczych programów lub grup programów [30]. Zaprojektowanie, implementacja oraz integracja z system PNOTES modułu ODM (ang. *Online Detection Module*, ODM) wykrywającego znaczący wzrost wykorzystania zasobów monitorowanej maszyny, przykładowo wykorzystania procesora lub sieci [31].

- Internet of Radio Light (IoRL), w ramach programu Unii Europejskiej Horyzont 2020 (2017-2020).

Projekt systemu bezpieczeństwa wykorzystującego mechanizmy eksploracji danych do wykrywania ataków sieciowych inicjowanych przez lub zagrażających użytkownikom podłączonym do sieci Internet z wykorzystaniem systemu IoRL. Aktualnie uruchamiany system będzie zaimplementowany jako aplikacja działająca w ramach kontrolera SDN [32].

Bibliografia

[1] Honeynet Team: Honeynet Project, Know Your Enemy: Learning about Security Threats, 2nd Edition, Boston: Addison-Wesley Professional, May 27, 2004, ISBN-13: 978-0321166463

[2] Baecher Paul, Koetter Markus, Dornseif Maximillian, Freiling Felix: The nepenthes platform: An efficient approach to collect malware, In Proceedings of the 9 th International Symposium on Recent Advances in Intrusion Detection (RAID06), LNCS 4219, ss. 165–184, 2006

[3] Dionaea home page, http://dionaea.carnivore.it/

[4] Banks James: The Heartbleed bug: insecurity repackaged, rebranded and resold, Crime, Media, Culture, Vol. 11 No. 2, ss. 1-21, 2015

[5] Ahmad Muhammad Aminu, Woodhead Steve, and Gan Diane: Early Containment of Fast Network Worm Malware, In Information and Computer Science National Foundation for Science and Technology Development Conference on IEEE, ISBN 978-1-5090-2100-0, ss. 195-201, 2016

[6] Agrawal Rakesh, Srikant Ramakrishnan, Fast algorithm for mining association rules, In J.B. Bocca, M. Jarke, and C. Zaniolo, editors. Proceedings of VLDB, ss. 487-499, 1994

[7] Ida Pro, https://www.hex-rays.com/products/ida/

[8] Digit Oktavianto, Iqbal Muhardianto, Cuckoo Malware Analysis, Packt Publishing, 2013, ISBN:1782169237 9781782169239

[9] Xen Hypervisor, https://xenproject.org/

[10] Mazurczyk, Wojciech, and Caviglione Luca: Information Hiding as a Challenge for Malware Detection, IEEE Security & Privacy, Vol. 13 (2), ss. 89–93, DOI:10.1109/MSP.2015.33.

[11] Gazet Alexandre: Comparative analysis of various ransomware virii, Journal in computer virology, 2010 Feb 1, Vol. 6(1), ss. 77–90, DOI: 10.1007/s11416-008-0092-2

[12] Malwr, https://malwr.com/

[13] Reverse.IT, Free Automated Malware Analysis Service - powered by Falcon Sandbox, https://www.reverse.it/

[14] Hybrid Analysis, https://www.hybrid-analysis.com/

[15] Kreutz Diego, Ramos Fernando M. V., et. el: Software-Defined Networking: A Comprehensive Survey,., Published in Proceedings of the IEEE 2014, DOI:10.1109/JPROC.2014.2371999

[16] Szczypiorski Krzysztof, Margasiński Igor, Mazurczyk Wojciech [i in.] : TrustMAS: Trusted Communication Platform for Multi-Agent Systems, w: On the Move to Meaningful Internet Systems: OTM 2008 / Meersman Robert, Tari Zahir (red.), Lecture Notes In Computer Science,

nr 5332, 2008, Springer Berlin Heidelberg, ISBN 978-3-540-88872-7, 978-3-540-88873-4, ss. 1019-1035, DOI:10.1007/978-3-540-88873-4_7

[17] Mazurczyk Wojciech, Cabaj Krzysztof, Szczypiorski Krzysztof: What are suspicious VoIP delays?, w: Multimedia Tools and Applications, Springer, vol. 57, nr 1, 2012, ss. 109-126, DOI:10.1007/s11042-010-0532-0

[18] Cabaj Krzysztof, Mazurczyk Wojciech, Nowakowski Piotr [i in.] : Towards Distributed Network Covert Channels Detection Using Data Mining-based Approach, w: ARES 2018 Proceedings of the 13th International Conference on Availability, Reliability and Security / Doerr Christian, Schrittwieser Sebastian, Weippl Edgar (red.), 2018, ACM, ISBN 978-1-4503-6448-5, ss. 1-10, DOI:10.1145/3230833.3233264

[19] Mazurczyk Wojciech, Wendzel Steffen, Cabaj Krzysztof: Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach, w: ARES 2018 Proceedings of the 13th International Conference on Availability, Reliability and Security / Doerr Christian, Schrittwieser Sebastian, Weippl Edgar (red.), 2018, ACM, ISBN 978-1-4503-6448-5, ss. 1-10, DOI:10.1145/3230833.3233261

[20] Cabaj Krzysztof, Caviglione Luca, Mazurczyk Wojciech [i in.]; The New Threats of Information Hiding: the Road Ahead, w: IT Professional, vol. 20, nr 3, 2018, ss. 31-39, DOI:10.1109/MITP.2018.032501746, 20 punktów MNiSW, IF=1.661,

[21] Cabaj Krzysztof, Radziszewski Paweł, Szczypiorski Krzysztof: Zastosowanie w dydaktyce zdalnego dostępu do sprzętu sieciowego, w: Przegląd Telekomunikacyjny- wiadomości telekomunikacyjne, vol. 8-9 2009, 2009, ss. 960-965

[22] Cabaj Krzysztof, Domingos Dulce, Kotulski Zbigniew [i in.] : Cybersecurity education: evolution of the discipline and analysis of master programs, w: Computers & Security, vol. 75C, 2018, ss. 24-35, DOI:10.1016/j.cose.2018.01.015

[23] Cabaj Krzysztof, Szczypiorski Krzysztof, Becker Sheila: Towards Self-defending Mechanisms Using Data Mining in the EFIPSANS Framework, w: Advances in Multimedia and Network Information System Technologies / Nguyen Ngoc Thanh, Zgrzywa Aleksander, Czyżewski Andrzej (red.), Advances in Intelligent and Soft Computing , nr 80, 2010, Springer, ISBN 978-3-642-14988-7, ss. 143-151, DOI:10.1007/978-3-642-14989-4_14

[24] Konorski Jerzy, Pacyna Piotr, Kasperek Jerzy [i in.] : Integracja Niskopoziomowego Podsystemu Bezpieczenstwa Dla Systemu IIP, w: Przegląd Telekomunikacyjny- Wiadomości Telekomunikacyjne, SIGMA NOT, vol. LXXXVI, nr 8-9/2013, 2013, ss. 1031-1037

[25] Konorski Jerzy, Pacyna Piotr, Kołaczek Grzegorz [i in.] : Theory and implementation of a virtualisation level Future Internet defence in depth architecture , w: International Journal of Trust Management in Computing and Communications, Inderscience Publishers, vol. 1, nr 3/4, 2013, ss. 274-299, DOI:10.1504/IJTMCC.2013.056431

[26] Cabaj Krzysztof, Kołaczek Grzegorz, Konorski Jerzy [i in.] : Security architecture of the IIP Systems on resources virtualize action level, w: Przegląd Telekomunikacyjny- Wiadomości Telekomunikacyjne, SIGMA NOT, vol. LXXXIV, nr 8-9/2011, 2011, ss. 846-851

[27] Konorski Jerzy, Cabaj Krzysztof, Kotulski Zbigniew [i in.]: Implementacja i testy architektury bezpieczeństwa na poziomie 2 Systemu IIP, w: Inżynieria Internetu Przyszłości. Część 2 / Burakowski Wojciech, Krawiec Piotr (red.), 2013, Oficyna Wydawnicza PW, ISBN 978-83-7814-099-3, ss. 46-76

[28] Cabaj Krzysztof, Kołaczek Grzegorz, Konorski Jerzy [i in.] : Architektura bezpieczeństwa Systemu IIP, w: Inżynieria Internetu Przyszłości. Część 1 / Burakowski Wojciech, Krawiec Piotr (red.), 2012, OW PW, ISBN 978-83-7814-042-9, ss. 43-60

[29] Konorski Jerzy, Pacyna Piotr, Kołaczek Grzegorz [i in.] : A Virtualization-Level Future Internet Defense-in-Depth Architecture, w: Recent Trends in Computer Networks and Distributed Systems Security / Thampi Sabu M. [i in.] (red.), Communications in Computer and Information Science, vol. 335, 2012, Springer Berlin Heidelberg, ISBN 978-3-642-34134-2, ss. 283-292, DOI:10.1007/978-3-642-34135-9_29

[30] Sosnowski Janusz, Gawkowski Piotr, Cabaj Krzysztof [i in.] : Analyzing Logs of the University Data Repository, w: Intelligent Tools for Building a Scientific Information Platform: From Research to Implementation / Bembenik Robert [i in.] (red.), Studies in Computational Intelligence, vol. 541, 2014, Springer International Publishing, ISBN 978-3-319-04713-3, ss. 141-156, DOI:10.1007/978-3-319-04714-0_9

[31] Sosnowski Janusz, Gawkowski Piotr, Cabaj Krzysztof: Exploring the Space of System Monitoring, w: Intelligent Tools for Building a Scientific Information Platform: Advanced Architectures and Solutions /Bembenik Robert [i in.] (red.), Studies in Computational Intelligence, vol. 467, 2013, Springer-Verlag Berlin Heidelberg , ISBN 978-3-642-35646-9, ss. 501-517, DOI:10.1007/978-3-642-35647-6_30

[32] Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech [i in.] : SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System, w: ARES 2018 Proceedings of the 13th International Conference on Availability, Reliability and Security / Doerr Christian, Schrittwieser Sebastian, Weippl Edgar (red.), 2018, ACM, ISBN 978-1-4503-6448-5, ss. 1-10, DOI:10.1145/3230833.3233248

Krzysztof Cabaj