SZKOŁA GŁÓWNA HANDLOWA W WARSZAWIE
WARSAW SCHOOL OF ECONOMICS

Studia Podyplomowe Zarządzanie Cyberbezpieczeństwem
edycja I

Grzegorz Data
Nr albumu 96345

Platforma do analizy, gromadzenia i wymiany informacji służących rozpoznaniu zagrożeń cybernetycznych

Praca dyplomowa
napisana w Instytucie Informatyki
i Gospodarki Cyfrowej

pod kierunkiem naukowym
dr Rafała Raczko

Warszawa 2017

STRESZCZENIE

Niniejsza praca dyplomowa ma na celu zobrazowanie zjawiska zagrożeń informatycznych od rysu historycznego do najnowszych trendów. Omówiono analizę zagrożeń oraz metody przeciwdziałania im. Zdefiniowano zjawisko rozpoznania zagrożeń cybernetycznych oraz zaproponowano budowę platformy do analizy, gromadzenia i wymiany informacji służących rozpoznaniu zagrożeń cybernetycznych w oparciu o aplikacje typu Open Source.

SUMMARY

This thesis aims to illustrate the phenomenon of computer threats from the historical overview to the latest trends. The analysis of threats and methods of counteracting them was discussed. The phenomenon of cybernetic threats was defined and proposed to build a framework for the analysis, collection and exchange of information for the detection of cyber threat intelligence based on Open Source applications.

SPIS TREŚCI

Wstęp

Charakter zagrożeń cyfrowych bardzo się zmienił od początku upowszechnienia się informatyzacji. W pierwszych latach istnienia komputerów osobistych hakerzy tworzyli wirusy komputerowe i dokonywali włamań głownie dla zabawy lub sławy. Sporządzali złośliwe oprogramowanie i przełamywali zabezpieczenia komputerowe głównie po to aby udowodnić, że potrafią to zrobić, albo przekazać jakiś komunikat. Dziś jest to duża gałąź nielegalnego biznesu lub narzędzie do prowadzania ataków na inne państwa. Już w 2011 r. w firma Norton w swym raporcie na temat cyberprzestępczości doniosła, iż we wrześniu 2011 dochód, osiągany z cyberprzestępczości przekroczył dochód osiągany z handlu narkotykami (Parnell, 2011). Jako pierwszy cyberatak na państwo uznaje się zmasowany atak hackerów na instytucje administracji rządowej, media i banki w Estonii.[1] Nic więc dziwnego że NATO, na szczycie w Warszawie w lipcu 2016 r postanowiło włączyć cyberprzestrzeń jako kolejny obszar działań operacyjnych, ze wskazaniem kluczowego elementu cyberprzestrzeni przy prowadzeniu wojny hybrydowej (Cyberdefence 24, Andrzej Kozłowski, 2016). By zwalczać narastające i ciągle zmieniające się niebezpieczeństwa pochodzące z cyberprzestrzeni potrzebne będą narzędzia do analizy tychże zagrożeń, a także dzielenia się wiedzą o nich z innymi, po to by chronić nasze domy, firmy i urzędy. Niniejsza praca jest próbą stworzenia środowiska do badania i dzielenia się wiedzą o malware i atakach sieciowych – systemu składającego się z wielu współdziałających aplikacji udostępnianych na otwartej licencji co nie jest bez znaczenia w instytucjach państwowych lub małych przedsiębiorstwach. Aplikacje te na bieżąco będą pobierać dane z wielu instytucji i organizacji zajmujących się bezpieczeństwem teleinformatycznym oraz monitorowaniem sieci pod kątem zagrożeń. Oprogramowanie to także może być źródłem informacji dla jednostek podległych bądź partnerów i organizacji stowarzyszonych. Zdefiniowano następującą tezę, iż platformy do analizy, gromadzenia i wymiany informacji służących rozpoznaniu zagrożeń cybernetycznych, mają realny wpływ na poprawę bezpieczeństwa głównie dzięki sprawnej wymianie informacji o źródłach, celach, technikach i taktykach stosowanych przez cyberprzestępców.

[1] Eksperci oceniają, że zmasowany atak, który trwał około trzech tygodni począwszy od 17 maja 2007 roku rozpoczął się po ostrym sporze Tallina z Moskwą wokół usunięcia radzieckiego pomnika z centrum Tallina, Rosja oczywiście zaprzeczyła jakiemukolwiek udziałowi w blokadzie serwerów Estonii. (The Guardian, Ian Traynor , 2007)

ROZDZIAŁ I. Cyfrowe zagrożenia

W dzisiejszych czasach hakerzy coraz rzadziej włamują się do sieci pokonując skomplikowane zabezpieczenia, firewalle, sondy sprawdzające anomalie w sieci. Znacznie łatwiej, szybciej i z dużo mniejszym ryzykiem wykrycia, mogą dostać się do środka organizacji skłaniając użytkownika do kliknięcia na spreparowany link, otwarcie dokumentu lub użycie klucza USB. Użytkownik wtedy uruchamia złośliwy program, który może usunąć bądź zaszyfrować efekty pliki na komputerze bądź wykraść je wysyłając na inny serwer. Dzięki akcjom phisingowym[2] mogą próbować przesłać automatycznie swój złośliwy kod do milionów użytkowników na całym świecie, tak masowa próba przełamania zabezpieczeń w klasyczny sposób była by niemożliwa.

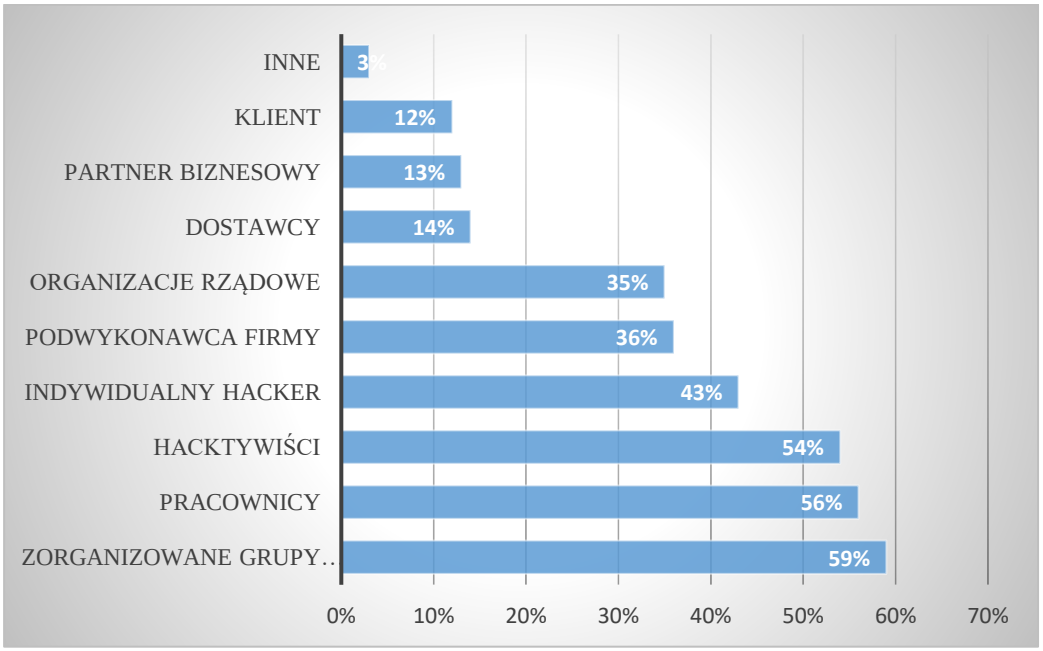
Szacowane koszty ataków ransomware, czyli złośliwego oprogramowania szyfrującego dane w roku 2016 szacowane są na ponad 1 miliard dolarów. Co sekundę 12 osób pada ofiarami cyberprzestępców, oznacza to ponad milion dziennie. Najczęściej atakowane sektory to służba zdrowia, fabryki, instytucje finansowe, urzędy i transport. W Polsce w 2016 roku 96% firm doświadczyło ponad 50 incydentów naruszenia bezpieczeństwa. Najczęstszymi formami ataku był phising (39%) oraz wykorzystanie zewnętrznego nośnika (23%) (PwC Polska, 2017). Na całym świecie w ostatnim roku konsumenci stracili przez działalność cyberprzestępców około 158 miliardów dolarów. Trzy na cztery banki z pierwszej dwudziestki największych banków w USA było zarażonych przez malware. Szacuje się, iż zyski z cyberprzestępczości mają wzrosnąć z trzech bilionów w roku 2015 do sześciu bilionów USD (Herjavec, Steve Morgan, 2016). Efektem malware są: uszkodzenia i zniszczenia danych, kradzież pieniędzy, utrata produktywności, kradzież własności intelektualnej, kradzież danych osobowych i finansowych, kradzież i usuwanie danych, utrata reputacji. Niniejszy rozdział przedstawi czym jest złośliwe oprogramowanie, jakie są jego źródła a także czy można i jak z nim walczyć.

I.1 Zagrożenia cybernetyczne

Historia sieci Internet czyli sieci rozproszonej bez wskazanego centrum sięga lat 60 XX w. lata 90 ubiegłego wieku przyniosły gwałtowną komercjalizację i rozwój tego środowiska. Wraz z rozwojem nowych usług – poczty, witryn internetowych czy

[2] Phishing to oszustwo internetowe, polegające na wyłudzeniu od użytkownika jego osobistych danych. Phishing obejmuje kradzież haseł, numerów kart kredytowych, danych kont bankowych i innych poufnych informacji.

komunikatorów rosła ilość korzystających z nich użytkowników – o ile w roku 1995 korzystało mniej niż 1 % ludzi na świecie, dziś korzysta z niej ponad trzy i poł miliarda osób co stanowi ponad 46 % światowej populacji (Worl Wide Web Consortium, 2017). W raz z rozwojem społeczeństwa informacyjnego towarzyszyło przenikanie różnych aspektów ludzkiej działalności do cyberprzestrzeni – dostęp do informacji, bankowości, zakupów, kontaktów z rodziną czy znajomymi. Niestety odzwierciedlenie fizycznej rzeczywistości w przestrzeni wirtualnej objęło także negatywne aspekty ludzkiej aktywności. Poczucie anonimowości oraz tworzące się nowe obszary nielegalnej działalności oraz agresji wobec innych podmiotów wykorzystywane jest przez przestępców, terrorystów a także wiele państw. Najczęściej motywami dzielności cyberprzestępców jest chęć zysku ale wiele osób łamie prawo za pomocą sieci także z innych pobudek – haktywiści[3] popełniają przestępstwa z pobudek ideologicznych, terroryści motywowani są politycznie. Często granice między nimi nie są ostre, incydenty przypisywane terrorystom są efektem wandalizmu, lub nieoficjalnie sponsorowane przez rządy różnych państw. Internet jako synonim dostępu do informacji jest źródłem danych wywiadowczych tak dla służb państwowych jaki dla biznesu. Internet to również kolejny obszar prowadzenia działań wojskowych tak defensywnych jak i ofensywnych. Analizę źródeł najczęstszych ataków cybernetycznych ukazuje rysunek 1, na którym widać największy udział zorganizowanych grup przestępczych w dokonywaniu cyberprzestępstw.



Rysunek 1. Źródła cyberataków. Źródło: (EY, 2015).

[3] Haktywizm to zjawisko połączenia aktywności politycznej i komputerowej , w celu zamanifestowania sprzeciwu wobec działań w sferze szeroko rozumianej polityki czy działań społecznych, a zwłaszcza wolności słowa, praw człowieka i dostępu do informacji

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki itp.);
- kradzieże tożsamości, podszywanie się pod inne osoby;
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych;
- blokowanie dostępu do usług (mail bomb, DoS[4] oraz DDoS[5]);
- spam (niechciane wiadomości elektroniczne);
- ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję);
- ataki APT.

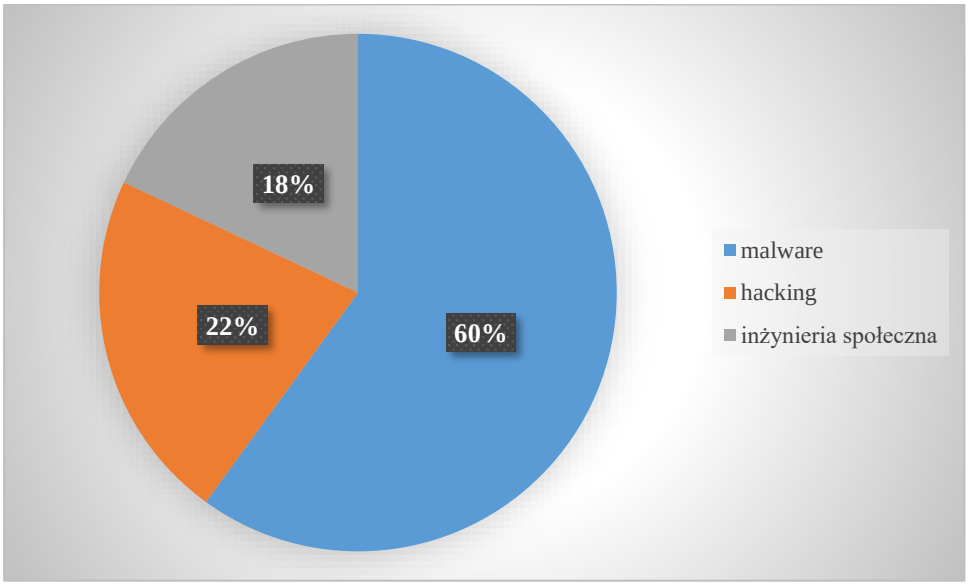
Ataki typu APT (ang. Advanced Persistent Threats) to złożone, długotrwałe I wielostopniowe działania kierowane przeciwko konkretnym osobom, firmom lub instytucjom.

- **Advanced** (zaawansowane) – ponieważ atakujący wykorzystują różne techniki i metody skutecznego przełamania zabezpieczeń, wykorzystując znane podatności, ale także wynajdując nowe, specjalnie do przeprowadzenia danego ataku,
- **Persistent** (przedłużone, trwałe, uporczywe) – ze względu na formalne zadanie przeprowadzenia skutecznego ataku. Ma on być wykonany tak, aby nie zwrócić niczyjej uwagi, a po uzyskaniu dostępu do jednego systemu ofiary poszerzyć kontrolę o kolejne, w sposób umożliwiający długotrwałą i stałą obecność oraz dozór.
- **Threat** (zagrożenie) – bowiem atakujący to zorganizowana grupa z odpowiednim zapleczem technicznym oraz budżetem. Zagrożenie jest stałe, dopóki atakujący posiada motywację (polityczną, ekonomiczną) do wykradania informacji ofiary. To nie użyte oprogramowanie jest niebezpieczne, a ludzie stojący za nim (Bejtlich, 2010).

[4] Ataki DoS (Denial of Service) mają na celu utrudnienie lub całkowite uniemożliwienie działania witryny internetowej, sieci, serwera lub innych zasobów. Typowe ataki DoS przeciążają serwery nieustającymi żądaniami powodując duże spowolnienie serwerów lub całkowitą ich blokadę

[5] Atak DDoS (Distributed Denial of service) różni się od ataku DoS jedynie tym, że przeprowadzany jest równocześnie z wielu komputerów.

Najczęściej opisuje się je jako prowadzone przez atakujących, tygodniami lub miesiącami zbierają dane o pracownikach danej firmy lub organizacji, by po jakimś czasie przystąpić do planowanego ataku. Wykorzystywane przez nich aplikacje i narzędzia są tworzone i użytkowane w sposób ukrywający wykrycie złośliwej aktywności przez ofiarę. Z tego powodu mogą bez przeszkód wykradać informacje przez długi czas. Ataki typu APT różnią się od najczęściej obserwowanych szybkich ataków na instytucje trudnością w wykryciu oraz szerokim zasięgiem. Przeprowadzają je zazwyczaj zorganizowane grupy lub państwa dysponujące znacznymi budżetami oraz czasem pozwalającym na zinfiltrowanie konkretnego celu – firmy bądź instytucji – a następnie precyzyjnego przeprowadzenia ataku, którego celem najczęściej jest kradzież wrażliwych danych lub rzadziej uszkodzenie systemu komputerowego.



Rysunek 2. Źródła złośliwych naruszeń bezpieczeństwa. Źródło (Verizon, 2016).

Wspólnym mianownikiem większości ataków cybernetycznych jak to ukazuje rysunek 2 jest złośliwy kod podrzucany ofierze w wiadomości phisingowej, znajdujący się na zmodyfikowanej witrynie internetowej, przeniesiony na nośniku pamięci. Kod taki może potem wykraść dane (wrażliwe, bankowe, poufne) lub zaszyfrować je żądając okupu, może także wykorzystać zainfekowany komputer lub urządzenie jako narzędzie do ataku na inne w postaci wysyłania spamu, ataków DoS, DDoS, lub wykorzystać jako stację pośredniczącą w przesyłaniu zakazanych treści (np. pornografii dziecięcej).

I.2 Historia malware

Za pierwszy „atak hackerski” tygodnik New Science uznaje przejęcie pasma radiowego przez brytyjskiego magika Nevila Maskelyne’go, podczas pokazu telegrafu

radiowego Gugliemo Marconiego w sali The Royal Institution w roku 1903. Marconi chciał zaprezentować swój wynalazek przesyłający bezpieczne i bezprzewodowo wiadomości na długie dystanse. W tym celu ustawił swoje urządzenie nadające w Kornwalii, zaś odbiornik zainstalowano w londyńskim teatrze około 480 km dalej. Zgromadzona publiczność z niecierpliwieniem oczekiwała na pokaz. Jednak przed rozpoczęciem transmisji brytyjski fizyk John Fleming - współpracownik Marconiego zauważył, że odbiornik zarejestrował pewne wiadomości przesłane alfabetem Morse'a,: *„szczury, szczury, szczury"*. Później kilka wersów z Szekspira i parę obelg skierowanych przeciw Marconiemu. Maskelyne chciał udowodnić, iż przesyłanie informacji telegrafem nie jest bezpieczne, można przejąć informację i nadać zmodyfikowaną (Marks, 2011).

Historia defektów oprogramowania komputerowego, ataków i wirusów jest tak stara jak sam przemysł komputerowy. Pierwszym opisanym problemem była ćma, która w roku 1947 dostała się do styków przekaźnika jednej z pierwszych rządowych maszyn cyfrowych MARK II powodując jego błędne działanie. Pani porucznik Grace Hopper wydobyła ją i zgodnie z przepisami załączyła do raportu. Owad[6] ów, stał się źródłem słowa „debugowanie" (odpluskwianie) czyli analizy błędów w oprogramowaniu. Grace Hopper zakończyła służbę w stopniu kontradmirała i zasłynęła jako twórca języka COBOL.

Według felietonisty i konsultanta do spraw komputeryzacji, Roba Rosenbergera, początki wirusów komputerowych sięgają roku 1949. Wtedy to właśnie John von Neumann, pionier informatyki, opublikował swoją pracę „*Theory and Organization of Complicated Automata*", w której wysunął postulat, że program komputerowy potrafi się powielać. W roku 1950, w laboratoriach Bella, naukowcy wprowadzili w życie ideę von Neumanna, pisząc grę komputerową o tytule *Core Games*. Jej reguły byłby proste; dwóch programistów uwalniało komputerowe „organizmy", które następnie walczyły o przejęcie kontroli nad komputerem. Gra została opisana w trzech artykułach pisma „Scientific American" w latach 1983 i 1984. Gene Spafford z uniwersytetu Purdue uznaje, że twórcą określenia „wirus" był David Gerrold, który posłużył się tym określeniem w swoich powiadaniach science fiction o losach maszyny G.O.D.5. (Lehtinen, et al., 2007)

Drugiego października 1988 r. Robert Morris student Uniwersytetu w Cornell stworzył program składający się z 99 linii, który miał, w założeniu autora „zmierzyć rozmiar Internetu". Wykorzystywał on 3 luki w oprogramowaniu, hasła dostępowe do serwerów łamał metodą siłowa dysponując słownikiem składającym się jedynie z 400 słów. Po pomyślnym wniknięciu do systemu robak m.in. sprawdzał czy jego kopia jest już uruchomiona w systemie, losowo (algorytm rzutu kostką) wybierał, która z nich ma pozostać w systemie, a która miała ulec samozniszczeniu. Jedna na siedem kopii Morrisa rezygnowała z „rzucania kostką" i działała

[6] Eksponat w postaci dziennika z wklejoną ćmą można zobaczyć obecnie w The Smithsonian Institute National Museum of American History.

dalej, niezależnie od innych obecnych wersji. Nie wiadomo, czy był to błąd w kodzie, czy próba zwiększenia szans na przeżycie robaka w systemie, jednak właśnie takie działanie prowadziło do „zatkania" zainfekowanej maszyny, co jest wczesnym atakiem DoS – na wielu komputerach jednocześnie działy dziesiątki kopii Morrisa. W efekcie zainfekowane zostało 6000 komputerów czyli 10 % z wszystkich podłączonych wówczas do Internetu. Straty szacowano na kwotę pomiędzy 100 tysięcy a 10 milionów dolarów, autor po przyznaniu się do winy został skazany na 3 lata w zawieszeniu, 10 000 dolarów grzywny oraz 400 godzin prac społecznych. Morris obecnie jest profesorem MIT (Kaspersky, Lab, 2013)

Za jeden z pierwszych wirusów infekujących komputery klasy IBM PC uważa się Brain, stworzony w 1986 roku przez braci 24 letniego Amjada i 17 letniego Basita Farooqa Alviego i z pakistańskiego miasta Lahore. Ich wirus miał być zupełnie nieszkodliwy, a jego celem było powstrzymanie ludzi przed kopiowaniem oprogramowania, nad którym bracia pracowali przez kilka lat. Brain infekował sektor rozruchowy dyskietki, zapobiegając kopiowaniu oraz umożliwiał jego twórcom śledzenie nielegalnych kopii ich programu. Bracia zmartwieni faktem, iż ludzie kradną ich oprogramowanie, zapisali w kodzie wirusa komunikat, który wyświetlał się na ekranach zainfekowanych komputerów:

```
Welcome to the Dungeon © 1986 Brain & Amjads (pvt). BRAIN COMPUTER SERVICES 730
NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791, 443248, 280530.
Beware of this VIRUS… Contact us for vaccination.
```

Co ciekawe autorzy podali kontakt do siebie a nawet stwierdzili, iż wirus chroniony jest prawem autorskim (Goodman, 2016). Od tego czasu twórcy wirusów stali się coraz bardziej sprytni oraz złośliwi, dodatkowo możliwość kontaktowania się użytkowników za początkowo za pomocą modemów i skrzynek BBS, później grup dyskusyjnych i pierwszych dostawców Internetu sprawiła, iż wirusy nie musiały już się rozprzestrzeniać „trampkonetem" (sneakersnet) – czyli osobami przenoszącymi nośniki danych, najczęściej dyskietki.

Pierwszym opisanym kinetycznym[7] efektem działania komputerowego konia trojańskiego była potężna eksplozja w ZSRR gazociągu transsyberyjskiego. Za eksplozję odpowiedzialne miało być CIA, które do przeprowadzenia sabotażu użyło zmodyfikowanego oprogramowania komputerowego. Stojący na czele Departamentu Sił Powietrznych w administracji Ronalda Reagana Thomas Reed w swoich wspomnieniach – w książce „*At the Abyss: An Insider's History of the Cold War*" opisał akcję, którą, jak twierdził, przeprowadziła CIA. Na podstawie informacji przekazanych przez Władimira Wetrowa, pracownika I Zarządu Głównego KGB, francuskiemu wywiadowi, CIA ustaliła, że Sowieci chcą wykraść oprogramowanie niezbędne do obsługi gazociągu z jednej z kanadyjskich firm. Amerykańscy agenci skłonili więc firmę, która znalazła się na celowniku KGB, do przygotowania

[7] Cyberatak kinetyczny to atak powodujący rzeczywiste fizyczne zniszczenia w infrastrukturze lub narażający życie ludzi.

zmodyfikowanej wersji oprogramowania, zawierającej tak zwaną logiczną bombę, czyli lukę w kodzie, dzięki której pozornie poprawnie działający program, po określonym czasie miał doprowadzić do katastrofy. Z książki Reeda wynika, że plan udało się w pełni zrealizować. Sowieci wykradli wadliwe oprogramowanie, które następnie zostało użyte do obsługi turbin, zaworów bezpieczeństwa oraz pomp w gazociągu. W momencie uaktywnienia się logicznej bomby oprogramowanie ustawiło pompy, turbiny i zawory tak aby ciśnienie gazu przekroczyło dopuszczalne parametry łączeń i spawów, co doprowadziło do gwałtownego wzrostu ciśnienia, którego efektem była potężna eksplozja. Zarejestrowały ją nawet amerykańskie satelity, a Dowództwo Obrony Północnoamerykańskiej Przestrzeni Powietrznej i Kosmicznej początkowo było przekonane, że w rejonie gazociągu doszło do zdetonowania bomby atomowej, jednakże nie zanotowano impulsu elektromagnetycznego, który by świadczył o wybuchu nuklearnym. Nie było ofiar w ludziach gdyż gazociąg przebiegał przez niezamieszkaną część Syberii, ale straty spowodowane całą akcją uderzyły w radziecką gospodarkę, dla której bardzo ważne były dewizy uzyskiwane ze sprzedaży gazu do Europy Zachodniej. Po ujawnieniu w 2004 roku przez Reeda szczegółów operacji pojawiły się wątpliwości, czy faktycznie miała ona miejsce. Rosyjskie media dotarły między innymi do oficera KGB w stanie spoczynku, który twierdził, że w 1982 roku faktycznie doszło do eksplozji gazociągu na Syberii, ale z powodu błędów konstrukcyjnych. (The New Yor Times, William Safire, 2004).

Pierwszy publiczny i motywowany politycznie atak DDoS przeprowadzono już 1994 roku, gdy grupa określająca się jako Zippies postanowiła zaprotestować 5 listopada (na ten dzień przypada angielskie święto zwane dniem Guya Fawkesa) przeciwko nowemu prawu zakazującemu organizacji imprez z mocną muzyką elektroniczną. Zaatakowane rządowe witryny zostały wyłączona na niemal tydzień. Nikt wówczas nie wiedział, w jaki sposób obronić się przed nowym zagrożeniem (Świechowski, 2011).

I.3 Definicja i taksonomia malware

Złośliwe oprogramowanie, zwane czasami również szkodliwym, malware (z ang. *malicious software*) lub szkodnikiem to wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze, groźne lub destrukcyjne działanie w stosunku do użytkownika komputera (Wikipedia Fundation, 2017).

Do szkodliwego oprogramowania zalicza się:

- **Backdoor** – przejmuje kontrolę nad zainfekowanym komputerem, umożliwiając wykonywanie na nim wszystkich czynności. Wykonuje wtedy działania wbrew wiedzy i woli ofiary. Najczęściej pozwala na łączenie się atakującemu bez jakiejkolwiek autentykacji.

- **Botnet** – podobny do backdoora, w tym, że pozwala na łączenie się atakującemu z zewnątrz z tą różnicą, że wszystkie komputery w tym samym botnecie odbierają i wykonują te same instrukcje z jednego serwera zarządzającego (*command–and–control*[8]).

- **Downloader** – Złośliwy program, którego jedynym zadaniem jest pobranie innego złośliwego kodu. Downloader zwykle jest instalowany przez atakującego po osiągnięciu dostępu do systemu aby pobrać inne złośliwe programy.

- **Programy szpiegujące i wykradające** (ang. *spyware*) – oprogramowanie zbierające dane o osobie lub organizacji bez jej zgody, takie jak informacje o odwiedzanych witrynach, hasła dostępowe, dane o kontach bankowych itp. Programy szpiegujące mogą wykonywać działania bez wiedzy użytkownika – zmieniać wpisy w rejestrze systemu operacyjnego i ustawienia użytkownika. Program szpiegujący może pobierać i uruchamiać pliki pobrane z sieci.

- **Launcher** – program uruchamiający inny złośliwy program w celu ukrycia pewnych funkcji lub zwiększenia uprawnień do systemu.

- **Rootkit** – jedno z najbardziej groźnych narzędzi hakerskich. Ogólna zasada działania opiera się na maskowaniu obecności pewnych uruchomionych programów lub procesów systemowych (z reguły służących hakerowi do administrowania zaatakowanym systemem). Rootkit zostaje wkompilowany (w wypadku zainfekowanej instalacji) lub wstrzyknięty w istotne procedury systemowe. Z reguły jest trudny do wykrycia z racji tego, że nie występuje jako osobna aplikacja. Zainstalowanie rootkita jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie ukryta kradzież danych lub infiltracja.

- **Scareware** – malware zaprojektowane aby zastraszyć użytkownika w celu dokonania zakupu czegoś lub wykonania określonej czynności (np. zalogowania się do określonej witryny)

- **Spam–sender** – oprogramowanie wysyłające spam

- **Wirus** – program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu powielania samego siebie bez zgody użytkownika. Ze względu na różne rodzaje infekcji wirusy dzielą się na:

    - wirusy gnieżdżące się w sektorze rozruchowym dysku twardego (ang. *boot sector viruses*),

    - wirusy pasożytnicze (ang. *parasitic viruses*),

---

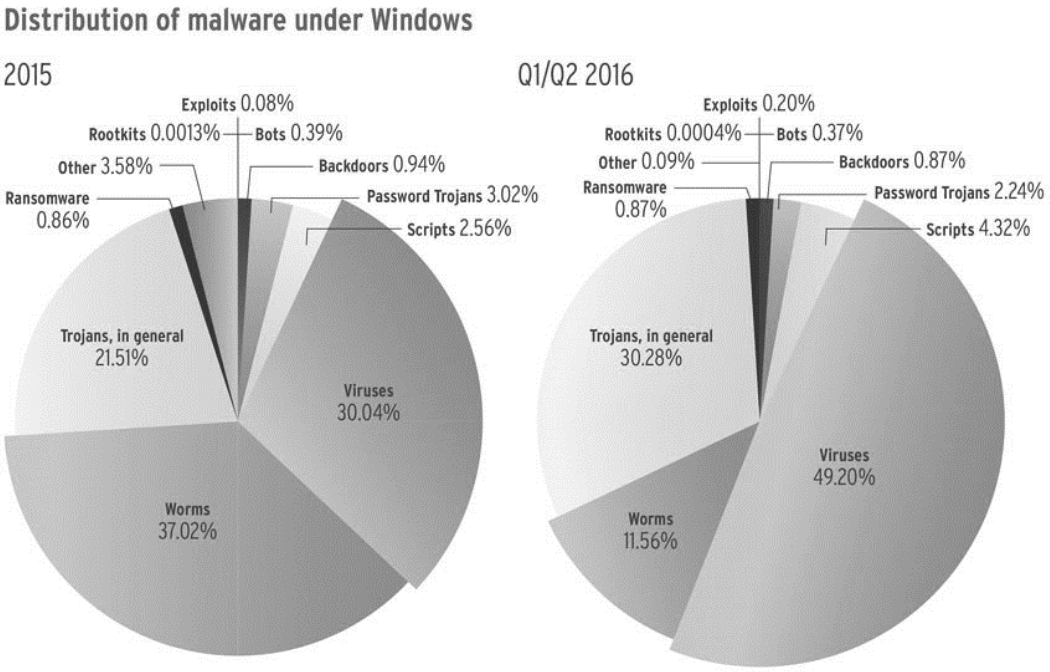
[8] Serwer Command and Control, C&C, C2 - serwer służący do koordynowania działań komputerów zainfekowanych botami, rootkitem, robakiem lub innymi formami złośliwego oprogramowania. Serwer C&C przesyła aktualizacje, wydaje instrukcje zakażonym komputerom jakie informacje wykraść i przesłać, jakie serwery zaatakować.

    - wirusy wieloczęściowe (ang. *multipartite viruses*),
    - wirusy towarzyszące (ang. *companion viruses*),
    - makrowirusy (ang. *macro viruses*).
- **Robaki** (ang. *worm*) – szkodliwe oprogramowanie podobne do wirusów, rozprzestrzeniające się tylko poprzez sieć. W przeciwieństwie do wirusów nie potrzebują programu „żywiciela". Często powielają się pocztą elektroniczną.
- **Wabbit** – program rezydentny niepowielający się przez sieć. Wynikiem jego działania jest jedna określona operacja, np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera.
- **Trojan** – nie rozmnaża się jak wirus, ale jego działanie jest równie szkodliwe. Ukrywa się pod nazwą lub w części pliku, który może wydawać się pomocny, jednak po uruchomieniu wcale nie pełni tej funkcji, której spodziewa się użytkownik. Trojan wykonuje w tle operacje szkodliwe dla użytkownika, np. otwiera port komputera, który może umożliwić późniejszy atak ze strony włamywacza (hakera).
- **Ransomware** – ogranicza dostęp do systemu komputerowego np. szyfrując wszystkie dokumenty i zdjęcia i wymaga zapłacenia okupu, aby ograniczenie zostało usunięte.
- **Scumware** (ang. *scum* – piana; szumowiny, męty) – żargonowe, zbiorcze określenie oprogramowania, które wykonuje w komputerze niepożądane przez użytkownika czynności.
- **Stealware/parasiteware** – służące do okradania kont internetowych,
- **Adware** – oprogramowanie wyświetlające reklamy,
- **Hijacker Browser Helper Object** – dodatki do przeglądarek, wprowadzające zmiany w konfiguracji bez wiedzy użytkownika.
- **Exploit** – kod umożliwiający bezpośrednie włamanie do komputera ofiary. Do wprowadzenia zmian lub przejęcia kontroli wykorzystuje się lukę w oprogramowaniu zainstalowanym na atakowanym komputerze. Exploity mogą być użyte w atakowaniu witryn internetowych, których silniki oparte są na językach skryptowych (zmiana treści lub przejęcie kontroli administracyjnej), systemów operacyjnych (serwery i końcówki klienckie) lub aplikacji (pakiety biurowe, przeglądarki internetowe lub inne oprogramowanie).
- **Keylogger** – odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody i inne poufne dane mogą dostać się w niepowołane ręce. Keyloggery mogą występować również w postaci sprzętowej.
- **Dialery** – programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika lub dzwoniące bez wiedzy użytkownika z telefonu komórkowego. Najczęściej są to numery o podwyższonej opłacie za połączenie, numery zagraniczne.

Mniej poważny malware to:

- fałszywe alarmy dotyczące rzekomo nowych i groźnych wirusów (ang. false positives); fałszywe alarmy to także nieprawidłowe wykrycia szkodliwych plików, które mogą generować programy antywirusowe, szczególnie na najwyższym poziomie analizy heurystycznej.
- żarty komputerowe, robione najczęściej nieświadomym początkującym użytkownikom komputerów (Sikorski & Honig, 2013), (Wikipedia Fundation, 2017).

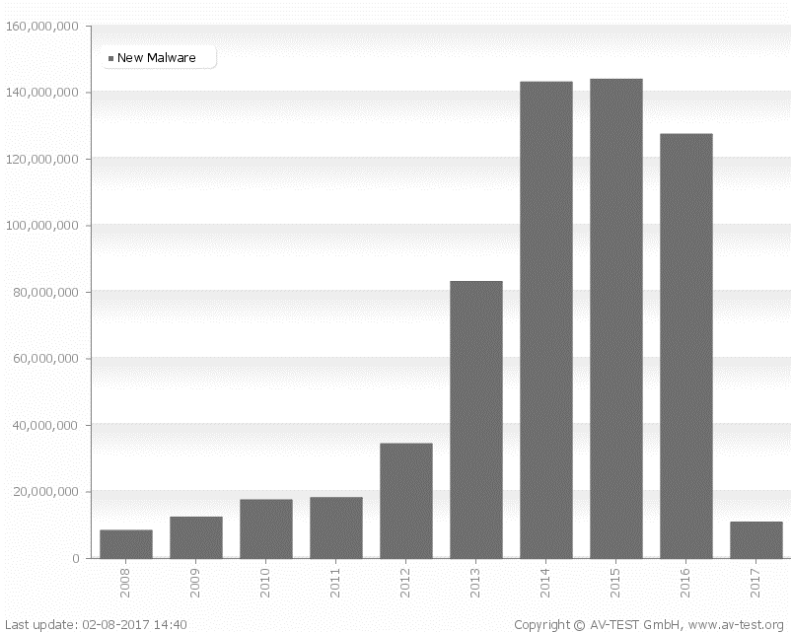
Oczywiście granice pomiędzy różnymi rodzajami malware nie są ostre, często złośliwe programy mają kilka z powyższych cech, niekiedy bywa wręcz, że malware posiada różne cechy w zależności w jakim środowisku jest uruchomiony. Jak widać na rysunku 3 taksonomia dość dynamicznie zmienia się w czasie.



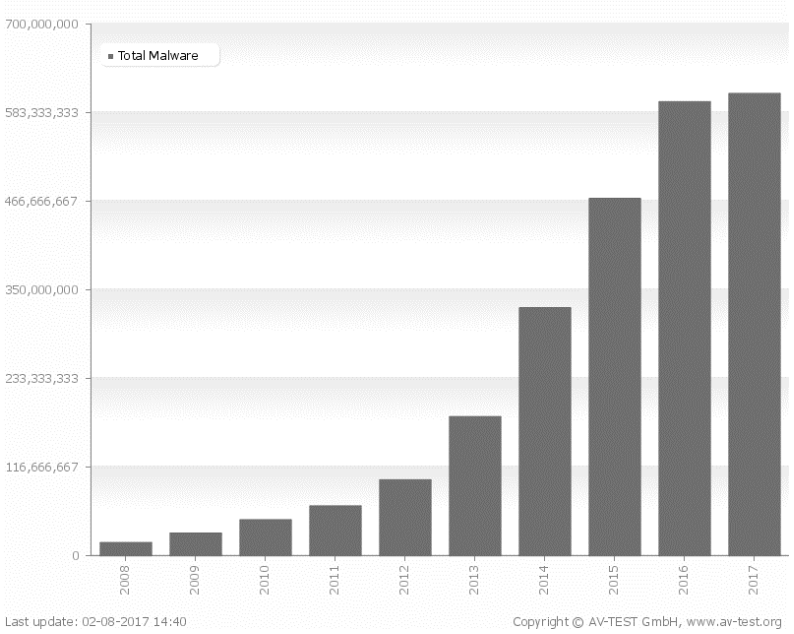
Rysunek 3. Taksonomia malware 2015–2016. Źródło: (AV-TEST, 2016).

Według niezależnej organizacji oceniającej oprogramowanie antywirusowe AV–TEST z Magdeburga dziennie pojawia się około 390 tysięcy nowych wirusów – co daje średnio pięć na sekundę (AV-TEST, 2017). Bardzo niepokojąca jest dynamika wzrostu tworzonego nowego malware, co obrazuje rysunek 4. Badacze malware odnotowują ponad 500 różnych technik służących do omijania wykrywania przez antywirusy, przy czym średnia ilość technik unikania wykrycia na jedną próbkę wynosi (Krugel, 2015). Aż 97% złośliwego oprogramowania ma unikalny charakter dla danego rodzaju działania, czyniąc bezpieczeństwo oparte na sygnaturach praktycznie bezużytecznym, dodatkowo z wszystkich pojawiających się nowych plików w sieci 15% to wykonywalny malware, jednocześnie badacze raportują, iż ufać można jedynie około 55% odwiedzanych witryn web (WEBROOT, 2016). Jeden z założycieli firmy Intel, Gordon Moore 19 kwietnia 1965 roku na łamach "Electronics Magazine"

sformułował prawo, które pierwotnie odnosiło się do rozwoju mikroelektroniki i mówiło iż „"Złożoność komponentów o minimalnych kosztach będzie się podwajała co roku..” okazało się, że prawo to doskonale przystaje do całego postępu w technologii (później Moore zrewidował czasokres do 18–24 miesięcy) (Bigo, 2006). Jeżeli się spojrzy na rysunek 5 (całkowita ilość malware) można zauważyć ze prawo Moore’a również w pełni opisuje rozwój złośliwego oprogramowania.



Rysunek 4. Ilość zupełnie nowych próbek malware pojawiających się w ciągu roku. Źródło (AV-TEST, 2017).



Rysunek 5. Ogólna ilość próbek pojawiających się w ciągu roku. Źródło: (AV-TEST, 2017).

Znana polska badaczka malware Joanna Rutkowska, autorka całkowicie nie wykrywalnego rootkita Blue Pill na konferencji Black Hat w roku 2006 przedstawiła prezentację, w której zdefiniowała malware jako część kodu, która zmienia zachowanie jądra systemu operacyjnego bądź czułość/skuteczność aplikacji zabezpieczających system bez świadomości użytkownika i w taki sposób, by operacje te były trudne do wykrycia. Podzieliła także malware na 4 typy (Rutkowska, 2006):

- **TYP 0** – Złośliwe oprogramowanie jako proces nie wchodzi w interakcje z żadną częścią systemu ani innymi procesami w nieautoryzowany sposób. Może jednak kasować pliki i dane z lokalizacji użytkownika lub też otwierać porty TCP, by komputer stał się częścią botnetu. Zasadniczym wyznacznikiem jest jednak to, że złośliwy kod nie kompromituje systemu operacyjnego i nie zmienia zachowania innych aplikacji oraz procesów uruchomionych w pamięci. Malware zostało przedstawione jako niezależnie działający proces.

- **TYP 1** – w systemie operacyjnym istnieją zasoby relatywnie stałe, lub takie które powinny być stałe (np. tylko do odczytu) oraz takie, które zmieniają się cały czas podczas działania systemu i wykonywania w nim różnorakich operacji. Do grupy pierwszych zasobów można zaliczyć pliki, np. wykonywalne, kod biosu, czy zawartość pamięci EEPROM. Z kolei do grupy zasobów zmiennych należą m.in. niektóre pliki konfiguracyjne oraz klucze rejestru systemowego a także, przede wszystkim sekcje danych działających procesów oraz jądra. Złośliwe oprogramowanie, które modyfikuje powyżej przedstawione zasoby stałe, klasyfikowane jest jako malware typu I. Konsekwentnie, złośliwy kod, który nie modyfikuje zasobów stałych, a wchodzi w interakcję z zasobami naturalnie zmiennymi (jak sekcje danych) jest klasyfikowane jako malware typu II. Według Joanny Rutkowskiej, wykrywanie złośliwego oprogramowania typu I powinno odbywać się za pomocą sprawdzania integralności zasobów stałych, by móc jednoznacznie stwierdzić, czy nie zostały one zmienione przez złośliwy kod. Metodą jaką jest sprawdzanie integralności danych wymuszające posiadanie odniesienia, z którym obiekty będą porównywane. W przypadku systemów operacyjnych z rodziny Windows nie ma z tym problemu ponieważ wzorce takie są dostępne (pliki EXE, SYS, DLL, itp.) i są podpisane cyfrowo przez korporację Microsoft.

- **TYP II** – malware typu II nie zmienia stałych zasobów systemu (sekcje kodu), lecz wchodzi w interakcję z zasobami dynamicznymi, takimi jak sekcje danych (np. poprzez modyfikowanie wskaźników funkcji w niektórych strukturach danych jądra, co pozwala wykonać złośliwy kod zamiast oryginalnego kodu systemu lub danego programu). W celu wykrycia złośliwego programowania typu II, należałoby przeanalizować całą sekcję danych należącą nie tylko do jądra i wszystkich sterowników, ale także do aplikacji zabezpieczających uruchomionych w systemie operacyjnym oraz stworzyć listę wszystkich wrażliwych na modyfikację obszarów. Proces ten mógłby okazać się bardzo skomplikowany, a przede wszystkim długotrwały, więc rozwiązanie problemu leżałoby częściowo po stronie producentów systemów oraz oprogramowania –

należałoby zadbać o odpowiednie oznakowanie wrażliwych struktur danych oraz oprogramowania zabezpieczającego w celu automatycznego sprawdzenia ich integralności.

- **TYP III** – Joanna Rutkowska tworząc Blue Pill dowiodła, iż możliwym jest stworzenie malware, które może przejąć kontrolę nad systemem operacyjnym bez zmian pamięci systemu oraz rejestrów sprzętowych. Malware tego typu dotyczy wirtualizacji na niskim poziomie, czyli przy użyciu hipernadzorcy (*hypervisor*) służącego do przeprowadzania procesu wirtualizacji i kontrolującego dostęp do zasobów sprzętowych. Najważniejszym problemem dotyczącym malware typu III jest to, że przez brak ingerencji w kod systemu i jądra, nie ma żadnej relacji prowadzącej do złośliwego kodu, który jest całkowicie odłączony od kodu systemu. Może rezydować w pamięci operacyjnej ale wygląda jak zupełnie losowe dane, wiec nie zostanie wykryty przez skaner integralności. Wykrycie malware typu III możliwe było by tylko przez obserwowanie skutków wprowadzanych w systemie. jednakże praktyczną metodą obrony przed tego typu malware była by jedynie prewencja.

I.4 Antywirus

Antywirusy to najpopularniejszy rodzaj oprogramowania chroniącego przed malware. Program antywirusowy to najczęściej rezydentny program–monitor śledzący wszystkie zdarzenia i procesy uruchomione w systemie komputerowym. Z jednej strony antywirusy są wstanie rozpoznać tysiące różnorakich złośliwych aplikacji a z drugiej zaś strony, bardzo łatwo je obejść i oszukać. Najważniejsze części każdego współczesnego programu antywirusowego to silnik oraz baza wzorców tzw. sygnatur wirusów. Sygnatury wirusów to informacje, które umożliwiają zidentyfikować dany typ lub nawet całą rodzinę wirusów. Najczęściej stosowane typy sygnatur to:

- sygnatury, które powstały przez wykorzystanie funkcji skrótu (hash),
- sygnatury bajtowe,
- sygnatury heurystyczne.

Najprostszą oraz najłatwiejszą do praktycznego zastosowania metodą tworzenia sygnatur złośliwego oprogramowania jest oczywiście wykorzystanie do tego celu popularnych funkcji skrótu. Tzw. skrót (hash) powstaje w wyniku zastosowania matematycznej funkcji, która to w praktyce pozwala na przyporządkowanie dowolnie dużej liczbie czyli np. dowolnemu programowi pewnej stosunkowo niewielkiej wartości o ustalonym rozmiarze. Tak utworzony hash dla znanego już złośliwego programu pozwala w przyszłości na w miarę jednoznaczne zidentyfikowanie danego wirusa. Zastosowanie tego typu sygnatur niesie ze sobą duże wady. Najmniejsza nawet zmiana w kodzie malware (nowy wariant wirusa, malware polimorficzny czyli zmieniający się przy każdym skopiowaniu) oznacza, że stara sygnatura nie wykryje nowych wersji wirusa. Poza tym, kolizje funkcji skrótu czyli przypadek, gdy różne

programy może mieć taki sam skrót jak malware mogą być przyczyną wykryć fałszywych (ang. *false positive*). Wszystko to powoduje, że aplikacje antywirusowe nie mogą polegać jedynie na tego typu sygnaturach.

Pewnym rozwiązaniem w przypadku malware'u polimorficznego lub złośliwych plików zawierających zmienne dane może być natomiast tzw. *fuzzy hashing*. Metody te generalnie pozwalają na utworzenie wspólnej sygnatury dla różnych danych wejściowych, które to jednak zawierają pewne wspólne. W pewnych przypadkach można jednak przyjąć, że pliki są podobne, gdy mają dużo podobnych fragmentów Tego typu metody są jednak dość wymagające pod względem obliczeniowym oraz nie gwarantują wcale bardzo dużej skuteczności. Obecnie istnieją bazy *known good* i *known bad*, zawierające informacje o znanych plikach, zarówno dobrych jak i złych. Podczas analizy pozwalają one na prostszą identyfikację tych plików, na które należy zwrócić uwagę jak i plików, które można zignorować podczas analizy. Zarówno dobre, jak i złe pliki mutują. W przypadku dobrych plików, jest to najczęściej poprawka, w przypadku tych złych np. modyfikacja wirusa. Wykorzystanie tego typu narzędzi pozwala uniezależnić się od bazy dokładnych sum kontrolnych i korzystać z logiki rozmytej. Można mieć na przykład bazę znanego złego oprogramowania i z jej pomocą identyfikować pliki podobne, które są być może nowymi wersjami znanych złośliwych programów.

Kolejnym sposobem generowania sygnatur złośliwego oprogramowania jest wykorzystywanie wybranych sekwencji bajtów obecnych w złośliwym kodzie lub w wykorzystywanych przez niego danych. Identyczne wzorce możemy zazwyczaj odnaleźć we wszystkich wariantach danego złośliwego programu, dlatego też metoda ta jest w praktyce dość skuteczna w walce z całymi rodzinami wirusów. Prostota tej metody sprawia, że jest ona wykorzystywana od pierwszych programów antywirusowych do dziś.

Współczesne programy antywirusowe wykorzystują również algorytmy heurystyczne. Heurystyka (gr. *heuresis* – odnaleźć) to metoda znajdowania rozwiązań, dla której nie ma gwarancji znalezienia rozwiązania optymalnego, a nawet prawidłowego. Algorytmów tych używa się np. wtedy, gdy pełny algorytm jest z przyczyn technicznych zbyt kosztowny, trwał by za długo lub gdy jest nieznany. Mimo, iż w pewnym sensie jest to algorytm „niepełnowartościowy" używa się go jeśli w akceptowalnym czasie umożliwia znalezienie dostatecznie dobrego, przybliżonego rozwiązania Generalnie mianem metod heurystycznych określa się w przypadku antywirusów wszystkie inne metody wykrywania zagrożeń, oprócz powyższych tradycyjnych metod sygnaturowych. Metody heurystyczne stanowią najbardziej skomplikowaną część metodologii każdego programu antywirusowego. Ponadto praktycznie każdy producent antywirusów rozwija własne zastrzeżone algorytmy heurystyczne i zwykle w tej dziedzinie w największym stopniu może się wykazać swą innowacyjnością i potencjałem zwykle tradycyjne sygnatury są niemal identyczne w przypadku wielu różnych producentów. Wiele firm wymienia się swoimi sygnaturami za pośrednictwem platform, jak na przykład VirusTotal.

Sygnatury heurystyczne polegają na sprawdzaniu wywołań API, śledzeniem zachowania poszczególnych programów, kontaktowania się z określonymi serwisami w sieci, śledzenia anomalii w systemie lub systemie plików (Smol, 2013).

I.5 Ataki zero–day i FUD

Z atakami typu *zero–day* mamy do czynienia, gdy informacja o błędach w oprogramowaniu nie jest publikowana, gdyż jej odkrywca sprzedaje ją cyberprzestępcom, a producent dowiaduje się o niej dopiero wtedy, gdy jest ona od pewnego czasu wykorzystywana do ataków. Niestety antywirusy głównie bazujące na różnorakich sygnaturach blokują złośliwy kod jedynie wtedy gdy jest podobny do innego już znanego.

FUD oznacza całkowicie niewykrywalny / nieusuwalny malware, z jęz. ang. *Fully Undetecdable* lub *Fully Unremovable*. Całkowicie niewykrywalny nie odnosi się tylko do nowych i nieznanych wirusów – wystarczy kod wirusa zaszyfrować, a proces odkodowania powierzyć innej aplikacji lub procesowi. Z chwilą pierwszego ataku, który powoduje ujawnienie się malware`u, następuje wykorzystanie zero–day`a i rusza proces zdobycia próbki, analiza i zniesienie statusu FUD, następnie dystrybucja aktualizacji, która obejmuje nowy malware.

I.6 Skuteczność antywirusów

W grudniu 2012 roku eksperci z firmy o izraelskich korzeniach mającej siedzibę w kalifornijskim mieście Redwood Shores o nazwie Imperva, zajmującej się monitorowaniem bezpieczeństwa danych wraz ze studentami izraelskiego Instytutu Technologii Technion w Hajfie poddali próbie standardowe narzędzia antywirusowe. Zebrali 82 nowe wirusy komputerowe (z własnych honeypotów[9] – czyli pułapek zastawionych w sieci, oraz hackerskich forów internetowych) i uruchomili je pod okiem programów wykrywających zagrożenia, wyprodukowanych przez ponad 40 największych na świecie firm zajmujących się tworzeniem takiego oprogramowania, w tym takich gigantów jak Microsoft, Symantec, McAfee i Kaspersky Lab. Dokonali tego poprzez wysłanie ich do usługi VirusTotal. Wynik: do wykrycia zagrożenia doszło w zaledwie 5% przypadków, co oznaczało, że 95% wirusów nie zostało wykrytych (IMPERVA, 2012). Oczywiście wywiązała się dyskusja specjalistów od bezpieczeństwa oraz mocna krytyka metodologii badań ze strony producentów oprogramowania antywirusowego. Niewątpliwie, z punktu widzenia statystyki wydaje się, że zarówno dobór próby, jak i jej liczność nie stanowią podstawy do wyciągania tak daleko idących wniosków na całą badaną populację. Trzeba pamiętać, iż serwis VirusTotal korzysta

[9] Honeypot (garnek miodu) to pułapka na intruzów, która pomaga wykryć nieautoryzowane próby korzystania z systemu, nielegalne pozyskiwanie danych czy inne nadużycia. W praktyce honeypot służy do poznawania technik używanych przez atakujących, a przede wszystkim do zbierania informacji.

jedynie z silników antywirusowych, działających z poziomu wiersza poleceń czyli podstawowej wersji aplikacji testującej próbki najczęściej jedynie w oparciu o bazę znanych sygnatur. W przewarzającej większości produktów wersja działająca z wiersza poleceń nie przeprowadza analizy heurystycznej podejrzanego pliku – nie analizuje źródła jego pochodzenia, jego zachowania w systemie czy podobieństwa do innych znanych przypadków. Zresztą nawet twórcy serwisu VirusTotal informują, iż korzystanie z niego w celu jakichkolwiek testów jest „złym pomysłem" (VirusTotal, 2017). Raport Anti–Virus Comparative porównujący 18 znanych na rynku aplikacji antywirusowych podaję średnią skuteczności na poziomie 86/100 (Anty-Virus-Comparatives, 2016). Miesięczne raporty firmy AV–Test wskazują na średnią skuteczność około 97 %.

W 2012 roku specjaliści z moskiewskiej firmy Kaspersky Lab odkryli bardzo skomplikowany złośliwy program o nazwie Flame, który wykradał dane z systemów informatycznych na całym świecie przez ponad pięć lat przed wykryciem. Flame potrafił aktywować mikrofony w komputerach i nagrywać toczące się w pomieszczeniach rozmowy. Dodatkowo wykonywał regularne zrzuty ekranu i szukał telefonów w pobliżu przy pomocy protokołu Bluetooth (McElroy & Williams, 2012). Mikko Hypponen, cieszący się wielkim szacunkiem dyrektor pionu badawczego w firmie F–Secure, nazwa ten przypadek porażką branży antywirusowej i stwierdzi, że on i jego koledzy mogą być „poza ligą we własnej dyscyplinie" (Simonite, 2012). Na bazie Flame, uznanego jako najbardziej skomplikowany wirus jaki kiedykolwiek odkryto (CrySyS Lab, 2012) (wielkość 20 MB czyli około 50 krotnie większy od standardowego malware), powstały inne:

STUXNET - wycelowany w ściśle określoną instalację komputerową (sterowniki PLC Siemensa wykorzystywane w wirówkach do wzbogacania uranu) skutecznie blokujący kompleks nuklearny w Iranie, korzystał jednocześnie z 5 exploitów (McMillan, 2010).

DUQU – posiadający kod bardzo zbliżony do Stuxnet'a jednakże mający inne cele – służył jedynie do wykradania danych z tym, że jego ofiary to komputery wykorzystywane w przemyśle. Najprawdopodobniej wykradane przez Duqu dane miały pomóc w przeprowadzaniu kolejnych, bardziej ukierunkowanych ataków (Symantec, 2011)

GAUSS - podobnie jak jego poprzednicy Stuxnet, Duqu i Flame został stworzony w tym samym frameworku i dzieli z nimi część kodu (m.in. funkcje odpowiedzialne za infekcję via USB). potrafi przechwytywać ciastka i hasła z przeglądarek, wykradać pliki konfiguracyjne i wysyła je autorom trojana, infekować dyski USB, kraść dane dostępowe do banków (głównie ze Środkowego Wschodu) oraz dane dostępowe do portali społecznościowych, skrzynek e-mail.

Autorstwo malware z rodziny FLAME'a przypisywane jest rządowi Stanów Zjednoczonych oraz Izraela, NewYork Times ujawnił, że to Barack Obama wydał nakaz ataku komputerowego na Iran. W efekcie stworzono Stuxnet, który wymknął się z pod kontroli (Sanger, 2012).

I.7 Nowe techniki wykorzystywane przez malware

Twórcy malware wykorzystują coraz to nowsze techniki celem ominięcia zabezpieczeń najczęściej zauważane przez analityków techniki to:

- Detekcja maszyny wirtualnej – malware bada środowisko i system operacyjny zaatakowanej maszyny, jeśli wykryje charakterystyczne biblioteki sterowniki urządzeń, które wskazują, iż ofiara jest maszyną wirtualna (np. VirtualBox VMWare lub Hyper–V malware zaprzestaje ataku i po prostu wyłącza się. uruchomienie w środowisku wirtualnym może wskazywać iż jest to środowisko sandbox służące do badania zachowania złośliwego oprogramowania. dlatego też malware w takim środowisku nie komunikuje się ze swoim centrum Command and Control (C2) aby nie zdradzać swoich technik i taktyk działania.

- Opóźnienie wykonania i badanie aktywności użytkownika – obie metody mają podobny cel – analiza w środowisku sandbox trwa określony czas i po tym czasie jest najczęściej przerywana. Na pracę w wirtualnym sandboxie może świadczyć brak reakcji użytkownika (np. poruszanie myszką, lub brak uruchomionych w tle innych aplikacji.

- Wielowątkowość – jeden z wątków malware jest strażnikiem badającym środowisko operacyjne, analizuje także oprogramowanie antywirusowe i dalsze działanie uzależnione jest od zainstalowanego systemu antywirusowego – następuje jego dezaktywacja lub ominięcie.

- Zaawansowana wielowątkowa kompresja kodu wykonywalnego celem uniemożliwienia jego debugowania i analizy. istnieją programy kompresujące lub wręcz szyfrujące kod malware.

- Zaciemnianie kodu – skrypty java są celowo zaciemniane stosując nazwy zmiennych czy funkcji jako ciągi pseudolosowe,

- Wieloprocesowe malware – kod jest podzielony pomiędzy wiele procesów, osobny proces odpowiedzialny jest za pobranie reszty zaszyfrowanego kodu z sieci Internet, inny proces rozszyfrowuje, jeszcze inny wykonuje szkodliwe działanie. często odbywa się to bez zapisu na dysk twardy komputera – skanowanie dysku nic nie wskaże, podobnie jak analiza pamięci operacyjnej bez głębokiej analizy powiązania pomiędzy procesami.

ROZDZIAŁ II. Analiza malware i sandbox

Analiza Malware to proces wydobywania informacji ze złośliwego oprogramowania za pośrednictwem statycznej i dynamicznej kontroli za pomocą różnych narzędzi, technik i procesów. Jest to metodyczne podejście do odkrywania głównego celu złośliwego oprogramowania poprzez ekstrakcję jak największej ilości danych ze złośliwego oprogramowania, jak to możliwe, gdy jest w stanie spoczynku i w ruchu. Malware w spoczynku to złośliwe oprogramowanie, które nie jest uruchomione w środowisku docelowym, podczas gdy złośliwe oprogramowanie w ruchu to oprogramowanie, które działa w środowisku docelowym. Dane ekstrahuje ze złośliwego oprogramowania poprzez wykorzystanie danych ekstrakcji i narzędzi monitorujących.

Często konieczne jest sprawdzenia dokumentów czy oprogramowania, które otrzymano z niezaufanego źródła czy nie zawiera złośliwych ukrytych funkcji. Analiza podejrzanego oprogramowania konieczna jest z kilku powodów, po pierwsze nie można polegać na oprogramowaniu antywirusowym, po drugie brak często jest narzędzi, wiedzy lub czasu do zaawansowanej analizy za pomocą reverse engineering, wówczas przydatne jest zastosowanie automatycznej analizy malware.

II.1 Analiza statyczna

Analiza statyczna polega na sprawdzeniu z jakim rodzajem pliku mamy do czynienia. rozszerzenia lub ikonki często bywają celowo zmienione. czynność ta polega na sprawdzeniu sygnatur nagłówków pliku, dzięki temu możemy przekonać się czy jest to plik wykonywalny EXE, skrypt java, dokument pdf zawierający szkodliwy załącznik. Najpopularniejszym narzędziem jest linuksowy program „file" zawierający bazę sygnatur, dzięki którym rozpoznaje typ pliku. Drugą czynnością jest wyszukanie ciągów znaków zawartych w pliku, pomocnym narzędziem jest linuksowy program „strings" przeszukuje on plik w poszukiwaniu co najmniej 4 znaków ASCII zakończonych znakiem terminatora, jeśli plik nie jest zaszyfrowany lub spakowany istnieje duża szansa wyszukanie np. URL z którym malware chce się połączyć lub nazw plików lub zasobów, które chce zaatakować bądź loginów (w przypadku ataku ukierunkowanego). Następnym etapem jest wygenerowanie skrótu funkcji hash MD5. Dzięki niej możemy sprawdzić w serwisie VirusTotal lub nawet za pomocą wyszukiwarki Google czy ktoś już nie analizował pliku i nie opisał jego działania. ostatnim etapem może być analiza samego kodu w deasemblerze na IDA Pro, Olly Dbg, Radare2 lub Hopper.

Sama analiza kodu nie zawsze pomoże nam zrozumieć jego działanie, dodatkowo często malware jest jedynie programem pobierającym z sieci przy infekcji dodatkowe moduły dlatego konieczna jest analiza dynamiczna

II.2 Analiza dynamiczna - sandbox

Do automatycznej analizy malware najbardziej optymalny jest sandbox. Sandbox (ang. *piaskownica*) to ściśle kontrolowane i izolowane środowisko (najczęściej wirtualne), w którym programy albo skrypty, co do których nie mamy pewności czy są bezpieczne, mogą zostać bez szkody uruchomione w pamięci. Dzięki aplikacjom analizującym zawartość pamięci, wywołania systemowe, operacje na dysku lub przesyłane dane możemy stwierdzić czy uruchomione oprogramowanie jest złośliwe i jaki jest naprawdę cel jego działania.

W obecnych czasach złośliwe oprogramowanie pojawia się na każdym kroku tak w postaci aplikacji jak i linku czy też dokumentu. Do automatycznej analizy malware najbardziej optymalny jest sandbox. Sandbox (ang. *piaskownica*) to ściśle kontrolowane i izolowane środowisko (najczęściej wirtualne), w którym programy albo skrypty, co do których nie mamy pewności czy są bezpieczne, mogą zostać bez szkody uruchomione w pamięci (specjaliści często używają określenia „detonacja"). Dzięki aplikacjom analizującym zawartość pamięci, wywołania systemowe, operacje na dysku lub przesyłane dane możemy stwierdzić czy uruchomione oprogramowanie jest złośliwe i jaki jest naprawdę cel jego działania.

II.2.1 Cuckoo Sandbox

Przykładem otwartego i bezpłatnego a zarazem zaawansowanego i modularnego oprogramowania do automatycznej analizy złośliwego oprogramowania jest Cuckoo Sandbox. W kilka minut po wysłaniu do systemu podejrzanego pliku, dokumentu czy linku Cuckoo potrafi przeanalizować próbkę i zaraportuje jakie operacje były wykonane w wyizolowanym środowisku. Dzięki temu możemy poznać i zrozumieć jak działa malware , jaki ma cel, kontekst i motywacje, nie musimy bazować jedynie na artefaktach pozostawionych w pracującym systemie które pozostawił malware. Cuckoo potrafi automatycznie badać malware uruchomione pod wirtualnych i fizycznych środowiskach MS Windows, Mac OS X, Linux i Android. Standardowo Cuckoo potrafi:

- Analizować różne złośliwe pliki (pliki wykonywalne, dokumenty zawierające eksploity doc, pdf ,xls, aplety Java) a także zainfekowane strony internetowe, w środowiskach wirtualnych Windows, OS X, Linux i Android.
- Śledzenie systemowych wywołań API i ogólne zachowanie plików Tworzenie usuwanie, pobieranie i wysyłanie do sieci Internet.
- Dokonać zrzut i analizę ruchu sieciowego, nawet jeśli jest zaszyfrowany (MITM). Ruch sieciowy może zostać kierowany do otwartej sieci Internet, TOR bądź VPN, można także zasymulować siec internetową pakietem INETSIM.
- Tworzyć zrzuty ekranu podczas wykonywania malware.
- Wykonywać zaawansowaną analizę pamięci zainfekowanego systemu zwirtualizowanego z wbudowanym wsparciem dla pakietu Volatility. (Cuckoo Fundation, 2017)

Cuckoo Sandbox analizuje poniższe typy plików:

- wykonywalne pliki Windows,
- pliki DLL,
- dokumenty PDF,
- dokumenty Microsoft Office,
- uRL'e i pliki HTML,
- skrypty PHP,
- pliki CPL,
- skrypty Visual Basic (VB),
- pliki ZIP,
- pliki Java JAR,
- pliki Python.

Dzięki modułowej konstrukcji Cuckoo można dostosować zarówno etapy przetwarzania analizy i raportowania do swoich potrzeb. Za pomocą wbudowanego API potrafi współpracować z innymi aplikacjami i serwisami służącymi do badania i analizy malware.

Cuckoo Sandbox jest tworzony społecznie przez zespół kilku deweloperów i specjalistów. Za rozwój tego systemu oraz pokrewnych projektów i inicjatyw odpowiedzialna jest Cuckoo Foundation – organizacja typu non profit zarejestrowana w Holandii. Cuckoo Sandbox jest licencjonowany przez Cuckoo Foundation i jest licencjonowany na bazie GNU General Public License wersja 3 — licencja wolnego i otwartego oprogramowania

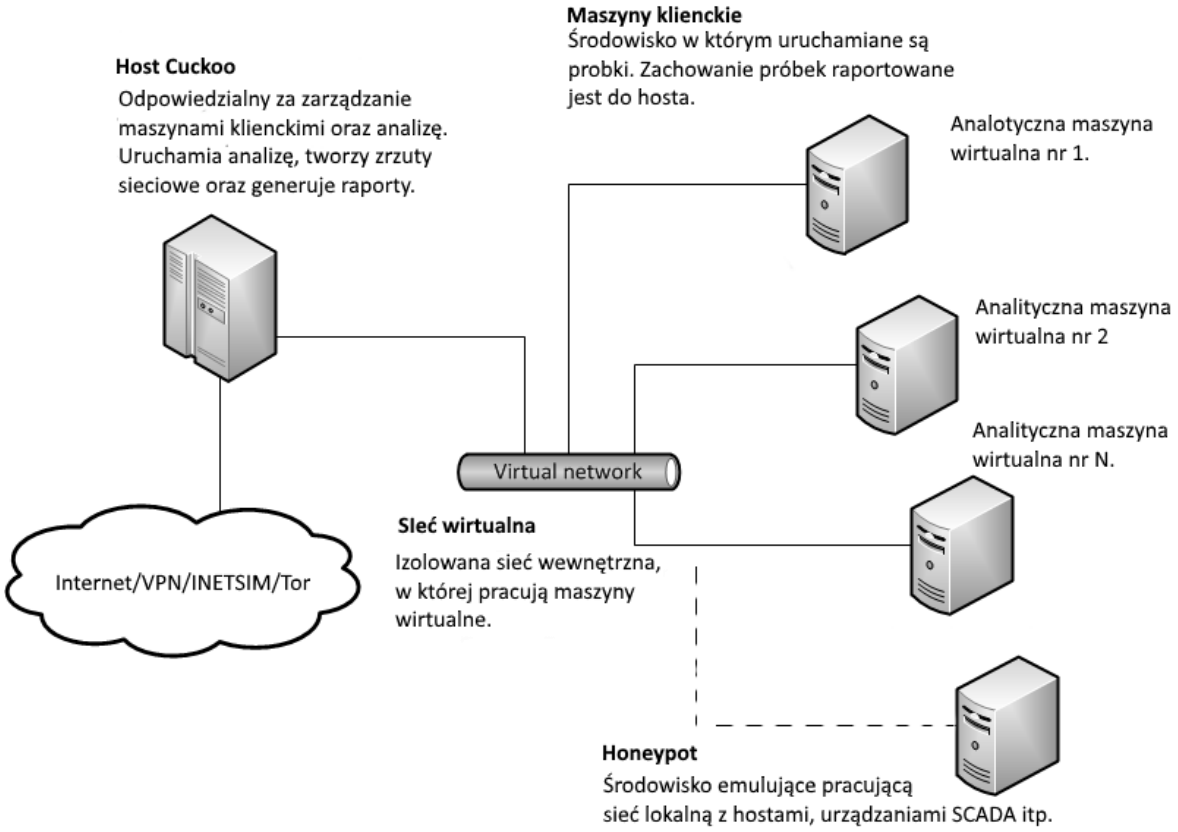
II.2.2 Działanie Cuckoo

System oczekuje na przesłanie próbki oprogramowania czy linku do witryny internetowej, po przesłaniu przygotowywane jest środowisko oraz wirtualna maszyna, w której zostanie uruchomiona próbka – podczas przesyłania próbki możliwe jest określenie parametrów analizy, jak priorytet typ wirtualnej maszyny (Windows XP, 7, Android, Linux) czy też dostęp do sieci (bezpośredni , VPN, TOR, INETSIM). Następnie Cuckoo uruchamia wybraną maszynę wirtualną z punktu przywracania (snapshot), przesyła do maszyny i uruchamia wybraną próbkę. Jeśli jest to próbka .exe to jest wykonywana w systemie operacyjnym maszyny wirtualnej, jeśli jest to dokument to otwierany jest edytor lub przeglądarka (MS Word, Adobe Acrobat Reader) link lub skrypt PHP/HTML uruchamiany jest w przeglądarce internetowej. W dalszej kolejności podczas działania uruchomionego malware tworzone są zrzuty ekranu, informacje o ruchu sieciowym i wszystkie inne o tworzonych czy kasowanych plikach lub wpisach w rejestrze systemu Windows i innych czynnościach zachodzących wewnątrz maszyny wirtualnej. Do tego dochodzą też zrzuty pamięci procesów lub całej pamięci RAM. Po zebraniu wszystkich informacji generowany jest raport w postaci strony HTML, lub dokumentu HTML i tworzone są pliki z danymi zebranymi podczas analizy – utworzone lub pobrane pliki przez badany malware lub jego procesy potomne, szczegółowa

analiza ruchu sieciowego oraz jego zrzut w postaci plików PCAP, pełne zrzuty zawartości pamięci RAM. (Bińkowski, 2016)

II.2.3 Architektura

Głównym elementem systemu jest oprogramowanie centralne Cuckoo zainstalowane w systemie Linux – tzw. *Cuckoo Host* bazujące na skryptach Python. Oprogramowanie to zarządza uruchomieniem i analizą przekazanej próbki malware, interfejsem webowym do obsługi aplikacji, a także maszynami typu *Guest* reprezentującymi wirtualne maszyny lub fizyczne komputery. Schemat budowy środowiska Cuckoo obrazuje rysunek 6. Każda analiza uruchamiana jest w czystym i odizolowanym środowisku wirtualnej maszyny lub fizycznego hosta.



Rysunek 6. Architektura systemu Cuckoo Sandbox. Źródło: opracowanie własne na podstawie (Cuckoo Fundation, 2017).

II.2.4 Instalacja

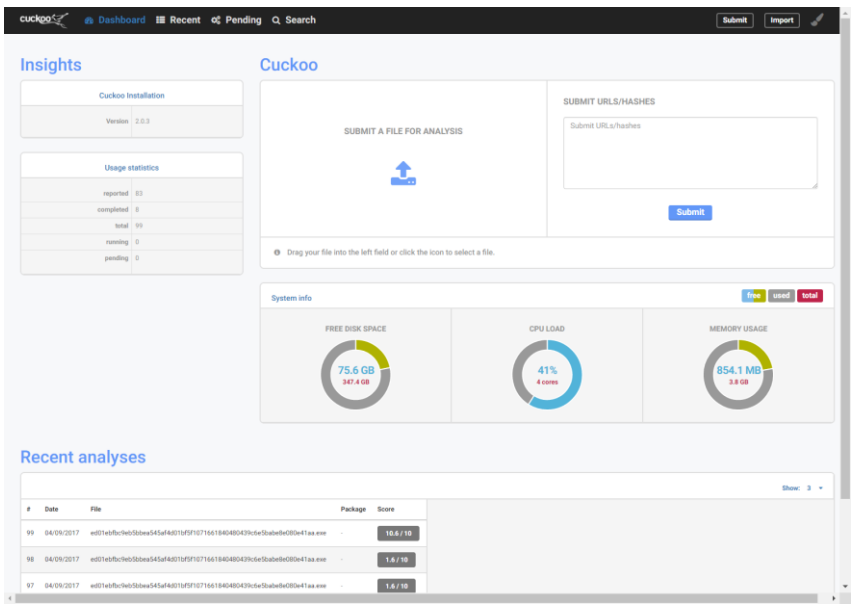
Przed przystąpieniem do instalacji Cuckoo Sandbox warto zauważyć, że wymaga on od użytkownika dobrej znajomości systemu Linux, a także podstawowej wiedzy z zakresu wirtualizacji i obsługi wirtualnych maszyn lub sieci. Dodatkowo przydatna będzie znajomość

języka Python a przynajmniej jego składni. Przydatna będzie także wiedza o malware w systemach informatycznych jego zachowaniu i rozprzestrzenianiu.

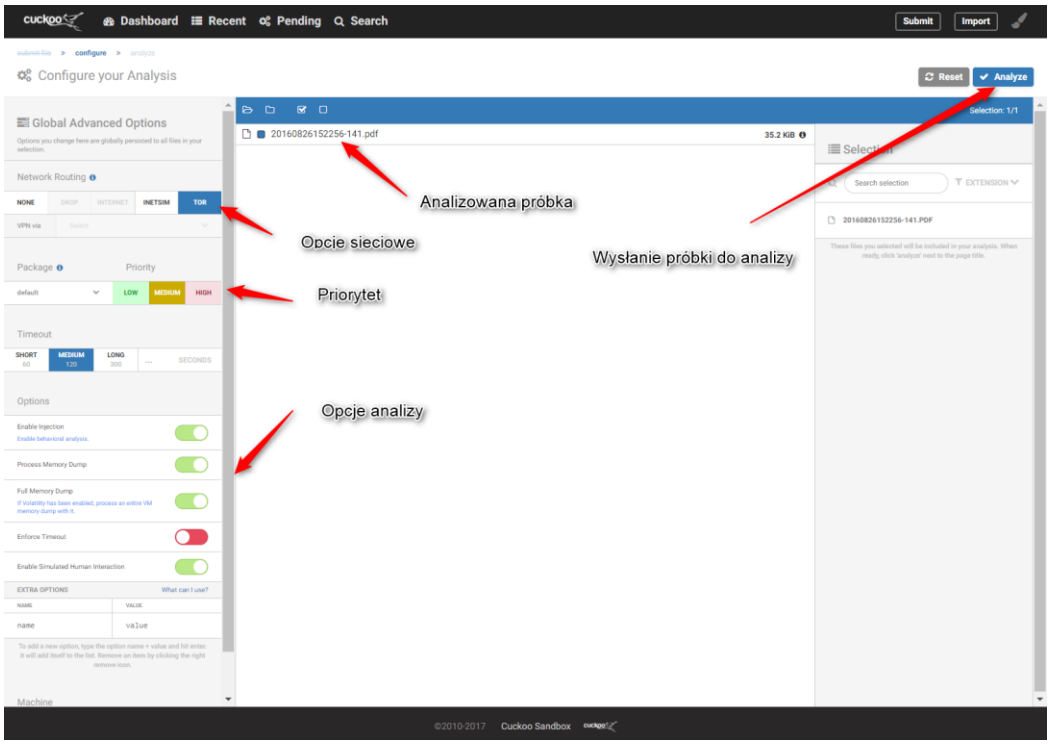
Sam proces instalacji systemu jest dość skomplikowany i czasochłonny, ponieważ wykorzystuje wiele elementów zewnętrznych. Niestety, pełny system Cuckoo nie zawiera gotowego instalatora, wszystkie więc komponenty należy zainstalować i skonfigurować samodzielnie. Proces instalacji jest w pełni opisany w dokumentacji produktu dostępnej online. W najnowszej wersji autorzy udostępnili możliwość instalacji za pomocą menagera pakietów python – pip. Autor pracy sporządził skrypt instalujący sandbox Cuckoo w środowisku Linux opartej na dystrybucji Ubuntu Server 16,04 LTS (Data, 2017).

II.2.5 Praca – przykładowa analiza

Interfejs sandboksa Cuckoo jest bardzo przejrzysty rysunek 7 przedstawia interfejs startowy. Rysunek 8 przedstawia interfejs służący rozpoczęciu pracy z analizowaną próbką, na rysunku 9 widzimy podsumowanie analizy z oceną punktową od 1 do 10 (WaanaCry otrzymał 10,6 pkt.) po lewej stronie widać odnośniki do szczegółowych analiz – zachowanie sytemu w sieci, analiza statyczna, dynamiczna, analiza wywołań API systemu, podrzuconych plików, istnieje możliwość eksportu poszczególnych fragmentów analizy bądź tez całości. Rysunek10 pokazuje sygnatury, które dowodzą złośliwości próbki zaznaczone kolorami w zależności od istotności. możemy zauważyć m.in. łączenie się z siecią TOR, kasowanie kopii pamięci *shadow* (brak możliwości odzyskania systemu), identyfikację próbki przez 60 znanych antywirusów w serwisie Virustotal, ilość zmodyfikowanych (zaszyfrowanych) plików oraz adresy z którymi działająca próbka usiłuje się połączyć. bardzo pomocne jest tworzenie zrzutów ekranu w poszczególnych fazach działalności malware. Współpracę z później omówionym systemem MISP obrazuje rysunek 24.

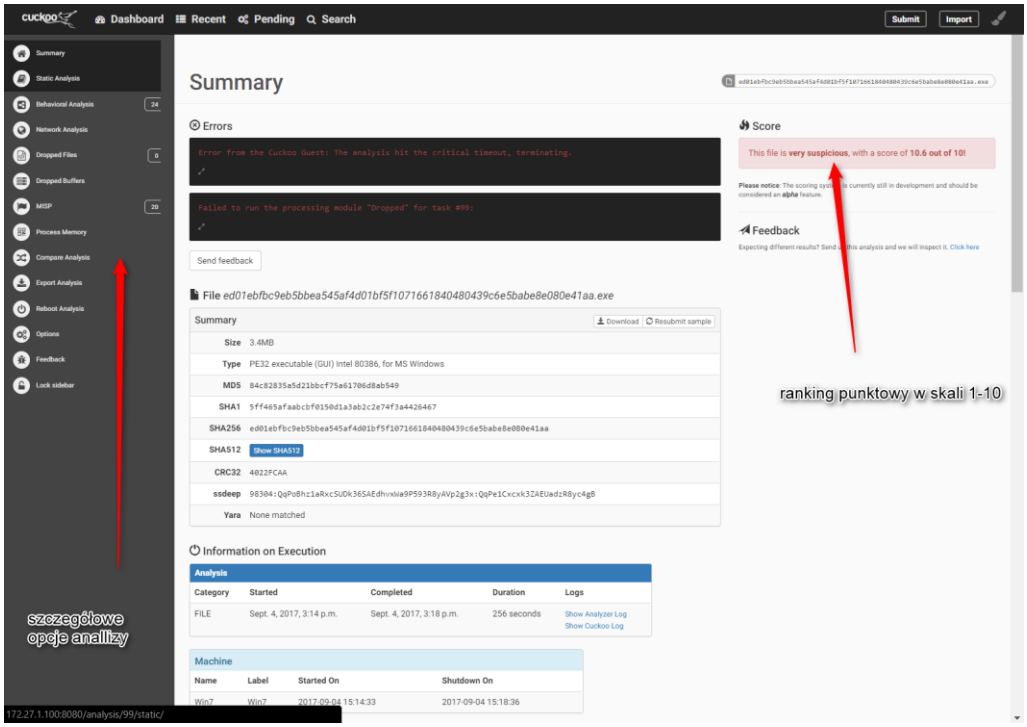


Rysunek 7. Interfejs startowy Cuckoo. Źródło: opracowanie własne na podstawie (Cuckoo Fundation, 2017).



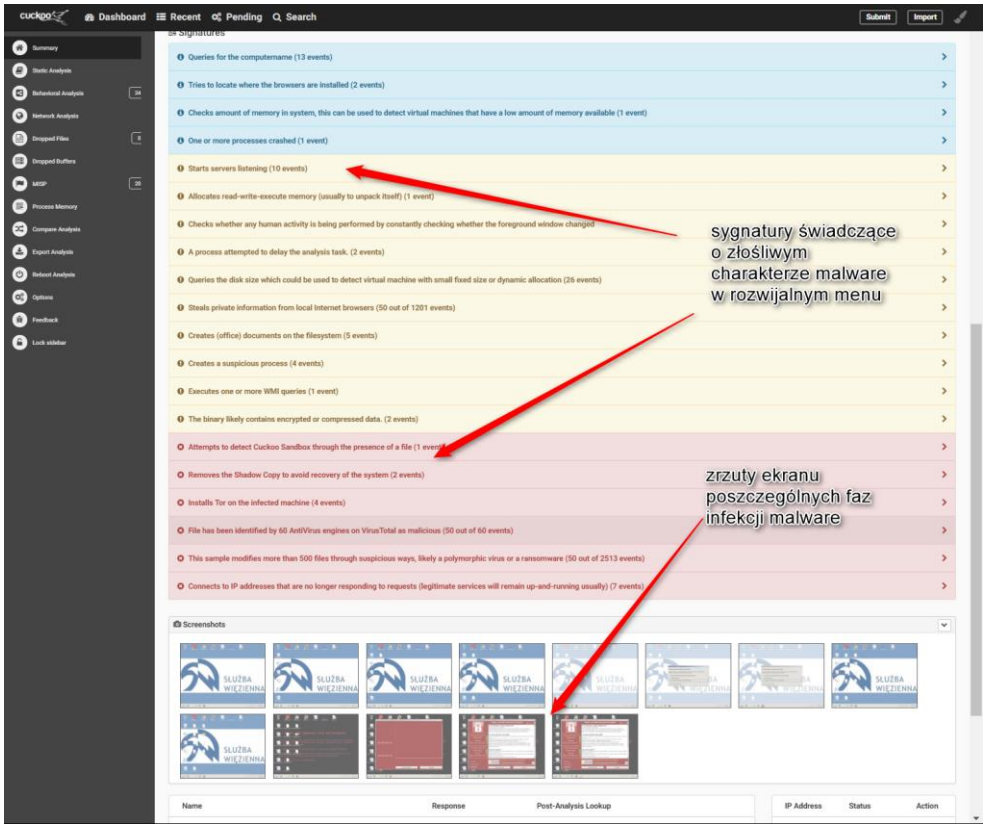
Rysunek 8. Przygotowanie analizy malware w środowisku Cuckoo. Źródło: opracowanie własne na podstawie (Cuckoo Fundation, 2017).

.



Rysunek 9. Raport z przeprowadzonej analizy – podsumowanie. Źródło: opracowanie własne na podstawie (Cuckoo Fundation, 2017).

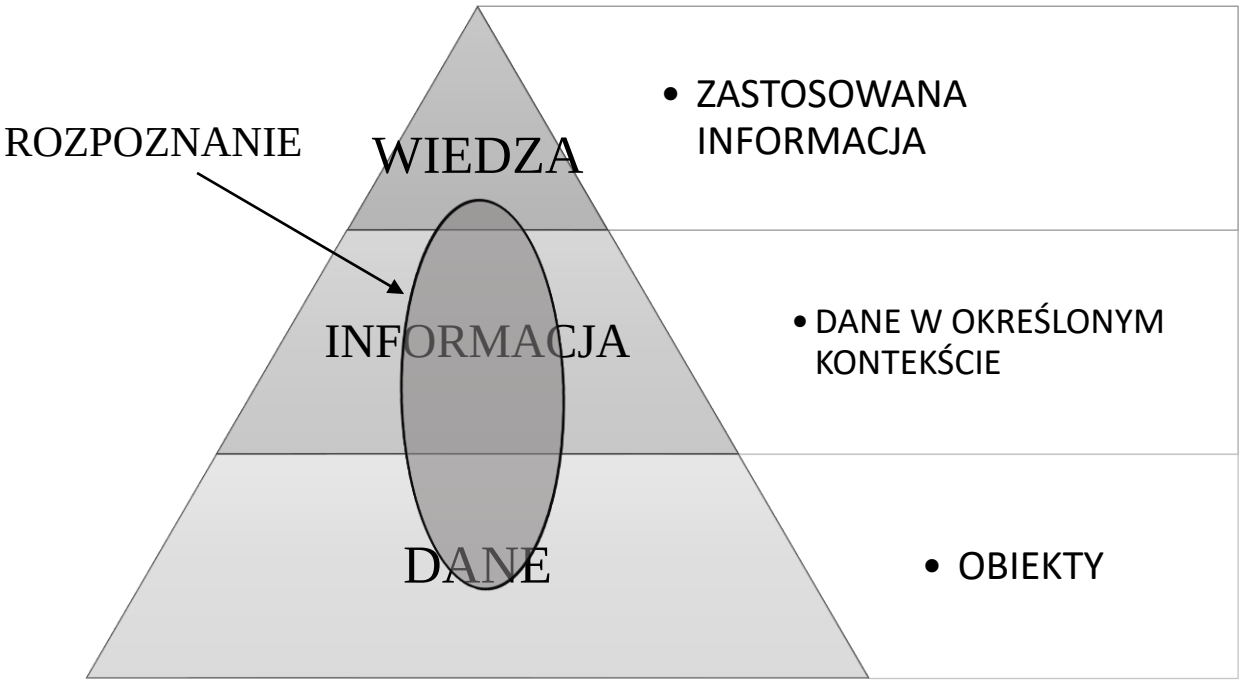
.



Rysunek 10. Analiza malware szczegółowy raport o działaniach malware. Źródło: opracowanie własne na podstawie (Cuckoo Fundation, 2017).

ROZDZIAŁ III. Cyber Threat Intelligence

Cyber threat intelligence – ze względu na wielorakie znaczenia słowa *intelligence*, które można tłumaczyć jako rozpoznanie, wywiad, czy nawet analizę zagrożeń. Najbardziej chyba odzwierciedlające ideę pojęcia tłumaczenie to rozpoznanie zagrożeń cybernetycznych (informatycznych). Jedna z najkrótszych definicji (przez analogię do *business intelligence*) to proces przekształcania danych o zagrożeniach cybernetycznych w informację (dane w określonym kontekście) a informacji w wiedzę. Dane to np. fakty, adresy, ciągi znakowe, informacja w tym sensie są dane w określonym kontekście czy też relacji, wiedza zaś to interpretacja lub wykorzystanie posiadanych informacji do rozwiania problemu lub podjęcia decyzji. Rozpoznanie było by wiec interpretacją opartą na dowodach, zebranych by zidentyfikować cele, motywacje techniki taktyki lub procedury sprawców zagrożenia. Rozpoznanie pomaga zrozumieć, złagodzić lub wyeliminować zagrożenia. Definicję powyższą dobrze definiuje schemat przedstawiony na rysunku 11 zaproponowany przez (Bank of England, 2016c, p. 13)



Rysunek 11. Schemat rozpoznania zagrożeń cybernetycznych. Źródło: (Bank of England, 2016c, p. 13).

III.1 Anatomia ataku cybernetycznego

III.1.1 Cyber Kill Chain

Dla lepszego zrozumienia ataku cybernetycznego na organizację firma Lockheed Martin wprowadziła pojęcie „Cyber Kill Chain" przez analogię do używanej już w wojsku koncepcji ataku. Proces ten określa, iż atak cybernetyczny składa się z 7 faz i tym samym organizacje mogą i powinny mieć kolejne możliwości wykrycia i powstrzymania ataku na każdym etapie. Etapy ataku ukazuje rysunek 12.

Poszczególne fazy ataku to:

1. **Rozpoznanie** – badania, identyfikacja i wybór celu, często obejmujące indeksowanie stron internetowych, takich jak materiały konferencyjne oraz listy adresów e–mail, sieci zależności oraz informacje na temat specyficznych technologii, atakujący nie musi nawet dotknąć sieci organizacji, wszystkie dane może pobrać przez wywiad z dostępnych z sieci źródeł;

2. **Uzbrojenie** – łączenie koni trojańskich (RAT – Remote Access Trojan) ze złośliwymi programami (ang. exploit) w celu stworzenia możliwej do dostarczenia paczki, często za pomocą automatycznego narzędzia (ang. weaponizer). Często jest to plik pdf, doc, skrypt, który potem zostanie umieszczony na uczęszczanej przez ofiarę witrynie.

3. **Dostarczenie** – przekazywanie ładunku do atakowanego środowiska. Najbardziej rozpowszechnione wektory dostawy dla "cyberbroni" w ramach ataków APT to załączniki e–mail (phising, spear–phishing), witryny internetowe (watering hole) i pendrive.

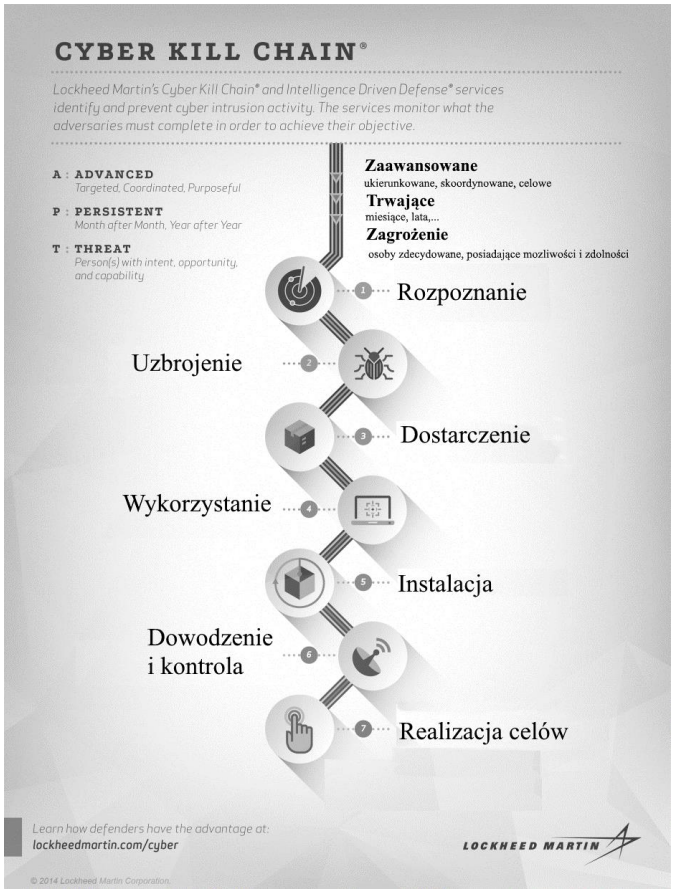
4. **Wykorzystanie** – po dostarczeniu niebezpiecznego ładunku do środowiska ofiary jest uruchamiany złośliwy kod (najczęściej ofiara klika na link w mailu, instaluje „dodatkowy driver" by obejrzeć materiał video). Najczęściej wykorzystuje się luki w aplikacjach lub systemie operacyjnym. Ostatnio faza ta składa się z dwóch części uruchamianiu jest najpierw mały program trudny do zidentyfikowania przez antywirusy tzw. Downloader, który to następnie pobiera z sieci właściwy złośliwy kod.

5. **Instalacja** – instalacja konia trojańskiego (RAT – Remote Access Trojan) lub tylnych furtek (ang. backdoor) w systemie ofiary pozwala atakującemu na trwałe utrzymanie dostępu do środowiska organizacji.

6. **Dowodzenie i kontrola** (ang. *Command and Control* – C2) – zaatakowany system wysyła sygnał do serwera kontrolnego o działaniu malware w celu ustanowienia kanału C2. Kierowanie aplikacją odbywa się ręcznie bądź automatycznie. Po ustanowieniu kanału C2 intruzi otrzymują pełny dostęp do zainfekowanego systemu. Do komunikacji używane są porty zwykle nie blokowane przez firewalle: http/https, ftp, dns ostatnio

także wykorzystywane są do sterowania komunikaty przekazywane przez sieci społecznościowe (Twitter, Facebook).

7. **Realizacja celów** – po przejściu przez pierwszych sześciu faz intruzi mogą podjąć działania w celu osiągnięcia zamierzonych celów. Najczęściej jest to wykradzenie danych lub użycie systemu jako stacji przesiadkowej do przesłania emaila lub dojścia do innej sieci lub systemu (Hutchins, et al., 2011).



Rysunek 12. Fazy ataku cybernetycznego. Źródło: opracowanie własne na podstawie (Hutchins, et al., 2011).

W celu maksymalizacji wykrycia zagrożeń, konieczne jest aby wszystkie fazy ataku były monitorowane. Matryca możliwych działań, które można podjąć na każdym etapie ataku przedstawiona jest w tabeli 1.

Tabela 1. Sposoby postępowania z atakami.

Faza	Detekcja	Blokada	Zakłócenie	Pogorszenie	Oszukanie
Rozpoznanie	Analityka witryny	Firewall			
Uzbrojenie	NIDS	NIPS			
Dostarczenie	Czujny Użytkownik	Filtr proxy	Antywirus	Kolejkowanie	
Wykorzystanie	HIDS	Aktualizacja	DEP		
Instalacja	HIDS	Środowisko chroot	Antywirus		
Dowodzenie i kontrola	NIDS	Firewall	NIPS	Serwer opóźniający (tarpit)	Przekierowanie DNS
Realizacja celów	Audyt logów			QoS	Honeypot

Źródło: (Hutchins, et al., 2011).

SecureWorks podaje kilka wytycznych do przerwania łańcucha ataku, proponując kwestie, które pomogą zrealizować system ochrony i przeciwdziałania atakom (SecureWorks, 2016).

- **Poznanie przeciwnika** – Konieczne jest wdrożenie procesu rozpoznania zagrożeń celem ustalenia praktycznych informacji o samym zagrożeniu, aktorach (przeciwnikach) oraz ich działaniach. Konieczna jest pełna wiedza o własnych zasobach, systemach i sieciach.
    - Kim jest atakujący i jak działa.
    - Jakie ma taktyki, techniki i procedury.
    - Jakie posiada doświadczenie.
    - Jakie są wskaźniki jego ataku i która fazę już osiągnął.
    - Czy jesteśmy gotowi przyjąć atak.

- **Wczesne rozpoznanie ataku** – Niezbędne jest elastyczne dostosowywanie polityk bezpieczeństwa i korelowanie informacji z różnych źródeł w celu osiągnięcia pełnego obrazu sytuacji.
    - Czy atakujący już funkcjonuje w sieci?
    - Czy posiadamy narzędzia do wykrycia ataku?
    - Czy potrafimy rozpoznać wszelkie wystąpienia ataku?
    - Czy potrafimy stwierdzić wskaźniki wszystkich dotychczasowych faz ataku?
    - Jak najszybciej potrafimy stwierdzić co jest celem ataku?

- **Zakłócenie ataku** – szefostwo musi ocenić realne szanse powodzenia operacji odparcia ataku a także umiejętności personelu. Jeśli odparcie jest niemożliwe bądź kwalifikacje załogi nie są wystarczające, konieczna będzie modyfikacja strategii dzięki informacjom zdobytym poprzez monitorowanie zagrożenia w czasie rzeczywistym.

- Czy posiadamy narzędzia do wykrycia i zablokowania ataku?
- Czy możemy ograniczyć rozprzestrzenianie się?
- Czy potrafimy przewidywać dalsze ruchy przeciwnika?
- Czy wiemy dostatecznie dużo aby przyjąć atak przeciwnika?
- Jak szybko możemy reagować?

- **Zwalczenie i usunięcie zagrożenia** – nie ma jednego panaceum na odparcie ataków, organizacje muszą oceniać swoja zdolność skutecznej reakcji na incydent. Specjaliści ds. bezpieczeństwa muszą oceniać i kontrolować przygotowanie organizacji do skutecznej reakcji na naruszenia bezpieczeństwa. Krytyczną kwestią jest posiadanie planu reakcji na wystąpienie incydentu informatycznego.

    - Jakie systemy są zajęte przez atakującego?
    - Jak odpowiedzieć na atak?
    - Czy plan reakcji przewiduje ataki ukierunkowane?
    - Czy potrafimy zapobiec kolejnemu atakowi?

Raport ENISA przedstawiony na rysunku 13ukazuje typowe ataki rozłożone na poszczególne fazy kill-chain.

Rysunek 13. Ataki cybernetyczne rozłożone na poszczególne fazy

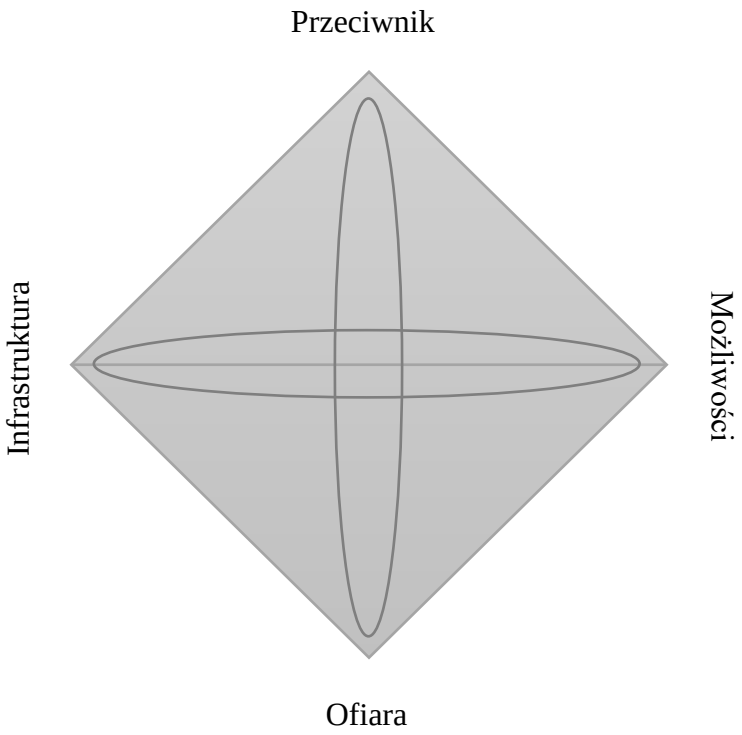
Rozpoznanie	**Uzbrojenie**	**Dostarczenie**	**Wykorzystanie**	**Instalacja**	**Dowodzenie i kontrola**	**Realizacja celów**
				MALWARE		
	Ataki bazujące na sieci WEB					
			Atak na aplikacje WEB			
DoS					DoS	
					BOTNET	
PHISING						
	SPAM					
				RANSOMWARE		
ZAGROŻENIE WEWNĘTZNE						
						ZNISZCZENIE/KRADZIEŻ/UTRATA
	ZESTAWY EXPLOITÓW					
UTRATA DANYCH						
KRADZIEŻ TOŻSAMOŚCI						
WYCIEK INFORMACJI						
CYBERSZPIEGOSTWO						

Źródło: opracowanie własne na podstawie (ENISA, 2014).

III.1.2 Model Diamentu

Inne podejście do oceny ataku informatycznego opublikowała organizacja Centre for Cyber Threat Intelligence and Therat Research w 2013 roku. Dokument ten skupia się na rozpoznaniu i zrozumieniu atakującego – jakich używa narzędzi, jaką posiada infrastrukturę, jakie ma motywacje. Zamiast analizować serie zdarzeń kładzie nacisk się powiązaniach

pomiędzy cechami ataku. Nad poszukiwania źródeł pojedynczych ataków przekłada lepsze zrozumienie natury zagrożenia z którym mamy do czynienia. Model diamentu, przedstawiony na rysunku 14. pozwala na budowanie jaśniejszego obrazu działania przeciwnika pozwalająca na sporządzenie bardziej efektywnej informacji o ataku. Dla przykładu modelowanie relacji na wiadomości phisingowej pozwala łatwiej ustalić kto wysłał kto otrzymał maila, jakie adresy i domeny zostały użyte (Caltagirone, et al., 2013).



Pola w modelu:

Przeciwnik – adres email, telefon, zasoby sieciowe

Infrastruktura – adres IP, nazwa domenowa, adres email

Możliwości – malware, exploit, narzędzia hackerskie, skradzione certyfikaty

Ofiara – Osoby, Zasoby sieciowe, adresy mail

funkcje dodatkowe – znacznik czasu, faza ataku, rezultat (sukces,porażka), kierunek

Rysunek 14.Model diamentu, Źródło: opracowanie własne na podstawie (MacGregor, 2015).

Korzyści stosowania modelu diamentu (ActiveResponse.org, 2016):

- umożliwia zastosowanie wskaźników kontekstowych i relacyjnych poprawiając współdzielenie rozpoznania o zagrożeniach cybernetycznych, poszerza zakres stosowania wskaźników.
- integruje pewność informacji z rozpoznaniem zagrożeń dzięki wykresom obrazującym atak
- poprawia skuteczność analizy dzięki łatwiejszej identyfikacji pośrednich możliwości oraz prostszego budowania nowych analiz

- zwiększa dokładność analizy poprzez możliwość generowania hipotez, dokumentacji, badań poprzez większa dyscyplinę w procesie analitycznym
- wspomaga prowadzenie rozwoju, planowania działań i strategii obrony poprzez łatwą integrację z większością platform.
- wzmacnia rozwój metod analitycznych poprzez sformalizowanie pierwotnych zasad na których można budować dalsze koncepcje
- wspomaga opis zdarzeń w czasie rzeczywistym poprzez mapowanie procesu analitycznego do zrozumiałej klasyfikacji oraz detekcji włamań.
- określa podstawy aktywności, taksonomii, wymiany informacji o zagrożeniach oraz zarządzania wiedzą.

III.2 Próba definicji rozpoznania zagrożeń cybernetycznych

Stosowanie tradycyjnych mechanizmów zabezpieczeń jest wystarczające na wewnętrzne potrzeby organizacji, ale w prawie nie zauważa ryzyk, które powodują zagrożenia pochodzące z zewnątrz. Hacktywizm, cyberkonflikty między państwami czy szpiegostwo przemysłowe to stałe elementy listy zagrożeń. Wskazane zatem jest aby mechanizmy obrony przed nimi miały charakter wyprzedzający i powinny funkcjonować niczym sprawny wywiad, gdyż właściwe jest założenie, że skuteczny może zostać przeprowadzony z prawdopodobieństwem graniczącym z pewnością. O ile tradycyjne cyberbezpieczeństwo obejmuje rekrutację i zatrudnienie ekspertów zajmujących się bezpieczeństwem informatycznym, ustalenie formalnych regulacji i polityk bezpieczeństwa oraz rozmieszczeniem urządzeń i aplikacji zabezpieczających infrastrukturę techniczną tak rozpoznanie zagrożeń cybernetycznych (Cyber Threat Intelligence) opiera się na gromadzeniu wiedzy o zagrożeniach stosując: biały wywiad (OSINT–Open Source INTelligence), informacje z mediów społecznościowych (SOCMINT – SOCial Media INTelligence) oraz informacje ze źródeł osobowych (HUMINT – HUMan INTelligence) a także wiedzę z deep– i dark–web. Kluczowym zadaniem cybernetycznego rozpoznania jest badanie, analiza trendów oraz zmian w takich obszarach jak cyberprzestępczość, cyberaktywizm (np. Anonymous) oraz cyberszpiegostwo (np. ataki APT). Oczywiście wiedza to musi być wzbogacona informacjami z własnej infrastruktury, gromadząc i korelując dane o zdarzeniach bezpieczeństwa. Należy zmienić optykę – nie zastanawiać się czy organizacja jest bezpieczna, lecz jakie czynności zostaną podjęte gdy zostaniemy zaatakowani. Konieczna jest proaktywna postawa z gotowością na cyberatak.

Według brytyjskiego Ośrodka Ochrony Infrastruktury Narodowej (CPNI), istnieją cztery rodzaje rozpoznania zagrożeń przedstawione na rysunku 15. (National Cyber Security Centre, 2015, p. 4), podobnie definiuje je brytyjska firma MWR Infosecurity współpracująca z CERT Wielkiej Brytanii (MWR Infosecurity, 2015).

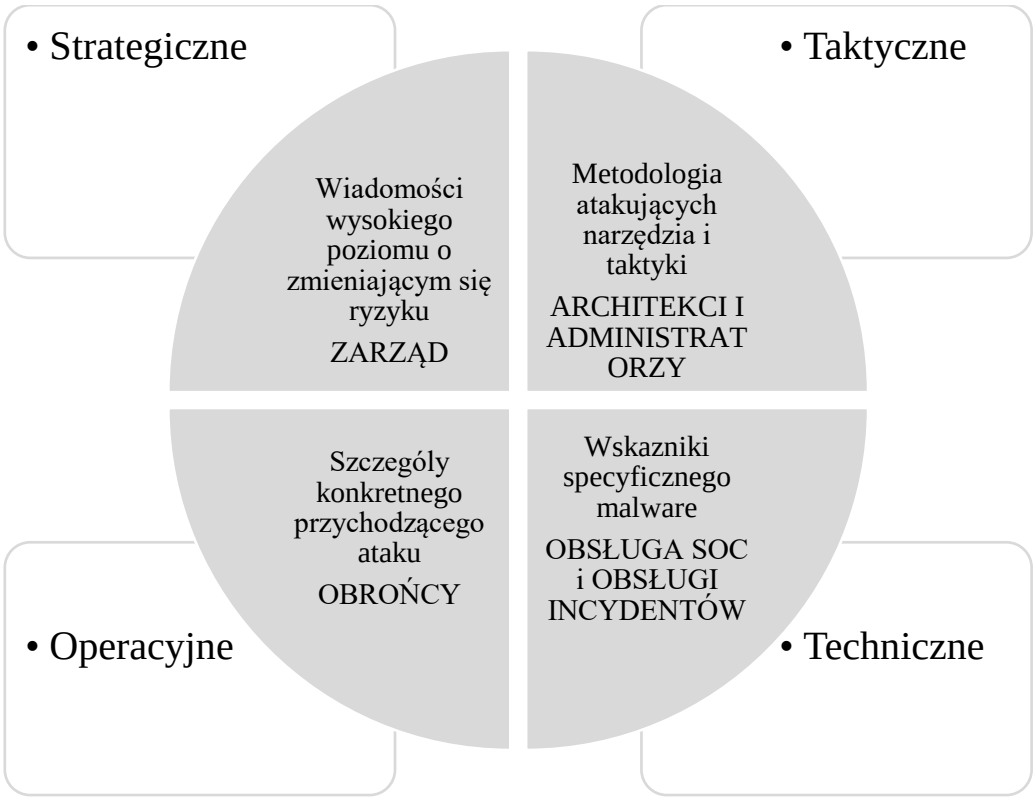
- **Techniczne**: Techniczne rozpoznanie cyberzagrożeń zawiera szczegółowe informacje o zasobach napastnika, takich jak narzędzia, kanały dowodzenia i kontroli oraz infrastruktura. Różni się od rozpoznania taktycznego tym, że koncentruje się na konkretnych wskaźnikach i szybkiej dystrybucji i reakcji, a zatem ma krótszy użyteczny okres eksploatacji. Fakt, że atakujący używa konkretnego złośliwego oprogramowania, to rozpoznaniem taktyczne, a wskaźniki przeciwko konkretnemu skompilowanemu przykładowi to rozpoznanie techniczne. Typowe przykłady wywiadu dotyczącego zagrożeń technicznych obejmują sumy szkodliwego oprogramowania lub phishingowych przynęt-dokumentów MD5, nagłówki wiadomości e-mail typu phishing, adresy IP dla urządzeń końcowych C2 lub nazw domen używanych przez C2. Idealne wskaźniki powinny pochodzić z aktywnych kampanii, które są obecnie doświadczane przez inne organizacje. Dzięki szybkiemu włączeniu tych wskaźników do infrastruktury defensywnej, takich jak firewalle, urządzenia filtrujące pocztę i rozwiązania zabezpieczające przed wyciekiem danych, organizacje mogą starać się wykrywać napastników - zarówno wtedy, gdy najpierw atakują, czy we wczesnych stadiach ataku. Przeszukując przeszukiwanie wcześniej zapisanych połączeń lub plików binarnych, można również wykryć ataki historyczne. Wyzwaniem często zgłoszonym przez organizacje próbujące wywiadu technicznego jest to, że sama ilość danych może szybko stać się przytłaczająca. W tym przypadku należy dokładnie rozważyć alokację zasobów, a organizacja może być bardziej selektywna w gromadzonych danych lub decydując się na budowę lub zakup dużych platform analitycznych, aby poradzić sobie z ilością danych. Ważne jest jednak, aby alokacja zasobów i rozwój zdolności były stale zbalansowane przed oceną korzyści płynących z wywiadu dotyczącego zagrożenia technicznego. Można by stwierdzić, że większe korzyści będą pochodzić z inwestowania w inne formy inteligencji. Istnieje wiele komentarzy w społeczności zabezpieczeń co do użyteczności technicznego rozpoznania zagrożeń, a niektóre twierdzą, że jest to bardzo skuteczny sposób zapobiegania i wykrywania kompromitacji, inni wątpią w jego użyteczność. Ta ostatnia grupa porównuje ją do sygnatur antywirusowych, ponieważ napastnicy mogą w niewielkim stopniu przystosować się, aby zapewnić, że ich narzędzia nie są rozpoznawane. Istnieje obawa, że duże ilości danych nie zawierają informacji kontekstowych, a zatem nie mogą dostarczyć większej analizy i oceny źródeł.

- **Taktyczne**: Rozpoznanie taktyczne może być jedną z najbardziej użytecznych form rozpoznania w zakresie ochrony organizacji. Jest to informacja dotycząca taktyki wykorzystywanej przez grupy napastnikówo - w tym ich narzędzi i metodologii - i jest często określana jako Taktyki, Techniki i Procedury (TTP - Tactics, Techniques and Procedures). Celem taktycznego rozpoznania zagrożeń jest zrozumienie, w jaki sposób aktorzy (*actors*- sprawcy) mogą atakować organizację, a także mapować tę wiedzę na sposoby, jak te ataki można złagodzić lub wykryć. Taktyczne rozpoznanie zagrożeń cybernetycznych jest wykorzystywana przez obrońców, takich jak architekci, administratorzy i personel ochrony. Źródłami informacji taktycznych są raporty

o incydentach, atakach i kampaniach publikowane w Internecie, statyczna i dynamiczna analiza malware.

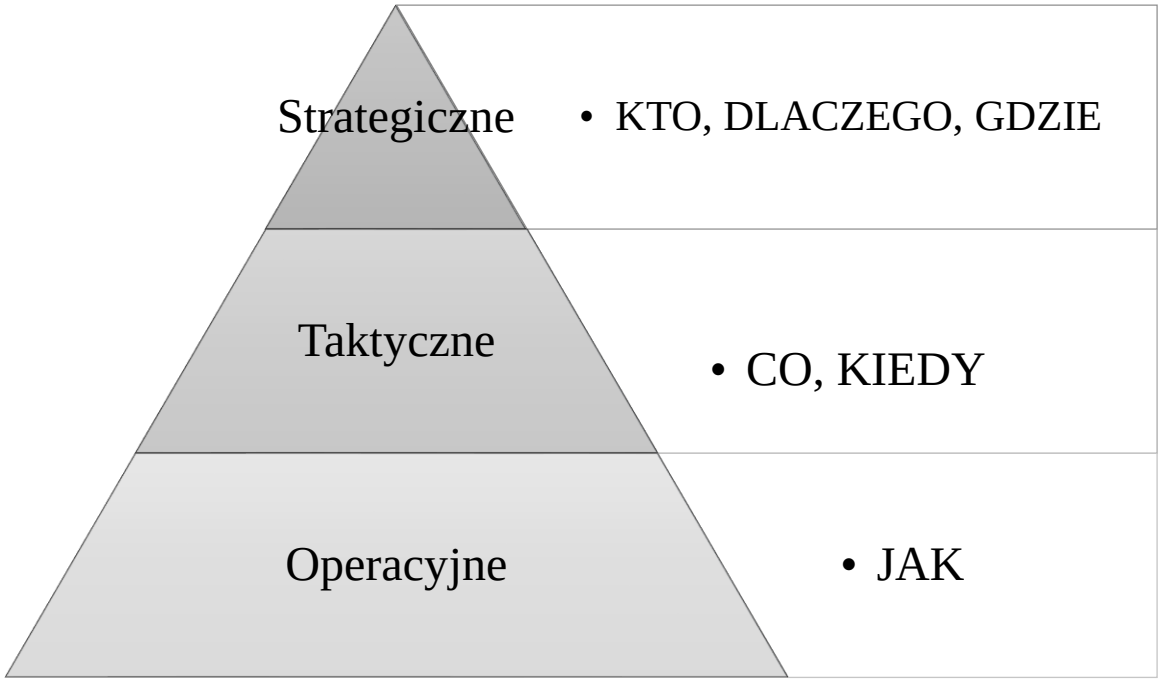
- **Operacyjne**: szczegółowa analiza poszczególnych ataków oraz określenie możliwości obrony na podobne zagrożenia w przyszłości. Operacyjne rozpoznanie zagrożeń to trafne informacje o konkretnych atakach przychodzących. Informuje o naturze ataku, tożsamości i zdolności atakującego - i wskazuje, kiedy może nastąpić atak. Służy do złagodzenia ataku: na przykład poprzez usunięcie ścieżek ataku lub utwardzenie systemu zabezpieczeń. Źródłem rozpoznania mogą być wszelakie socialmedia, fora dyskusyjne, źródła osobowe, grupy dyskusyjne,

- **Strategiczne**: wiedza o zmieniającym się ryzyku (strategicznych przesunięciach) konieczny jest ośrodek dowodzący do określenia krytycznej oceny zagrożeń. Strategiczne rozpoznanie zagrożenia jest przeznaczone dla kierownictwa wysokiego szczebla w organizacji, zazwyczaj zarząd lub osoby reprezentujące zarząd. Ma ona na celu pomóc strategom zrozumieć obecne zagrożenia oraz zidentyfikować dalsze zagrożenia, o których jeszcze nie są świadomi. Zajmuje się takimi pojęciami jak ryzykiem i prawdopodobieństwem, a nie aspektami technicznymi, jest używany przez zarząd do prowadzenia strategicznych decyzji biznesowych i zrozumienia wpływu podejmowanych decyzji. Materialnie jest często w formie prozy, na przykład raportów lub briefingów - zarówno podczas konferencji, jak i spotkań indywidualnych z kadrą kierowniczą i członkami zarządu. Posiada silny biznesowy nacisk, który jest używany do prowadzenia strategii. Źródłami rozpoznania mogą być oceny sytuacji geopolitycznej (trendy, ambicje, strategie) analizy i raporty finansowe i giełdowe, polityczne kontakty międzyludzkie, artykuły publikowane w prasie autorstwa wysoko postawionych osób. Większość tych danych można odnaleźć stosując źródła o otwartym dostępie (OSINT).



Rysunek 15. Rodzaje rozpoznania zagrożeń Źródło: (MWR Infosecurity, 2015).

Allan Liska rozróżnia trzy poziomy rozpoznania: strategiczny, taktyczny i operacyjny. Poszczególne typy rozpoznania uporządkowane są hierarchicznie, jak to obrazuje rysunek 16.: na szczycie znajduje się rozpoznanie strategiczne, dotyczące długoterminowych trendów zagrożeń. Analiza strategiczna opiera się na ocenie i przewidywaniu przyszłych zachowań w oparciu o dotychczasowe działania. Skuteczność rozpoznania strategicznego zależy od głębokiej wiedzy analityków oraz zrozumieniu działania i dostosowaniu się do potencjalnych przeciwników. Poniżej na piramidzie hierarchii znajduje się rozpoznanie taktyczne bazujące na ocenie bezpośrednich możliwości przeciwnika. Koncentruje się na mocnych stronach, słabościach oraz intencjach wroga. Sprawnie poprowadzona taktyczna ocena przeciwnika pozwala na najbardziej sprawne alokowanie własnych zasobów. Najniższy poziom to rozpoznanie operacyjne, które funkcjonuje w czasie rzeczywistym, pochodzi najczęściej z dzienników zdarzeń firewalli, ruterów, honeypotów dlatego niezbędne jest sprawne gromadzenie danych z urządzeń. Cechą rozpoznania operacyjnego jest bardzo krótki czas życia. (Liska, 2015)



Rysunek 16. Piramida rozpoznania. Źródło: (Liska, 2015).

Gartner – przedsiębiorstwo analityczno–doradcze specjalizujące się w zagadnieniach strategicznego wykorzystania technologii oraz zarządzania technologiami definiuje rozpoznanie zagrożeń jako wiedzy bazującej na dowodach, przy wykorzystaniu kontekstu, mechanizmów wskaźników, implikacji, zgłoszeń o powstających lub istniejących zagrożeniach. Kluczowymi wyzwaniami są: trudność w określeniu wskaźników ryzyka kiedy nie znamy przeciwników i ich intencji, przygotowanie bezpieczeństwa powinno odbywać się na około trzy lata do przodu a nie tylko na istniejące zagrożenia (Gartner, 2014).

Bank of England twierdzi wręcz iż testy penetracyjne tak często używane celu podniesieniu bezpieczeństwa, nie są już adekwatne do ochrony bezpieczeństwa sektora bankowego i zaleca ochronę instytucji finansowych w oparciu o rozpoznanie zagrożeń cybernetycznych (Bank of England, 2016a, pp. 21-22) (Bank of England, 2016b).

Efektywny program rozpoznania posiada kilka obszarów, na których można się skoncentrować. Podział rozpoznania zagrożeń na konkretne funkcje pozwala lepiej go skalować, gdyż poszczególni członkowie zespołu mogą być bardziej wykwalifikowani w określonych aspektach rozpoznania. Mogą skupić się i rozwijać na poszczególne części cyklu, łatwiej też będzie śledzić konkretne słabości lub braki w poszczególnych etapach (MWR Infosecurity, 2015). Poszczególne etapy cyklu rozpoznania przedstawia rysunek 17:

- **Wymagania**: Krok, który jest często pomijany, a może być kluczem do udanego programu. Kierownictwo musi określić, co chcą wiedzieć konkretnie i co powinien im powiedzieć program rozpoznania zagrożeń. Na przykład wymóg może brzmieć następująco: "Informuj nas o wszystkich powszechnie znanych, powszechnie wykorzystywanych lukach w ciągu jednego dnia od ich poznania". Wymagania mogą

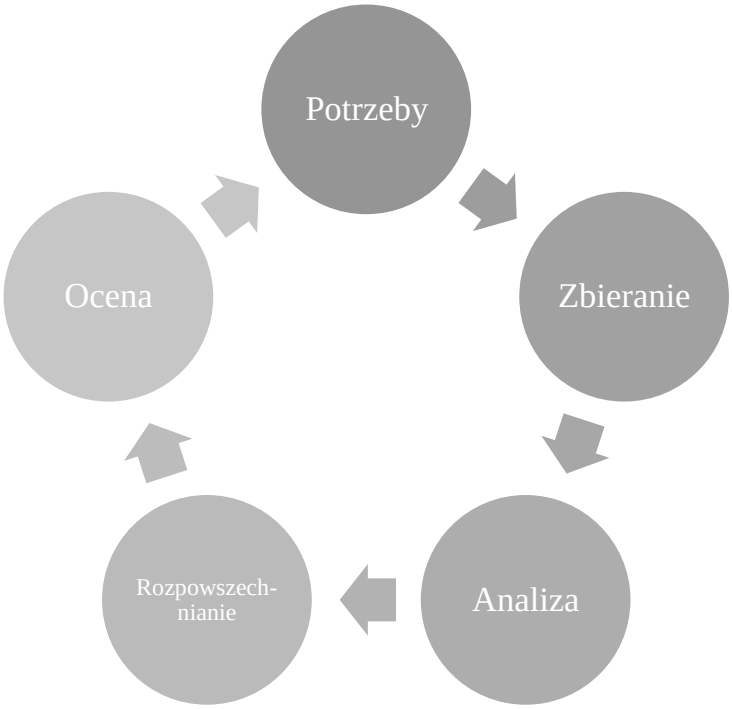
być bardziej wymagające dla zespołów rozpoznania zagrożeń, np. "Uzyskiwanie szczegółowych informacji i próbek większości narzędzi do zdalnego dostępu do zestawów przestępczych dla naszych zespołów ds. forensyki". Zespoły muszą współpracować z decydentami, aby uzgodnić wymogi, które są nie tylko możliwe do osiągnięcia, ale przede wszystkim dostarczą produktów, na których organizacja będzie mogła działać.

- **Zbieranie**: Krok, który może dominować w znacznej części budżetu zespołu do rozpoznania zagrożeń cybernetycznych, polega na gromadzeniu informacji lub danych, które należy przeanalizować. Informacje mogą pochodzić z wielu różnych źródeł, takich jak kanały informacyjne, płatne usługi lub kanały, fora a nawet źródła ludzkie. Prawie wszystkie informacje o zagrożeniach wymagają jakiejś analizy. Zrozumienie, które źródła mogą generować pożądane informacje, które są wiarygodne i dostarczają wartościowych informacji i w jakim czasie je wykorzystać nie jest banalnym procesem.

- **Analiza**: przekształcanie danych w informacje, które mogą być później wykorzystane często wymaga analizy. W niektórych przypadkach analiza będzie stosunkowo prosta, np. przeanalizowanie pliku danych do zestawu reguł „deny" i alertów zapory. W innych przypadkach będzie wymagało wyodrębnienia odpowiednich informacji z większego zbioru, na przykład z raportu i zrozumienia, które elementy mają zastosowanie do aktywów organizacji. Ważną rolę dla analityka ma poszukiwanie możliwości tworzenia nowych typów inteligencji poprzez syntezę z bieżącej wersji. Na przykład analityk może poświęcić czas na czytanie dokumentów, aby wyodrębnić wskaźniki kompromisu, a także określić operacyjne informacje, które mogą być przekazane obrońcom sieci. Lub po przeczytaniu takich dokumentów i innych źródeł analityk może identyfikować trendy, które można zebrać razem w produkt strategiczny wywiadu dla wyższego zarządzania. czasem okazuje się ze zebrane dane nie zawierają ważnych danych analitycznych i należy powrócić do etapu zbierania.

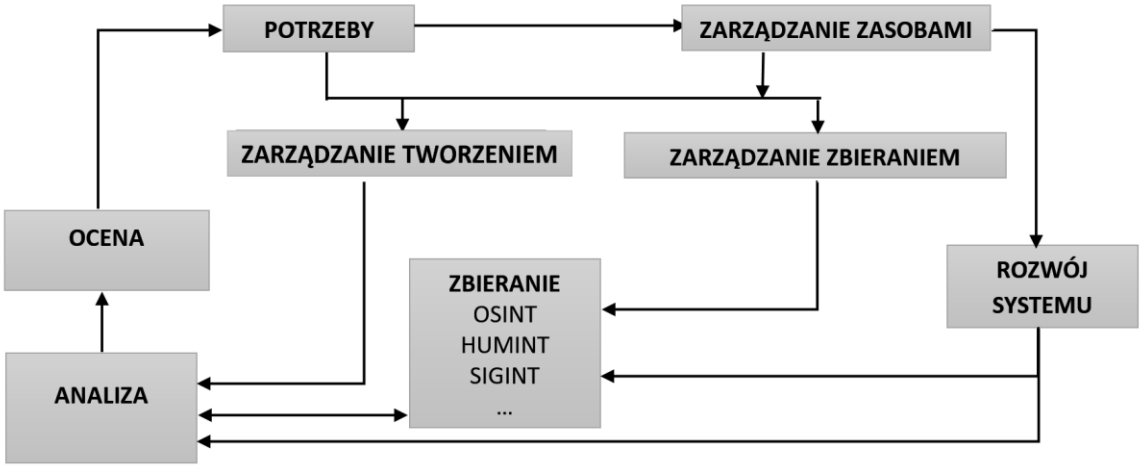
- **Produkcja / rozpowszechnianie**: na tym etapie tworzony jest i rozpowszechniana jest informacja o rozpoznaniu (wywiadowcza) dla klientów (kierownictwo, administratorzy sieci, obrońcy itp.). informacja będzie się różnić w zależności od podtypu rozpoznania i klienta. Na przykład może wymagać od raportu, informacji dla obrońców lub po prostu zatwierdzonej reguły dodanej do sprzętu chroniącego sieć.

- **Ocena**: Innym często zaniedbywanym etapem rozpoznania w sytuacjach zagrożenia jest ocena informacji w celu zapewnienia jej zgodności z pierwotnymi wymaganiami. Jeśli wymagania zostały spełnione, informacja może dodatkowo spełniać wymogi, aby pomóc opracować nowe, głębsze wymagania, które opierają się na rozpoznaniu - a cykl wywiadowczy może się powtórzyć. Jeśli analiza zagrożeń nie spełnia wymagań, sugeruje w pewnym momencie awarię, a model cyklu można wykorzystać do ustalenia, gdzie wystąpiła awaria. Czy wymagania były nierealne? Czy proces zbierania używał złych źródeł? Czy dane zawarte w źródłach zostały pobrane, ale nie zostały wyciągnięte podczas analizy?



Rysunek 17. Cykl rozpoznania. Źródło: (MWR Infosecurity, 2015).

W 1996 roku Amerykańska Senacka Komisja ds. Wywiadu opublikowała badanie, jak wywiad mógłby wyglądać w XXI wieku, jeśli zostałby zaprojektowany od podstaw. Badanie to zaproponowało funkcjonalny przepływ informacji wywiadowczych, który może być wykorzystany jako podstawa dojrzałego, skalowalnego programu rozpoznania zagrożeń informatycznych jak pokazano na rysunku 18. Pomimo podobieństwa do cyklu wywiadowczego rozpoznania zagrożeń, istnieją pewne subtelne różnice. Przepływ funkcjonalny różni się między zarządzaniem wywiadem a realizacją, a rozróżnienie to może być użyteczne przy tworzeniu i zarządzaniu zespołami organizacji. Potrzeby pozostają kamieniem węgielnym i dobrym punktem wyjścia do cyklu.



Rysunek 18. Przepływ informacji wywiadowczych. Źródło: (U. S. Government Publishing Office, 1996).

III.3 Korzyści ze stosowania rozpoznania zagrożeń cybernetycznych

INSA (Intelligence and National Security Alliance) stowarzyszenie środowisk wywiadowczych z siedzibą w Arlington zrzeszające byłych i obecnych pracowników NSA, CIA, Rady Bezpieczeństwa Narodowego, Narodowej Rady Wywiadu w swym raporcie wymienia główne zalety z taktycznego rozpoznania cybernetycznego (INSA, 2015, p. 3):

- Zapewnia kontekst i przydatność ogromnej ilości danych. Wiele organizacji posiada dostęp do terabajtów danych bez możliwości jej zrozumienia i filtrowania tak by uczynić je użytecznymi. Na poziomie taktycznym, kluczowe jest odfiltrowanie szumu. Taktyczne cyber–rozpoznanie wprowadza procesy metodyczne, które pomagają zarządzać przychodzącymi danymi, zamieniając je w cenną i praktyczną wiedze o zagrożeniach.

- Pozwala organizacjom rozwijać proaktywną postawę i wzmocnić cyberbezpieczeństwo oraz ogólne zasady zarządzania ryzykiem. Rozpoznanie na poziomie taktycznym musi być wystarczająco precyzyjne, tak aby wspierać zdolność organizacji do zminimalizowania ryzyka. Poprzez identyfikację organizacyjnych i sieciowych podatności a także wzorów postępowania przeciwnika rozpoznanie cybernetyczne może zapewnić prawdopodobną drogę ataku, odsłaniając obszary najwyższego ryzyka określając słabości tak techniczne jak i organizacyjne .

- Pomaga podejmować lepsze decyzje w trakcie i po wykryciu cyberzagrożenia. Zgromadzona w systemie informacja o zagrożeniach i dzienniki zdarzeń (logi), może zapewnić pełniejszy obraz tego, jak przeciwnik zyskał lub próbuje zdobyć dostęp do organizacji. Wskaźniki kompromitacji (IOCs) obejmujące sygnatury wirusów oraz pliki malware, adresy IP i inne wskazówki nieprawidłowej aktywności sieciowej, które mogą

pomóc ujawnić TTP (Taktyki, Techniki i Procedury) przeciwnika jest, a także, jakie dane mogły zostać przejęte. Wskaźniki kompromitacji mogą ujawnić kim jest przeciwnik, jakie może mieć intencje i motywacje.

- Ukierunkowuje cyberbezpieczeństwo na tor proaktywny, z możliwością przewidywania następnych ataków, a nie tylko reaktywny, reagujący po zaistniałym fakcie. Większa ilość zgromadzonych analiz i danych pozwoli organizacji na organizację lepszej obrony i doskonalenie technik rozpoznania cybernetycznego.

Wobec wyrafinowanych i bezwzględnych „cyberprzeciwników", organizacje muszą ciągle doskonalić swoje zdolności obronne. Mogą zatrudnić zespoły zdolnych obrońców sieci komputerowej, ale nawet najbardziej elitarni eksperci mogą nie być w stanie zabezpieczyć „cybergranic" bez użycia równie sprawnych narzędzi.

To czego potrzebują to platforma do przechowywania bardzo szczegółowych informacje na temat każdego indywidualnego zagrożenia. Potrzebują także instrumentów do wykonywania zaawansowanych analiz tych danych do tworzenia swoistych informacji wywiadowczych. I muszą być w stanie udostępniać te informacje na bieżąco wśród członków zespołu obrony, tak aby zapobiec następnym atakom cybernetycznym, zanim one nastąpią, a nie już po stwierdzonym fakcie.

III.4 Źródła rozpoznania zagrożeń cybernetycznych

- Wewnętrze – źródła wewnętrzne to wszystkie informacje zbierane wewnątrz organizacji. Najczęściej to informacje gromadzone przez firewalle, systemy zapobiegania włamaniom (IPS), systemy zabezpieczeń, antywirusy, dzienniki zdarzeń systemów czyli większość informacji wewnętrznej bierzemy z sieci organizacji. Cenną informacją są analizy po włamaniowej komputerów i odnalezione w nich cyfrowe dowody. Pełna dogłębna analiza pozwala zidentyfikować narzędzia bądź taktykę, technikę i procedury (TTP) atakujących, które nie zmieniają się tak często jak adresy czy domeny.

- Społecznościowe – ta kategoria obejmuje każdą społeczność dzieląca się informacjami o rozpoznaniu zagrożeń, która posiada relacje zaufania i wspólne interesy. Może być to także nieformalna grupa np. przedsiębiorców reprezentujących tę sama gałąź przemysłu lub zrzeszenie wyższych uczelni.

- Zewnętrzne – kategoria ta zawiera wszystkie informacje zdobywane spoza własnej organizacji lub zaufanych partnerów. Istnieją dwa typy źródeł zewnętrznych. Pierwszym z nich są źródła publiczne. Źródła te są dostępne dla każdego i zwykle są bezpłatne. Brak kosztów ponoszonych za dostęp do tych źródeł może wiązać się brakiem gwarancji dostępu to tychże usług. Istnieje wiele takich baz w sieci udostępniających adresy IP, domeny skróty niebezpiecznych plików, w różnych

formatach, często po uprzedniej rejestracji (SANS Institute , 2013, pp. 9-10), (Liska, 2015).

III.4.1 Zbieranie informacji o zagrożeniach

Informacja to nie rozpoznanie, lecz jest surowcem, który może w nie zostać przekształcony przez analizę. Podział na kategorię oraz zawartość źródło i wykorzystanie informacji o zagrożeniach obrazuje tabela 2.

Tabela 2. Kategorie informacji o zagrożeniach.

	Wskaźniki zagrożenia	Dane o zagrożeniach	Strategiczne rozpoznanie zagrożeń
Zawiera	Hashe plików, dane o reputacji adresów i domen	Statystyki, trendy, dane z badan i analiz malware	Informacje o przeciwnikach ich motywacjach, intencjach, taktykach technikach i procedurach
Kluczowe wykorzystanie	zwiększa efektywność technik blokowania i generowania alertów	Pomaga zidentyfikować wzorce związane z atakami,	Pomaga analizować ataki, stwierdzić naruszenia bezpieczeństwa, zwiększyć działania obronne
Podstawowe źródło	Honeypoty i skanery sieciowe	Statystyczna analiza wskaznikw, badań i wyników sandboksingu	Fora hackerskie, deepweb, kontakty ze środowiskiem hackerskim

Źródło (Friedman & Bouchard, 2015, p. 24).

III.4.2 Źródła informacji o zagrożeniach

Wielo organizacji, firm lub instytucji państwowych udostępnia różnorakie bazy danych z informacjami o atakach, podatnościach lub wskaźnikami kompromitacji.

- Bazy podatności
    - CVE (Common Vulnerabilities and Exposures) to lista powszechnie znanych podatności (umożliwiających uzyskanie dostępu w sposób bezpośredni – vulnerability oraz pośrednio, mogących prowadzić do kompromitacji systemu –exposure) Udostępniane w postaci XML, HTML, CSV lub TXT
    - CPE (Common Plaform Enumeracon) Ustrukturyzowany schemat nazewnictwa dla systemów i platform technologii informacyjnej dobrze określony format nazw, język do opisu złożonych platform, opularne nazwy zebrane są w CPE Dictionary

- CVSS Common Vulnerability Scoring System –platforma wymiany charakterystyk podatności i ich wpływu na infrastrukturę posiada ocenę krytyczności luk w bezpieczeństwie
- NVD National Vulnerability Database – repozytorium danych dotyczących luk w bezpieczeństwie, stanowiące syntezę CVE + CPE + CVSS • Zarządzane przez NIST (National Institute of Standards and Technology) dane w postaci XML, RSS
- Verisign's iDefense (www.verisigninc.com)
- Symantec's DeepSight (www.symantec.com)

- Źródła danych o podejrzanych adresach i domenach
  - Publikacje producentów antywirusów: Blue Coat (www.bluecoat.com), McAfee (www.mcafee.com), i Symantec (www.symantec.com)
  - Publikacje dostawców internetu: Norse (www.norse–corp.com), Verisign (www.verisigninc.com), Verizon (www.verizon.com), orange.pl
  - Publikacje organizacji zajmujących się spamem i zwalczaniem zagrożeń: Abuse.ch (www.abuse.ch), Blocklist.de (www.blocklist.de), Emerging Threats (www.emergingthreats.net), and Spamhaus (www.spamhaus.org)

- Honeypoty – to serwery lub grupy serwerów przyłączone do sieci Internet emulujące różne popularne usługi takie jak serwer WWW, FTP, SSH, bazy danych lub całe sieci w oczekiwaniu na jakąkolwiek próbę ataku, a po wykryciu ataku zbiera wszelkie informacje związane z każdym połączeniem o źródle, metodach, wykorzystanym do ataku malware, czego szukał intruz w systemie. Istnieją zaawansowane wersje honeypotów przeznaczone dla ogromnych sieci będących własnością wielkich ISP, jak również w miarę proste systemy nadające się doskonale do ochrony małej sieci firmowej lub domowe. Honeypoty celowo zawierają podatności, braki w zabezpieczeniach tak aby można było określić techniki i wskaźniki kompromitacji wykorzystywane przez cyberprzestępców.

- Skanery sieci – najbardziej znane skanery podatności to Nessus firmy Tennable, OpenVAS rozwijany przez społeczność Open Source, który powstał jako rozwidlenie (fork) projektu Nessus po jego skomercjalizowaniu oraz Nexpose stworzony przez firmę Rapid7. Jednym z najlepszych skanerów sieci Internet jest witryna shodan.io. Projekt zapoczątkowany przez Johna Matherly'ego, w ramach którego powstała nietypowa wyszukiwarka. Jednak w odróżnieniu do stanardowych wyszukiwarek treści internetowych, takich jak np. Google, Shodan pozwala na wyszukiwanie komputerów, rozmaitych urządzeń sieciowych, routerów a nawet pracujących na nich specyficznych wersji oprogramowania. Technicznie to skaner otwartych portów, który dodatkowo analizuje i indeksuje tzw. bannery. Najważniejsze metadane które indeksuje to miasto,

państwo, okolice danych współrzędnych geograficznych, nawa hosta, adres podsieci, nazwa systemu operacyjnego otwarte porty, a także nie zmienione domyślne hasła

- Bazy sygnatur i próbek malware – istnieje wiele portali udostępniających sygnatury malware, informacje o pojawiających się nowych odmianach złośliwego oprogramowania oraz powiązania miedzy pojawiającymi się już w historii podobnymi próbkami. Informacje takie są przydatne przy analizie TTP. Przykładem takiego portalu jest Team Cymru (www.team–cymru.com) lub Virustotal (www.virustotal.com). W sieci Internet można znaleźć wiele otwartych baz, które gromadzą probki malware przykładowe to: Malc0de, Malware Domain List, Malware URLs, VX Vault, URLquery, CleanMX, ZeusTracker. do pobierają można użyć różnych dostępnych skryptów jednym z popularniejszych jest maltrieve stworzony przez Kyle Maxwell'a (github.com/krmaxwell/maltrieve) lub „repozytorium żywego malware" - The ZOO Yuval'a Nativ (github.com/ytisf/theZoo).

- Zamknięte źródła informacji i relacje między ludzkie. to przeciwieństwo otwartych baz internetowych. zamknięte społeczności, do których dostęp wymaga weryfikacji lub wprowadzenia przez innych członków. Przykładem jest grupa Intel471 (intel471.com), która skupia się na zbieraniu informacji wywiadowczych infiltrując zamknięte fora i grupy dyskusyjne na całym świecie, znając ich kulturę, zwyczaje i język gromadzi dane sprawcach ataków, cyberprzestępcach i haktywistach oraz ich powiązaniach.

III.5 Reguły wymiany informacji

W świecie tradycyjnego wywiadu "*Need To Know*" czyli „wiedza konieczna" to podstawowa zasada bezpieczeństwa. Ograniczając informacje osobom, które rzeczywiście tego potrzebują, zmniejsza się prawdopodobieństwo skradzenia danych, gdy dostęp danego użytkownika (lub określonego komputera) zostanie naruszony. Jednak w świecie rozpoznania zagrożeń cybernetycznych ważniejszą jest zasada "*Need to Share*". Wszystkie formy rozpoznania zagrożeń, jeśli są dzielone, pomogą innym organizacjom w obronie przed atakami. Ustanawiając wspólne wspólnoty i relacje, każdy może czerpać korzyści z rozpoznania zagrożeń innych. Firma może ponieść straty, gdy ktoś włamie się do komputera z konkurencyjnej, ponieważ informacje skradzione mogą być często używane przeciwko innym organizacjom z tego samego sektora. Ponadto wiele ataków nie jest skierowanych do pojedynczej organizacji w izolacji, a raczej skierowane do wielu organizacji - często w tym samym sektorze - a zatem dyskusja i zrozumienie ataków może być cenne dla wszystkich powiązanych firm. Gdy całe społeczności są atakowane, społeczności te muszą bronić: celem jest podniesienie baru i stały wzrost kosztów dla napastników (MWR Infosecurity, 2015).

Tak więc bezdyskusyjną kwestią jest fakt iż, dla zwiększenia bezpieczeństwa IT niezbędna jest regularna wymiana informacji o zagrożeniach i sposobach radzenia sobie z nimi pomiędzy organizacjami działającymi w poszczególnych branżach. Jednakże nie wszystkimi informacjami można się dzielić z każdym. Często istnieje potrzeba bardziej precyzyjnego

określenia grupy odbiorców dlatego też powstał zbiór reguł nazwany TLP (Traffic Light Protocol).

III.5.1 Traffic Light Protocol

TLP to zestaw reguł, zgrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości (US-CERT, 2017). Znaczenie kolorów tak dla wysyłającego jak i dla odbiorcy pokazują tabele 3 i 4.

Tabela 3. Znaczenie kolorów TLP dla odbiorców wiadomości.

Kolor	Znaczenie dla odbiorcy
TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań.
TLP: GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: WHITE	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).

Źródło: (US-CERT, 2017).

Tabela 4. Znaczenie kolorów TLP dla autorów wiadomości.

Kolor	Znaczenie dla autora
TLP: RED	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP: AMBER	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP: GREEN	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP: WHITE	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Źródło: (US-CERT, 2017).

Informację o użytym kolorze TLP zwykle umieszcza się w nagłówku lub stopce przekazywanej wiadomości, przeważnie stosując zapis w formacie: „TLP: [Kolor]”. Należy pamiętać, że TLP nie jest używany do oznaczania informacji tajnych lub poufnych.

III.5.2 Chatham House Rule

Istnieje ciekawy dodatek do protokołu TLP, wprowadzone przez CIRCL (Computer Incident Response Center Luxembourg). Jest to tag CHR (Chatham House Rule) mówiący, że nie wolno ujawniać źródła wiadomości. Reguła Chatham House została opracowana w 1927 roku w gmachu Chatham House w Londynie[10] i udoskonalona w 1992 oraz 2002. Reguła ta brzmi: „Kiedy spotkanie, lub jego część, odbywa się według reguły Chatham House, uczestnicy mogą swobodnie korzystać z uzyskanych informacji, pod warunkiem, że tożsamość i przynależność mówiącego, ani jakiegokolwiek innego uczestnika, nie zostaną ujawnione”. Przykładowo, reguła Chatham House może być używana, gdy zgłaszający lukę w zabezpieczeniach nie chce być ujawniany (CIRCL, 2016b).

Klasyfikacja TLP AMBER może być wyrażona w następujący sposób:

```
TLP:RED informacja…
```

Jeśli istnieje konieczność rozszerzenia klasyfikacji zgodnie z zasadą Chatham House:

```
TLP:AMBER TLP:EX:CHR informacja…
```

Jeśli istnieją różne klasyfikacje TLP w tym samym dokumencie, należy wyraźnie podać klasyfikację w każdej z linii.

```
TLP:AMBER informacja pierwsza…

TLP:GREEN informacja druga…
```

III.6 Wskaźniki kompromitacji (IOC)

Informacje o zagrożeniach istnieją od wielu lat, ale dopiero od niedawna są używane przez środowisko bezpieczeństwa w sposób bardziej strukturalny i konsekwentny. Organizacje odchodzą już od tradycyjnego sposobu obsługi incydentu bezpieczeństwa przez czekanie na powiadomienie o incydencie i odpowiedz na niego. Nowatorskie podejście zaleca do podjęcia aktywnych działań do zwalczania malware w celu zabezpieczenia całej infrastruktury informatycznej. Każda kompromitacja systemu, pozostawia ślady po sobie, które później

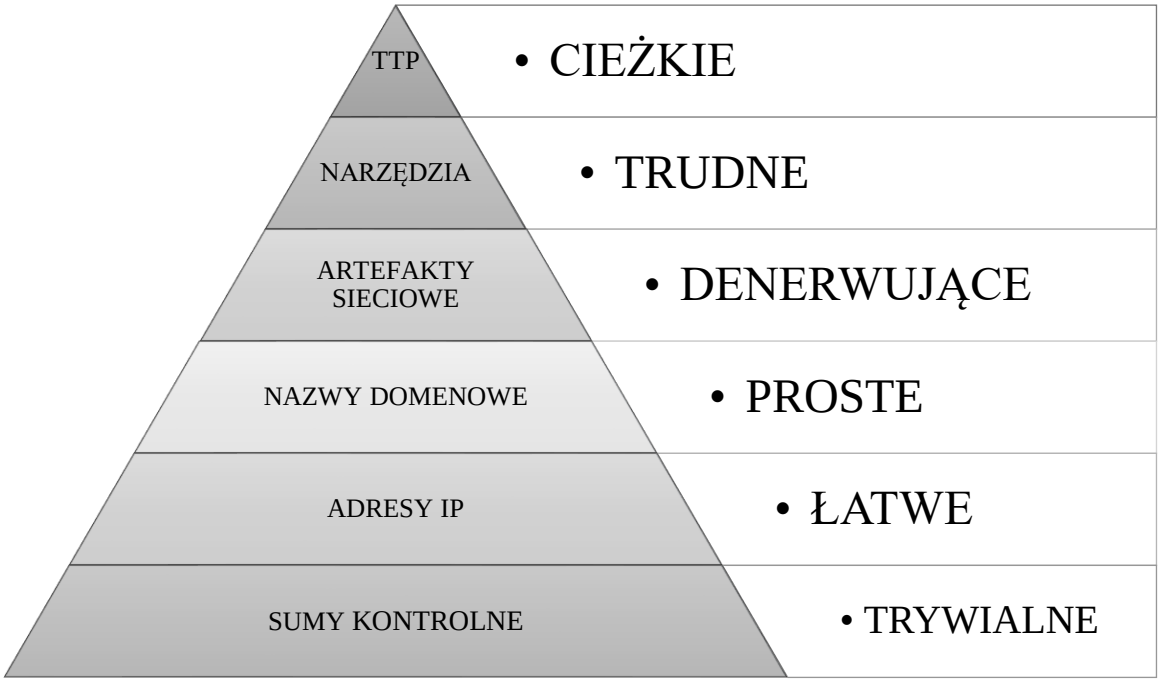
[10] Chatham House - nazwa oficjalna: *Royal Institute of International Affairs*, Królewski Instytut Spraw Międzynarodowych, najważniejszy brytyjski i jeden z ważniejszych na świecie think tanków zajmujących się badaniem stosunków międzynarodowych

można wykorzystać do identyfikacji zagrożeń lub hakera. Wskaźniki kompromitacji to właśnie te szczególne cechy, które możemy podzielić na :

- objawy widoczne dla użytkownika (np. wiadomość e–mail z charakterystycznym nagłówkiem lub treścią),
- specyficzne dla systemu operacyjnego (sumy kontrolne MD5 plików zawierających malware, ścieżki dostępu, w których się znajdują, klucze rejestru i ustawienia OS),
- charakterystyczny ruch sieciowy (adresy IP, nazwy domen, anomalie w wykorzystaniu protokołów),
- globalne IOC (wykonywane przez atakujących czynności operacyjne, jak np. specyficzne ataki, tworzenie użytkowników systemowych itp.) (Janusz, 2015).

Należy pamiętać, iż wskaźniki kompromitacji obejmują dane i metadane o podejrzanej i szkodliwej aktywności, w tym wektory ataku słabości, które wykorzystują a także działania łagodzące lub deaktywujące. Nie zawierają żadnych danych osobowych lub danych wskazujących na organizację, która została zaatakowana.

Badacz cyberbezpieczeństwa David Bianco sformułował pojęcie „piramidy bólu" przedstawionej na rysunku 20, czyli zależność między rodzajami wskaźników które można użyć, aby wykryć działania przeciwnika i ile problemów (bólu) mogło by mu spowodować ich rozpoznanie i zablokowanie (Bianco, 2014). Im wyżej wskaźnik położony jest na piramidzie tym trudniej go pozyskać Wskaźniki kompromitacji mają także różną długość życia w zależności od tego jak atakujący mogą zmieniać pewne cechy i jakim arsenałem narzędzi dysponują. Najszybciej można zmienić sumy kontrolne pliku – wystarczy drobna zmiana i hash będzie różny od oryginału, często w akcjach phishingowych dla każdego maila tworzony jest inny plik. Rzadziej . zmieniają się adresy IP oraz nazwy domen. Najdłużej żyjące, a tym samym najcenniejsze z punktu widzenia obrony, są IOC opisujące wszelkie „działania operacyjne" (TTP– Techniki Taktyki i Procedury). Czasami jest to błąd popełniony przez osoby piszące złośliwe oprogramowanie (np. logowanie się na nietypowe konto), częste używanie konkretnego narzędzia lub techniki. Cechy te, poza tym że pozwalają identyfikować nawet kolejne generacje tego samego zagrożenia – wskazują z dużym prawdopodobieństwem samych atakujących.



Rysunek 19. Piramida bólu. Źródło: (Bianco, 2014).

III.7 Protokoły wymiany informacji o malware

Wymiana informacji o zagrożeniach, jak już wspomniano, to jedna z najważniejszych kwestii przy budowie systemu rozpoznania zagrożeń informatycznych, gdy rozpoznanie ma dotyczyć grupy organizacji lub wręcz ogółu niezbędne jest dzielenie się informacjami, tak by lepiej chronić zasoby i szybciej reagować na pojawiające zagrożenia. W Stanach Zjednoczonych w dniu 17 marca 2016 r., US Department of Homeland Security ogłosił wdrożenie systemu Automated Indicator Sharing (AIS), który pozwala na wymianę informacji o rozpoznaniu zagrożeń cybernetycznych pomiędzy organizacjami prywatnymi i publicznymi. Zwiększenie szerokości i szybkości wymiany informacji zmniejszy liczbę incydentów bezpieczeństwa wśród organizacji (DHS, 2016). Wielu specjalistów od bezpieczeństwa informatycznego używa stwierdzenia *„sharing is caring”* (dzieląc się /wiedzą/ pomagasz innym) (The Economist,, 2015). Niektórzy z nich wręcz twierdzą, że w świetle coraz to szybciej zmieniających charakter ataków dla wspólnego bezpieczeństwa dzielenie się wiedzą cenniejsze jest nawet od zachowania poufności. Odpieranie nowoczesnych adaptacyjnych ataków, które mutują co kilka godzin (szybciej niż spływają sygnatury) jest praktycznie niemożliwe dla klasycznych firewalli, dlatego też sprawna wymiana wiedzy o przeprowadzanych atakach jest niezbędna dla szybkiego reagowania na pojawiające się zagrożenia (McAfee, Vincent Weafer, 2016).

Bank Anglii definiuje trzy zasadnicze kryteria wymiany informacji:

- **Właściwa treść** – informacja musi być kompletna, tak by bazując na niej odbiorca mógł odeprzeć bądź złagodzić skutki zagrożenia

- **Właściwa forma** – informacja musi być zwięzła, zrozumiała bez używani żargonu nadmiernej ilości rysunków czy tabel.

- **Właściwy czas** – informacja musi być rozpowszechniana we właściwych ramach czasowych tak by odbiorca mógł podjąć skuteczne decyzje

Powyższe kryteria są ściśle współzależne. Najlepsze rozpoznanie na świecie będzie bezużyteczne, jeśli nie będzie zrozumiane lub zostanie wysłane za późno, lub gdy przeładowana grafika lub wykresy będą starały się ukryć niskiej jakości opracowanie.

Zdefiniowane są również formy dostarczania informacji (MITRE Corporation, 2014a):

- Proste alerty wysyłane mailem, faksem lub SMS.
- Szczegółowe raporty zawierające zestawienia tabelaryczne wykresy, multimedia.
- Automatyczne przekazy wysyłane pomiędzy komputerami wykorzystują otwarte lub zamknięte standardy wymiany (dla systemów SIEM, antywirusów, firewalli, systemów IPS, IDS, lub narzędzi do forensyki.
- Interfejsy do systemów wewnętrznych (np. baz danych)
- Interfejsy API dla aplikacji do generowania zapytań lub ładowania danych
- Zabezpieczone portale internetowe zapewniające dostęp na żądanie do baz i analiz

Każda z form posiada swoje zalety i wady, raporty w formie narracji z wykresami i tabelami są łatwiejsze dla zrozumienia dla kadry zarządzającej, z drugiej zaś strony ciężko jest przetłumaczyć je do formatu zrozumiałego przez urządzenia.

Ze względu na dynamiczną naturę zagrożeń cybernetycznych informacje o nich powinny być możliwie najszybciej rozpowszechniane do innych systemów bezpieczeństwa stosowanych w organizacji, i przez nie zrozumiałą. Formaty zapisu informacji stosowane przez różne firmy lub organizacje najczęściej bazują na formacji XML. Dane zapisane w ten sposób najczęściej definiują techniczne aspekty zagrożenia, nazwy domen, adresy IP, charakterystyczne ciągi znaków, funkcje skrótu, wpisy do rejestru czy charakterystyczne żądania http. Dane te pozwalają analitykom zrozumieć anatomię ataku. Pomimo nacisku na techniczny charakter danych coraz częściej pojawiają się wskaźniki definiujące motywacje czy markery geopolityczne. Istnieją narzędzia „tłumaczące te składniki i przedstawiające je jako zrozumiałe dla człowieka :

Przykłady standardów:

- **Open IOC** (Open Indicators of Compromise) – standard ogłoszony przez firmę Mandiant w 2011 roku, jest rozszerzeniem schematu XML do definiowania i udostępniania wskaźników zagrożeń. Chociaż jest to standard sponsorowany przez firmę został również wydany jako standard otwarty i wspierany przez społeczność opensource. Schemat zawiera kompleksowy zestaw około 500 atrybutów służących do definiowanie szczegółowych technicznych wskaźników kompromitacji (IOC), standard jest rozszerzalny, OpenIOC jmoże być konwertowany lub przetwarzany do innych

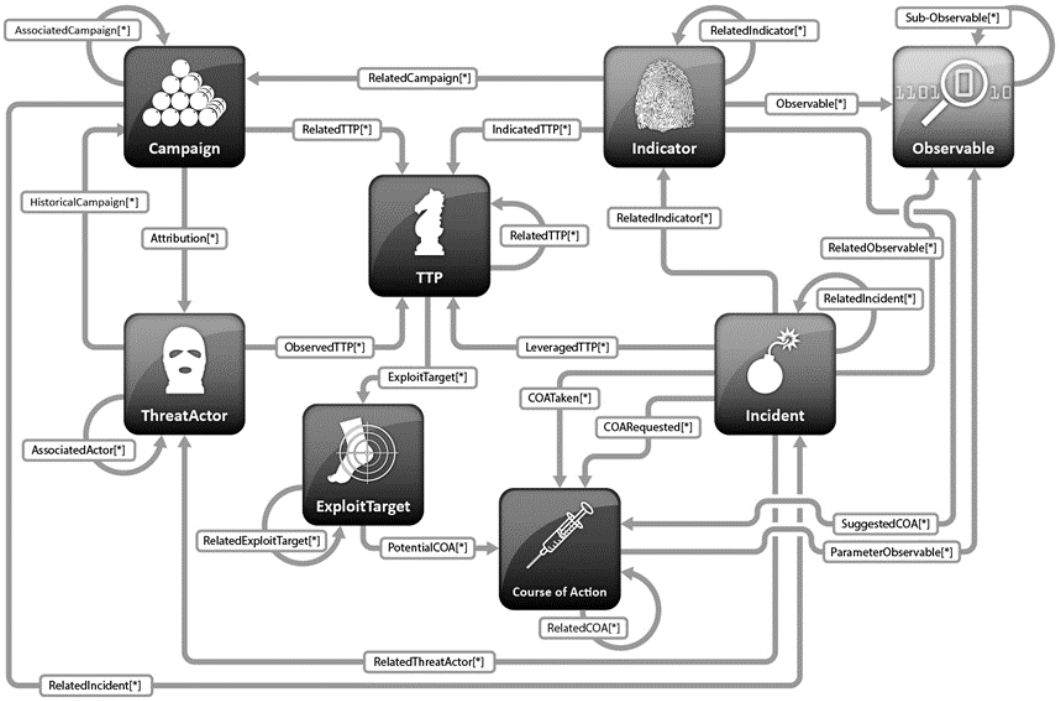
formatów definiujących IOC. OpenIOC jest wykorzystywany przede wszystkim w produktach Mandianta ale inni można z niego korzystać w innych produktach. Z tego formatu korzysta m.in. McAfee, z projektów opensource korzysta np. pyioc. (MEDIANT, 2013).

- **CybOX** (Cyber Observable eXpression) – standard zapoczątkowany przez firmę Mitre[11] w 2010 roku, jest rozszerzeniem schematu XML do definiowania i udostępniania wskaźników kompromitacji zwanymi obserwablami (observables). CybOX zawiera ponad 70 predefiniowanych obiektów, które mogą być wykorzystane do określenia obserwabli, technicznych zdarzeń bezpieczeństwa lub innych właściwości. Dzięki szerokim możliwością jego użycia do definiowania różnorakich zagrożeń można go używać w systemach arządzania i rejestrowania zdarzeń, charakteryzowania malware, systemom wykrywania i przeciwdziałania intruzom (IDS/IPS), reagowania na incydenty oraz kryminalistyki cyfrowej (MITRE Corporation, 2014a).

- STIX (Structured Threat Information eXpression) – standard zdefiniowany przez Mitre w 2012 roku, jest również rozszerzeniem schematu XML do definiowania i udostępniania wskaźników kompromitacji IOC oraz technik, taktyk i procedur – TTP. Składa się po części z obserwabli określonych przez Cybox. można również definiować relacje pomiędzy składnikami, na przykład: TTP (wzorce ataku, malware, exploity, narzędzia) mogą być powiązane z konkretnym aktorem (sprawcą) zagrożenia, którego możemy również scharakteryzować nadając mu atrybuty. możliwe jest również opisanie incydentu, celów ataku (słabości, podatności, błędnych konfiguracji), nazwanie i opisanie kampanii a także kierunków przeciwdziałania atakowi, Architektura standardu pokazana jest na rysunku 21. Źródła rozpoznania zagrożeń cybernetycznych z podziałem na typy ukazuje rysunek 22. Rozszerzenia zostały tak zdefiniowane aby współdziałać z innymi standardami, takimi jak TLP, OpenIOC, sygnaturami Snort i edytorem YARA. STIX jest sponsorowany przez Departament Bezpieczeństwa Wewnętrznego USA (DHS) i utrzymywany przez Mitre (MITRE Corportion, 2014b). Narodowy CERT USA podaje, iż standard STIX jest wynikiem wspólnych wysiłków w celu opracowania ujednoliconego, strukturalnego języka do reprezentowania informacji o zagrożeniach. Standard ten stworzona tak aby przekazać pełen zakres potencjalnych elementów danych o zagrożeniach cybernetycznych i stara się być wyrazisty, elastyczny, rozszerzalny , zautomatyzowany a także co najważniejsze czytelny dla człowieka jak to tylko możliwe. standard jest otwarty wiec cała społeczność może uczestniczyć w jego rozwoju (US-CERT, 2014). Z dużych

[11] MITRE jest amerykańską organizacją non-profit z siedzibą w Bedford w stanie Massachusetts i McLean w Wirginii . Zarządza centrami badań i rozwoju finansowanymi przez fundusz federalny (FFRDCs) wspierania kilku amerykańskich agencji rządowych. www.mitre.org

organizacji wykorzystujących STIX warto wymienić IBM, Intel, Lockheed Martin, Microsoft, RSA, Soltra, Splunk, ThreatConnect, Tripwire, Verisign oraz większość organizacji CERT narodowych (OASIS, 2016).

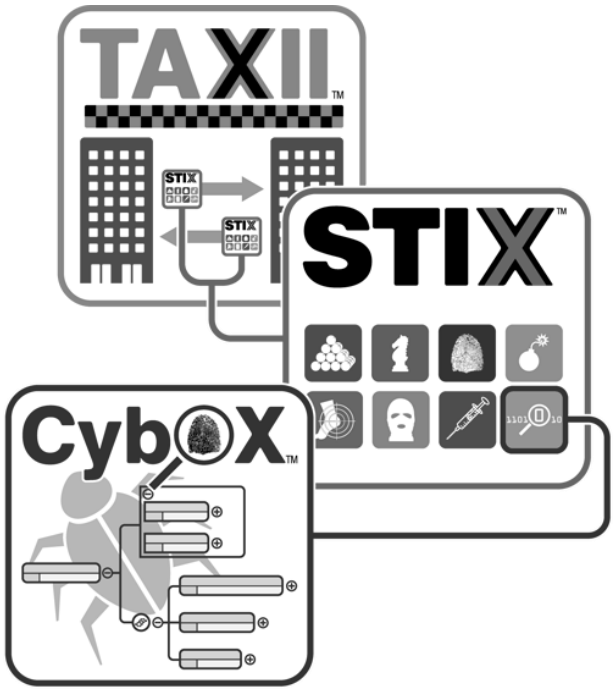


Rysunek 20. Architektura STIX, Źródło: (MITRE Corportion, 2014b).

Rysunek 21. Źródła rozpoznania w STIX. Źródło: opracowanie własne na podstawie (Smith, 2016).

- **TAXII** (Trusted Automated eXchange of Indicator Information) – standard zaproponowany przez Mitre w 2012 roku. Definiuje zestaw usług i wymiany wiadomości o rozpoznanych zagrożeniach. TAXII jest preferowaną metodą wymiany informacji w standardzie STIX. Używa XML i HTTP do transportu wiadomości. Obsługuje szeroką gamę modeli udostępniania, takich jak metoda gwiaździsta (hub–and–spoke) lub peer–to–peer, działających w trybie push i pull. Użytkownicy mogą klasyfikować i wymieniać się informacjami z partnerami w takiej formie jaką zdefiniują. TAXII został przyjęty jako planowany standard przez Microsoft w ramach Microsoft Active Protections Program (MAPP, jest również wykorzystywany przez Financial Services Information Sharing Analysis (MITRE Corporation, 2014c). Darmową otwartą platformą do wymiany informacji o zagrożeniach w formacie STIX za pomocą protokołu TAXII jest baza „Hail a TAXII" utrzymywana przez firmę Soltra zajmującą się cyber threat intelligence; w marcu 2017 roku zawierała ponad siedemset tysięcy wskaźników. baza pobiera wskaźniki z kilku największych baz: Abuse.ch, CyberCrime Tracker, EmergingThreats, Lehigh.edu, MalwareDomainList, blutmagie.de – Tor Exits, dshield BlockList, phishtank.com (Soltra, 2015)

Powiazanie pomiędzy wskaźnikami kompromitacji CybOX, wykorzystującym je standardem STIX i protokołem wymiany informacji TAXI najlepiej pokazuje rysunek 23.



Rysunek 22. Powiązanie pomiędzy CybOX, STIX i TAXII. Źródło: (US-CERT, 2014).

- **MAEC** (Malware Attribute Enumeration and Characterization) – rozwijany przez Mitre, ustandaryzowany język służący do definiowania i rozprowadzania informacji na temat złośliwego oprogramowania w oparciu o atrybuty takie jak zachowanie, artefakty

i wzorce ataków. Można go porównać z definicjami powszechnie stosowanymi w wykrywaniu złośliwego oprogramowania opartych na sygnaturach (MITRE Corporation, 2014d).

- **Microsoft Interflow™** - platforma zapewniania bezpieczeństwa I wymiany informacji o zagrożeniach dla profesjonalistów z dziedziny cyberbezpieczeństwa. to część programu Microsoft Active Protections Program (MAPP), rozpoczętego w 2008 by zapewnić bezpieczeństwo producentom oprogramowania.

- **IODEF** (Incident Object Description and Exchange Format) – standard zapoczątkowany w 2007 roku przez Internet Engineering Task Force, jako rozszerzenie schematu XML do wymiany informacji o incydentach bezpieczeństwa komputerowego między zespołami reagowania na incydenty komputerowe (CSIRT) IODEF jest zdefiniowany w dokumencie RFC 5070. Jest to model danych (ponad 30 klas i podklas), zawierający najczęściej wymieniane elementy danych oraz powiązane kontekstami wskaźniki i incydenty. Oferuje również mozliwość dokumentowania przepływu pracy (Danyliw, et al., 2007). Jest to standard otwarty wspierany przez społeczność i bardzo elastyczny – Grupa Anti–Phishing Working rozszerzyła standard IODEF do wspierania raportowania phishingu i innych zdarzeń poczty elektronicznej w systemie CIF. (Danyliw, Meijer i Demchenko (2007).

- **IODEF–SCI** – (IODEF for Structured Cyber security Information) – jest rozszerzeniem standardu IODEF zaproponowanym przez grupę Managed Incident Lightweight Exchange (MILE) Rozszerzenie dodaje obsługę dodatkowych informacji zawierających wzór ataku, platforma, lukę bezpieczeństwa, słabości systemu, raport zdarzeń, weryfikację i metodę naprawy.

- **RID** (Real time Inter–network Defense) – opracowywany przez Internet Engineering Task Force, to standard dzielenia się danymi o incydentach. RID jest również znany jako RFC 6545. RID to schemat XML na podstawie IODEF z rozszerzeniami.

- **VERIS** (Vocabulary for Event Recording and Incident Sharing) – zapoczątkowany w 2010 roku przez Verizon, schemat gromadzenia i udostępniania wywiadu o incydentach bezpieczeństwa. Schemat obejmuje dane demograficzne ofiar, opis incydentu, informacje o odkryciu i środkach zaradczych, oceny wpływu na infrastrukturę a także w ograniczonym zakresie wskaźnikach kompromitacji. Jak widać VERIS jest przeznaczony bardziej do użycia strategicznego niz taktycznego. (VERIS (2014)).

- **OTX** (Open Threat eXchange), uruchomiona w 2012 r AlienVault, publicznie dostępna usługa udostępniania informacji o zagrożeniach. OTX współpracuje z systemem firmy Open Source SIEM (OSSIM). Użytkownicy mogą konfigurować swój system SIEM tak by przesłać komunikaty o rozpoznaniu zagrożeń OTX. Zebrane dane są potwierdzone przez AlienVault a następnie dostarczane do wszystkich użytkowników OSSIM, korzystających z OTX. Informacje OTX mogą być również dostępne dla użytkowników

innych systemów do wymiany informacji o zagrożeniach (np. CIF lub CRITS). W przeciwieństwie do zamkniętych sieci wymiany informacji wywiadowczych o zagrożeniach dostępnych odpłatnie lub tylko na zaproszenie, OTX jest dostępny dla każdego, kto zdecyduje się w nim uczestniczyć. W związku z tym można zakładać, że jest to najbardziej autorytatywny system wymiany informacji o zagrożeniach pozyskiwanych z otwartej społeczności na świecie. Dodatkowo firma Alienvault współpracuje z Intelem i HP w celu (Alienvault, 2012).

- **CIF** (The Collective Intelligence Framework) – opracowany przez Research and Education Network Information Sharing and Analysis Center (REN–ISAC) w 2009 roku, jest systemem do zarządzania informacji o zagrożeniach. CIF opiera się na standardzie IODEF. Użytkownicy mogą łączyć wiele źródeł rozpoznania z różnych miejsc. Rodzaje zagrożeń zmagazynowanych w CIF to adresy IP, domeny i adresy URL związane ze szkodliwą aktywnością. CIF także zawiera informacje na temat typu zagrożenia, nasilenia ataku i zaufania do danych. REN–ISAC (CSIRT Gadgets Foundation, 2015).

- **YARA** (Yet Another Ridiculous Acronym) – opracowany przez Victora Alvareza z firmy Virustotal jest specyficzne tekstowe lub binarne sygnatury malware i narzędzi hakerskich połączone warunkami logicznymi, składnia jest zbliżona do języka Perl. YARA jest wykorzystywana m.in. przez takie projekty/laboratoria jak: Virus Total, FireEye, Kaspersky, CrowdStrike, Blue Coat, Trend Micro oraz Websense (Virustotal, 2013).

- **CAPEC (The Common Attack Pattern Enumeration and Classification)** – to kompleksowy słownik i klasyfikacja taksonomii znanych ataków stworzona przez Mitre. Jest to projekt sponsorowany przez Department of Homeland Security USA. Celem projektu było zapewnienie publicznie dostępnego katalogu wzorców ataku wraz z kompleksową schematu klasyfikacji i taksonomii. (MITRE, 2008).

III.8 Dziesięć najlepszych praktyk w zakresie rozpoznania zagrożeń.

Firma InThreat zdefiniowała 10 najlepszych praktyk wywiadowczych celem zoptymalizowania działań w sferze rozpoznania zagrożeń (inThreat, 2017):

1. **Skoncentruj się na celu**

   Rozpoznanie zagrożeń informatycznychma na celu zwiększenie bezpieczeństwa dla różnych typów użytkowników. Należy zapewnić odpowiednią i dostosowaną treść dla każdego odbiorcy.

2. **Postępuj zgodnie z zasadami**

W programie Cyber Threat Intelligence podstawowe zasady dotyczą przede wszystkim zaufania. należy się upewnić, że zasady zapewniające zaufanie są przestrzegane.

3. Myśl jak cały ekosystem

Wydajność procesu rozpoznania zagrożeń opiera się na poprawnym wykorzystaniu ludzi, procesów i technologii. Szkolenia mogą pomóc ludziom, wytyczne mogą zdefiniować proces, narzędzia Open Source mogą generować lepszą inteligencję. Należy pamiętać, aby zawsze mieć wkład, który jest cenny dla ekosystemu.

4. Jak najwięcej dziel się informacją

Jeśli chodzi o rozpoznanie zagrożeń kluczowym jest dzielenie się informacjami. Informacje dostarczone przez nas mogą pomóc innym. konieczne jest dzielenie się informacją kiedy to tylko możliwe.

5. Nigdy nie łam zasady TLP

TLP jest definiowany przez źródło, właściciela informacji. Należy postępować zgodnie z klasyfikacją TLP we wszystkich cyklach inteligencji.

6. Nie ujawniaj źródła / Chatham TLP

Istnieje wiele powodów by go nie ujawniać. Konieczne jest upewnienie się, że wewnętrzne procedury i narzędzia umożliwiają udostępnianie informacji bez nazwania źródła.

7. Opieraj się na faktach

Społeczne aspekty badań mogą prowadzić do subiektywnej interpretacji. Zbyt wiele świadectw może prowadzić do błędnej interpretacji. Sprawdź przede wszystkim wszystkie pisemne dokumenty.

8. OPSEC prowadzi do błędnych interpretacji

Bezpieczeństwo operacyjne zwykle zaciemnia szerszy obraz sytuacji. Lepiej mieć niekompletną układankę niż układankę z złymi kawałkami i fałszywymi dodatkami. Oceń pewność siebie i powstrzymaj śledztwo, gdy zaufanie jest ograniczone.

9. Używaj standardów

Normy i standardy umożliwiają interakcję między produktami a organizacjami a także pozwalają kompatybilnym produktom osiągnąć jednorodny poziom interakcji. Upewnij się, że narzędzia i dane są zgodne z obowiązującymi standardami.

10. Pytaj i używaj informacji zwrotnej

Etap rozpowszechniania wiedzy w cyklu wywiadowczym jest cenny, gdy dostarczane są sprawdzone informacje. Upewnij się, że często sprawdzasz jakość dostarczanych informacji.

ROZDZIAŁ IV. Platformy do zarządzania rozpoznaniem zagrożeń cybernetycznych

Dotychczasowe tradycyjne podejście do bezpieczeństwa informatycznego bazowało na różnych narzędziach i procesach służących do obrony sieci, prowadzenia reakcji na incydenty oraz analizy zagrożeń. Integracja i udostępnianie danych między nimi często było procesem ręcznym opierającym się na arkuszach kalkulacyjnych lub wymianie plików przez emaile. Platforma do zarządzania rozpoznaniem zagrożeń to technologia pomagająca organizacjom agregowanie korelowanie i analizowanie danych o zagrożeniach informatycznych. Importuje dane z wielu źródeł i formatów, przetwarza i koreluje te dane a następnie potrafi eksportować je do istniejących systemów bezpieczeństwa. Platforma ta automatyzuje proaktywne zarzadzanie bezpieczeństwem

IV.1.1 Możliwości i cechy platformy do zarządzania rozpoznaniem zagrożeń

Anton Chuvakin, wiceprezes działu badań i rozwoju w firmie Gartner na swoim firmowym blogu zdefiniował cechy platformy do zarządzania rozpoznaniem zagrożeń. Platforma taka powinna składać się z trzech filarów: udostępniania informacji, magazynowania danych oraz reakcji w czasie rzeczywistym. (Chuvakin, 2014) Odniósł się przy tym do autorskiej platformy ThreatData zaprezentowanej przez Facebook (Hammel, 2014) Platforma taka, wg Chuvakina powinna:

- Pozwalać na zbieranie danych o rozpoznaniu zagrożeń w różnych otwartych formatach (OpenIOC, STIX, CSV),
- Magazynować wszystkie dane również z historycznych analiz w celu wyszukiwania, dalszej analizy i porównywania do nowych zagrożeń
- Normalizować, wzbogacać i łączyć zebrane dane, by mogły zostać użyte przez inne współpracujące narzędzia.
- Sprawnie wyszukiwać i posiadać rozbudowany interfejs zapytań
- Udostępniać dane w różnych formatach

Gartner definiuje platformę zarządzającą rozpoznaniem zagrożeń na kilku obszarach. Ważne jest, aby przepływ informacji na poszczególnych etapach odbywał się w miarę

możliwości automatycznie tak aby usprawnić zarzadzanie, wykrywanie, , analizowanie i śledzenie zagrożeń (Lawson & McMillan, 2014). Główne obszary to:

Zbieranie – platforma zbiera i agreguje wiele formatów danych z wielu źródeł (STIX, CSV, OpenIOC, także emaile) .

Korelacja – platforma powinna automatycznie analizować i korelować przechwytywane informacje, tak by na bieżąco można było stwierdzić kto prowadzi atak, w jaki sposób oraz jakie przedsięwziąć środki ochronne. Funkcjonalność ta powinna być automatyczna.

Kategoryzacja – w natłoku wielkiej ilości zebranych danych konieczny jest mechanizm oznaczania danych etykietowania a także możliwość hierarchizowania informacji

Analiza – platforma automatycznie analizuje wskaźniki zagrożeń i powiązanie między nimi by umożliwić pełne, właściwe i terminowe rozpoznanie zagrożeń. Wskazanym jest by dane analityczne były przedstawiane za pomocą graficznych wizualizacji powiązań pomiędzy nimi.

Integracja – jest to jeden z kluczowych wymogów platformy. Przetworzone dane musza z powrotem powrócić do narzędzi służących bezpieczeństwu np. urządzeń sieciowych tak by spowodować blokowanie intruza. Podobnie dane uzyskane z zewnątrz po odpowiednim przetworzeniu powinny skutkować automatycznym przekazaniem ich do firewalli, IPS itd. Do pełnego wykorzystania tych funkcji powinna przyczynić się funkcjonalność API wbudowana w platformę umożliwiająca automatyzację bez angażowania użytkowników.

Działanie – sprawne wyszukiwanie określonych danych w różnych kategoriach, lub w określonych przedziałach.

Dzielenie – dojrzałą platforma zarządzająca rozpoznaniem zagrożeń powinna także umożliwiać tworzenie informacji zwrotnych do innych organizacji celem przyspieszenia i usprawniania pracy w organizacji lub instytucjach współpracujących, szerszych społecznościach czy też ośrodkach analitycznych. Informacje wytworzone przez nasz ośrodek mogą przyczynić się budowania większych strategii obrony.

IV.2 CRITS – platforma do zespołowych badan nad zagrożeniami

CRITS to narzędzie z interfejsem webowym, które łączy w sobie instrumenty analityczne z bazą zagrożeń cyberprzestrzeni. CRITS to nie tylko repozytorium informacji o atakach i malware, ale także rozbudowana platforma do prowadzenia analiz malware, korelowania wiadomości o złośliwym oprogramowaniu. Analizy i korelacje mogą być także zapisywane, wykorzystywane po za bazą CRITS dzięki serwisom umożliwiającym eksport i import danych.

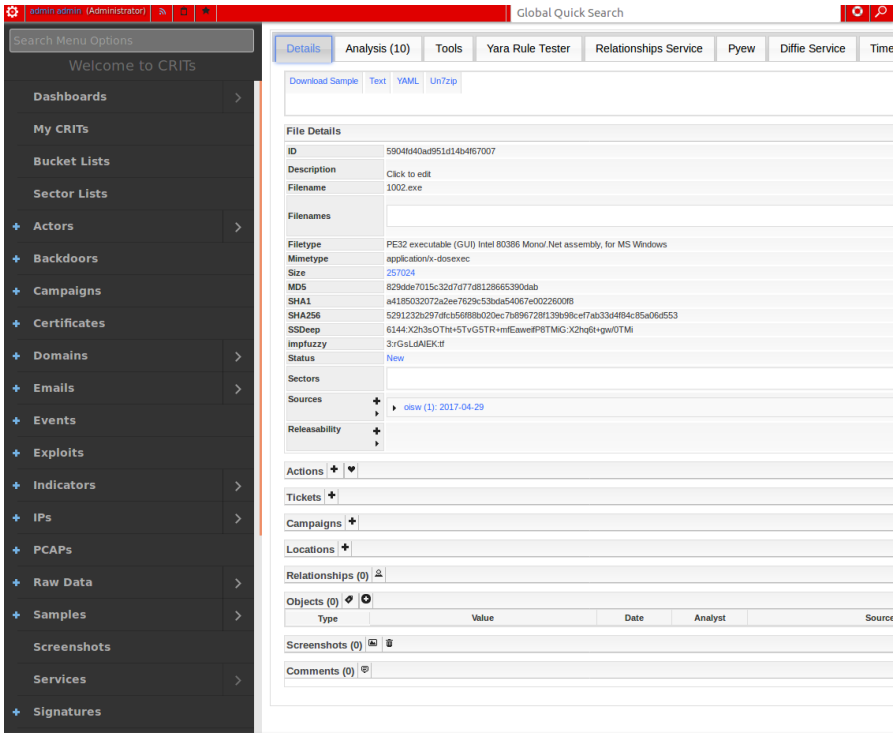
IV.2.1 Historia, założenia

CRITS został stworzony przez Mike'a Goffina – inżyniera ds. analityki cyber zagrożeń w MITRE w roku 2010 jako narzędzie do zarządzania złośliwym oprogramowaniem. Projekt miał z założenia miał być napisany w Pythonie, przy użyciu biblioteki Django i składować dane w bazie MySQL. Początkowo pozwalał na magazynowanie próbek malware i danych o przechwyconych pakietach PCAP, później dodano przechowywanie e-maili, danych o adresach IP i domenach. Następnie wprowadzono wskaźniki kompromitacji. Na końcu dodano możliwość dodawania informacji o kampaniach, certyfikatach, wydarzeniach, surowych danych i celach. 18 czerwca 2014 r. kod projektu został uwolniony i opublikowany na serwerze Github na licencji Open Source .

IV.2.2 Platforma

CRITS to platforma analizy zagrożeń, która ułatwia agregację, analizę i dzielenie się technicznymi informacjami o zagrożeniach cybernetycznych. Zarządza olbrzymią ilością danych zgromadzonych przy analizie pojedynczych, często odmiennych ataków cybernetycznych i przeprowadza analizy w celu odkrycia wzorców w celach, narzędziach i technikach przeciwnika. CRITS składa te pozornie rozłączone kawałki układanki w spójny obraz zagrożenia cybernetycznego. Używając wspólnego słownictwa, CRITS natychmiast rozpowszechnia to "zdjęcie" do innych użytkowników, aby zapobiec przyszłym naruszeniom.

Platforma CRITs może obsługiwać wiele różnych typów użytkowników, od analityków zajmujących się złośliwym oprogramowaniem po ekspertyzy w inżynierii wstecznej. Głębokość i różnorodność informacji dzielonych między wielu specjalistów mogą pomóc w ciągłym otwarciu nowych sposobów korzystania z tego narzędzia. Interfejs oferowany przez aplikację pokazany jest na rysunku 23,



Rysunek 23. CRITS badanie próbki malware. Źródło: opracowanie własne.

IV.2.3 Współpraca z innymi aplikacjami i serwisami

Wielką zaletą aplikacji CRITS jest mnogość serwisów i aplikacji z którymi można ją połączyć celem sprawnej i pełniejszej analizy. Do analizy można zaprząc silniki antywirusowe, sandbox, narzędzia do analizy binarnej (exiftool, macro extract, office meta, pdfinfo peinfo), aplikacje do analizy ruchu sieciowego (carver, ChopShop). CRITS współpracuje z sandboksem Cuckoo, pozwala dezasemblować kod w samej aplikacji dzięki wtyczce do deasemblera Pyew. badane próbki i wskaźniki kompromitacji można oznakowywać tagami oraz przyporządkowywać do danych kampanii czy aktorów.

Rysunek 24. Dodatki i pluginy do CRITS'a. Źródło: opracowanie własne.

IV.3 MISP

MISP (*Malware Information Sharing Platform*) jest oprogramowaniem rozpowszechnianym na licencji Open Source służącym do zbierania, przechowywania, dystrybucji i udostępniania wskaźników zagrożenia bezpieczeństwa cybernetycznego i analizy na temat incydentów związanych z bezpieczeństwem cybernetycznym i analizy złośliwego oprogramowania. MISP został zaprojektowany przez i dla analityków, specjalistów zajmujących się incydentami bezpieczeństwa, do wspierania ich działalności na co dzień tak, aby efektywnie dzielić się informacjami. MISP powstał by wspomóc misje NCIRC TC – *NATO Computer Incident Response Capability Technical Centre.* Umożliwia współdzielenie informacji o malware w zaufanej społeczności bez konieczności udostępniania informacji o kontekście incydentu. System ten posiada łatwo przeszukiwane repozytorium z wielokierunkowym mechanizmem dzielenia się informacjami. MISP posiada także dość zaawansowaną automatyzacje przy eksporcie i imporcie danych i łączeniu się z innymi systemami. Głównym celem tej aplikacji jest przyśpieszenie wykrywania incydentów bezpieczeństwa, które nie mają jeszcze zdefiniowanych sygnatur lub wyrafinowanych ataków APT (NATO Communications and Information Agency, 2015)

MISP dostarcza funkcjonalności do wspierania wymiany informacji, ale również wykorzystania tych informacji przez systemy ochrony sieci NIDS (*Network Intrusion Detection*

System), ochrony przed wyciekiem informacji LIDS, ale również systemy analizy dzienników systemowych, czy SIEM *(Security information and event management*).

IV.3.1 Cechy MISP

- Wydajna baza wskaźników kompromitacji oraz wskaźniki pozwalające na przechowywanie informacji technicznych i nietechnicznych o złośliwych próbkach, incydentach, atakujących i rozpoznaniu.

- Automatyczna korelacja odnalezionych powiązań między atrybutami i wskaźnikami złośliwego oprogramowania, kampaniami i analizami.

- Wbudowana funkcjonalność współdzielenia, ułatwiająca wymianę danych za pomocą różnych formatów. MISP automatycznie synchronizuje zdarzenia i atrybuty od innych serwerów MISP. Zaawansowane funkcje filtrowania mogą być wykorzystane tak aby można było utworzyć różnorakie polityki udostępniania informacji w organizacji oraz pojemności grupowego udostępniania i mechanizmów dystrybucji poziomie atrybutów.

- Intuicyjny interfejs użytkownika dla użytkowników końcowych do tworzenia, współdziałania i aktualizacji informacji o wydarzeniach i wskaźnikach kompromitacji. Graficzny interfejs pozwala płynnie nawigować między zdarzeniami i ich korelacją. Zaawansowane funkcje filtrowania i listy ostrzegawcze pobierane z różnych otwartych źródeł, pomagające analitykom współdzielić informacje o wydarzeniach i atrybutach.

- Przechowywanie danych w formie strukturalnej (umożliwiające zautomatyzowane korzystanie z bazy danych dla różnych celów, np. jako źródło danych dla systemów bezpieczeństwa) ze wsparciem wskaźników cyberbezpieczeństwa a także wskaźników oszustwa, (fraud) do współpracy z sektorem finansowym.

- Eksport: generowanie sygnatur dla IDS (Suricata, Snort i Bro), OpenIOC, tekst, CSV, MISP XML lub JSON do integracji z innymi systemami (NIDS HIDS) STIX (XML i JSON), NIDS oraz wiele innych formatów – łatwe rozszerzanie przez dodatkowe moduły.

- import: import całych zestawów, , import z OpenIOC sandoboksa, ThreatConnect CSV. wiele innych formatów – podobnie jak przy eksporcie łatwe rozszerzanie przez dodatkowe moduły.

- Elastyczne narzędzie importowania z otwartego tekstu, tak by ułatwić integrację niestrukturalnych raportów do MISP.

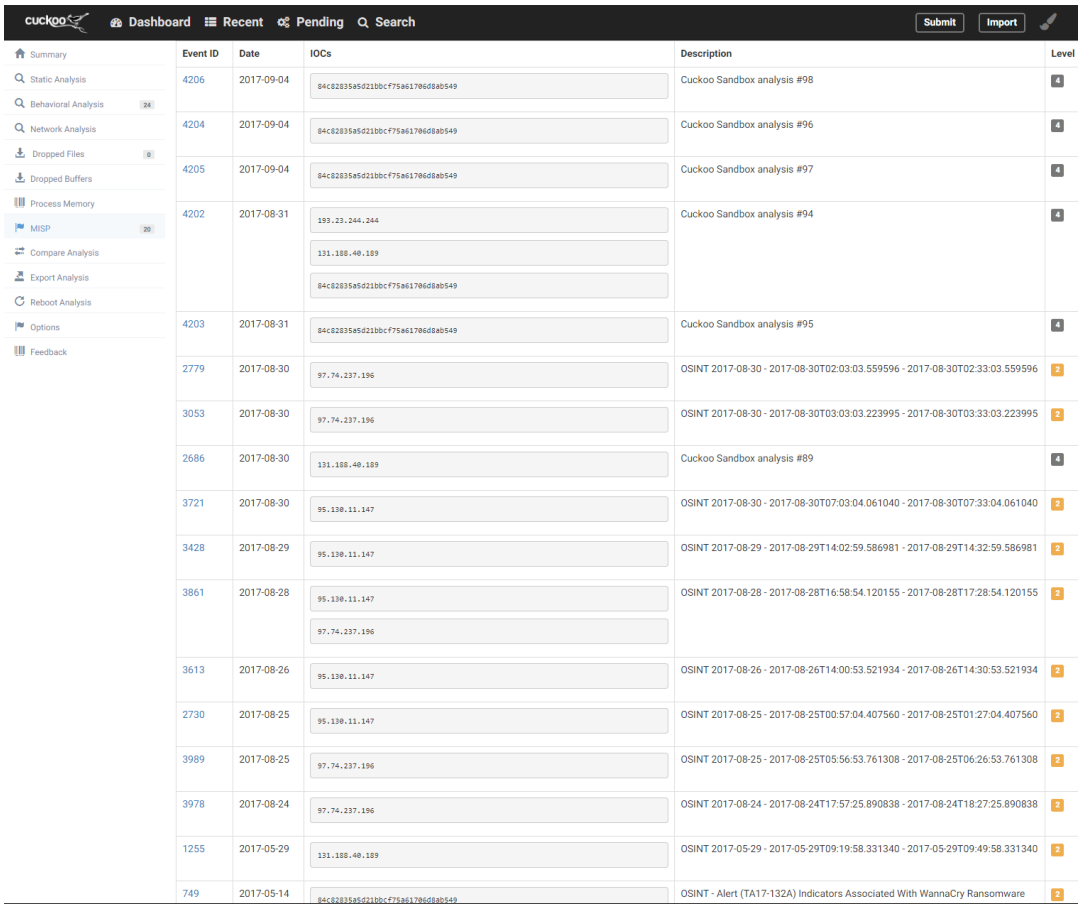
- System współpracy przy obsłudze incydentów i atrybutów pozwalających użytkownikom MISP zaproponować zmiany lub aktualizacje atrybutów i wskaźników.

- udostępnianie danych: automatycznej wymiana i synchronizacja z innymi organizacjami i społecznościami korzystającymi z MISP.
- Elastyczny interfejs API do integracji MISP z własnymi aplikacjami. MISP posiada wbudowaną bibliotekę python PyMISP pozwalającą na korzystanie z systemu przez inne systemy
- Elastyczny system klasyfikacji incydentów umożliwiający korzystanie z własnego lub istniejącego systemu klasyfikacji. Taksonomia może być wykorzystywana lokalne ale również współdzielona między współpracującymi systemami MISP.
- Moduły rozszerzające w Pythonie, aby rozwinąć system MISP do własnych potrzeb.
- Eksport danych w formacie STIX (XML i JSON).
- wbudowane szyfrowanie i podpisywanie zgłoszeń poprzez PGP lub S/MIME w zależności od preferencji użytkownika.

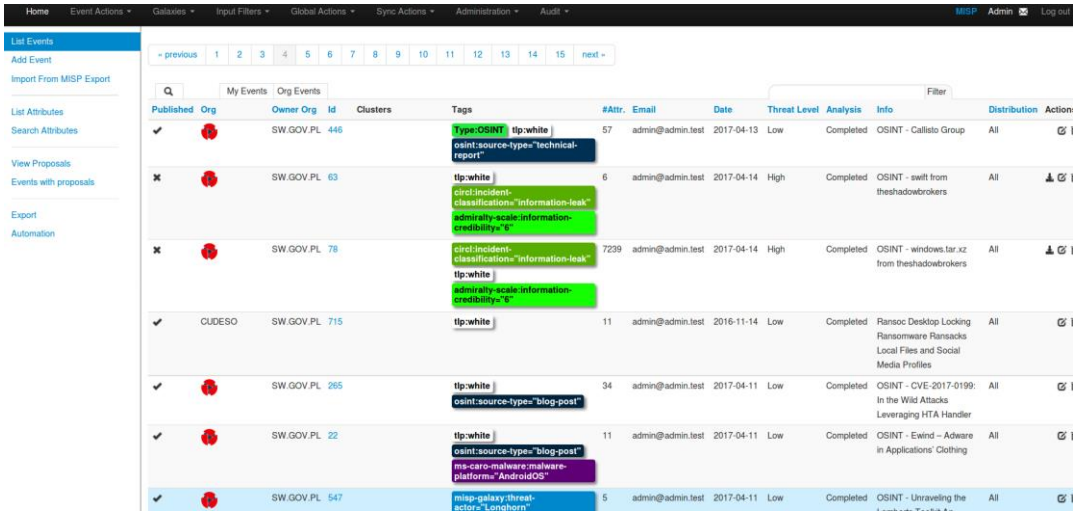
Przechowywane dane są natychmiast dostępne dla współpracowników organizacji partnerskich, istnieje możliwość powiadamiania o nowych danych szyfrowanym emailem jeśli tylko zaznaczymy odpowiednie opcje

System potrafi generować gotowe sygnatury dla innych systemów w następujących formatach Snort/Suricata IDS, STIX, OpenIOC, tekst lub csv . MISP pozwala także na automatyczny import danych z innych systemów. Import danych można wykonać z różnych formatów: OpenIOC, z pliku tekstowego, z sandboksów, lub z innych formatów za pomocą szablonów. Oczywiście można importować dane z innych instancji MISP uruchomionych w naszych organizacjach partnerskich. Dzięki takiej współpracy możemy od razu zobaczyć relacje i wskaźniki miedzy już opracowanymi raportami przez inne organizacje a badanymi przez nas próbkami.

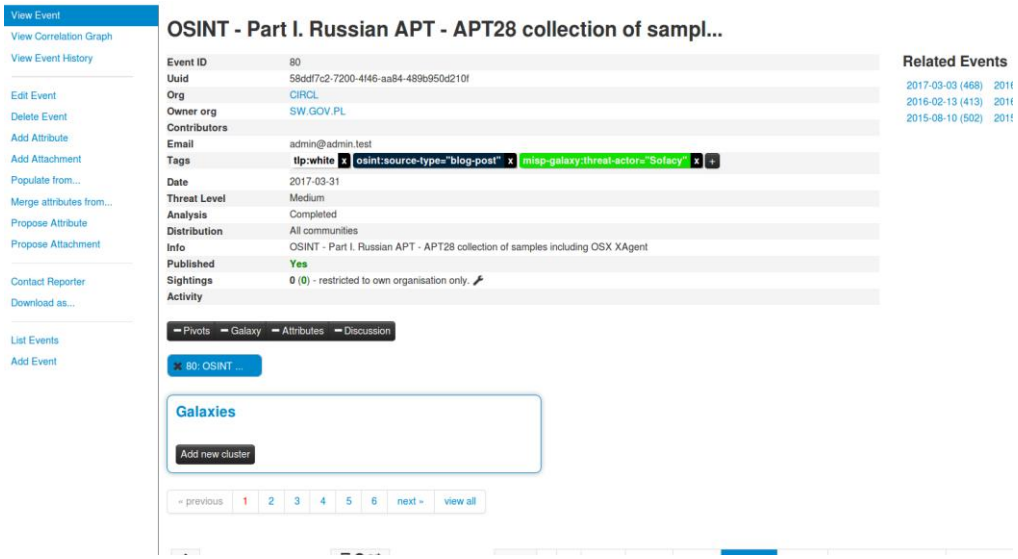
MISP bardzo dobrze współpracuje z opisywanym w rozdziale II.2.1sandboksem Cuckoo tak jako źródło danych do bieżącej analizy, jak i repozytorium przeprowadzonych już analiz do dalszej pracy. Współpracuje także z opisywanym w rozdziale IV.4 niniejszej pracy IntelMQ, oraz LOKI z rozdziału IV.6.



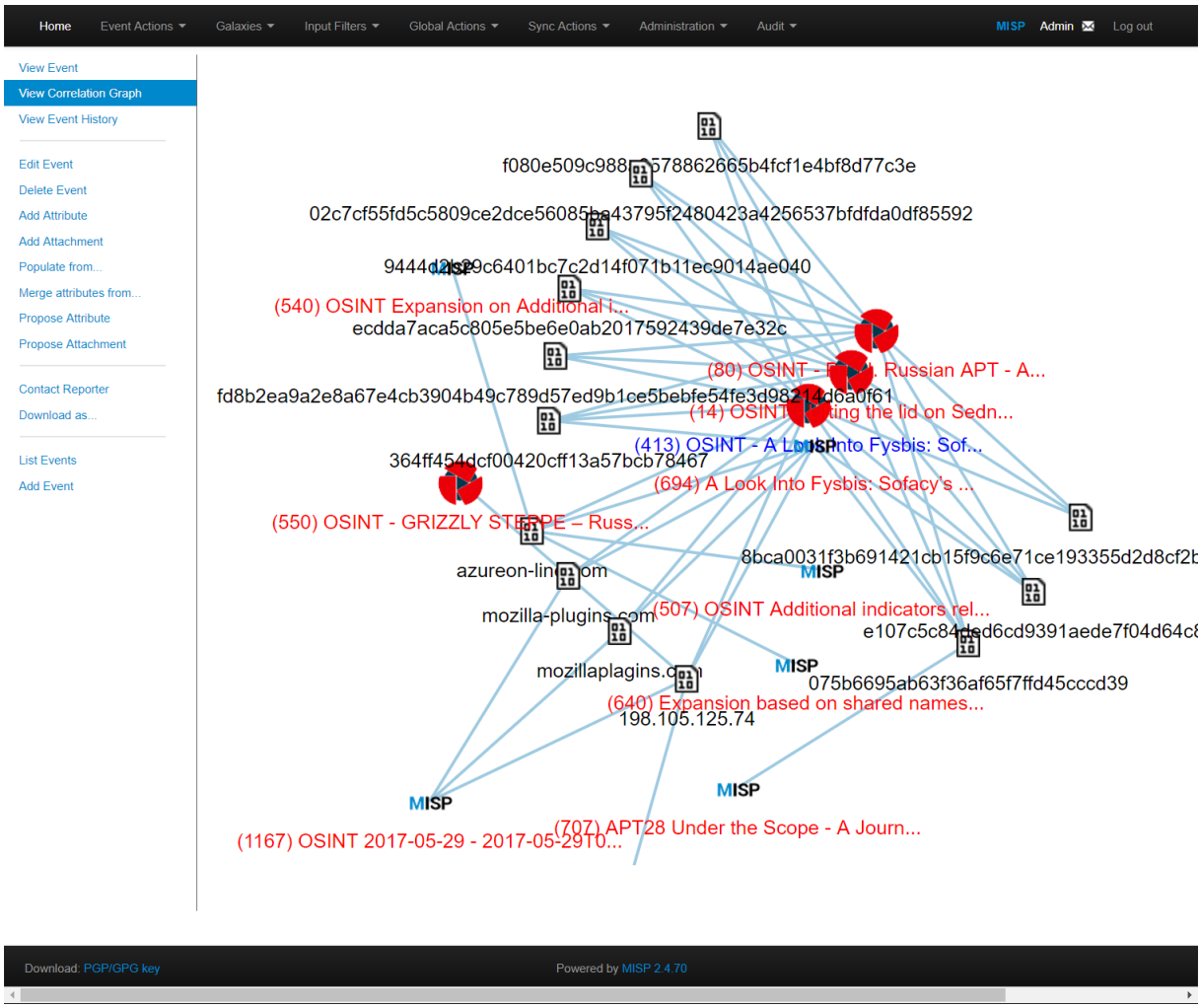
Rysunek 25. Współpraca sandboksa Cuckoo z MISP. Źródło: opracowanie własne.



Rysunek 26. Interfejs MISP Źródło: opracowanie własne.



Rysunek 27. Informacja o jednym z ataków grupy APT28. Źródło: opracowanie własne.



Rysunek 28. Graf powiązań jednego z ataków APT28. Źródło: opracowanie własne.

MISP to nie tylko oprogramowanie typu open source, a także duża społeczność użytkowników MISP, którzy tworzą, utrzymują i działają w aplikacji dzieląc się informacjami na temat zagrożeń i wskaźników bezpieczeństwa internetowego na całym świecie. CIRCL prowadzi dużą społeczność MISP składającą się z ponad 500 organizacji, adresowaną głównie do organizacji prywatnych, firm, instytucji finansowych lub firm zajmujących się bezpieczeństwem IT (CIRCL, 2016). CiviCERT to organizacje zrzeszone w ramach partnerstwa między dostawcami treści internetowych i usługodawców, organizacjami pozarządowymi i osobami, które przyczyniają się do czasu i zasobów społeczności, aby globalnie poprawić świadomość bezpieczeństwa społeczeństwa obywatelskiego.

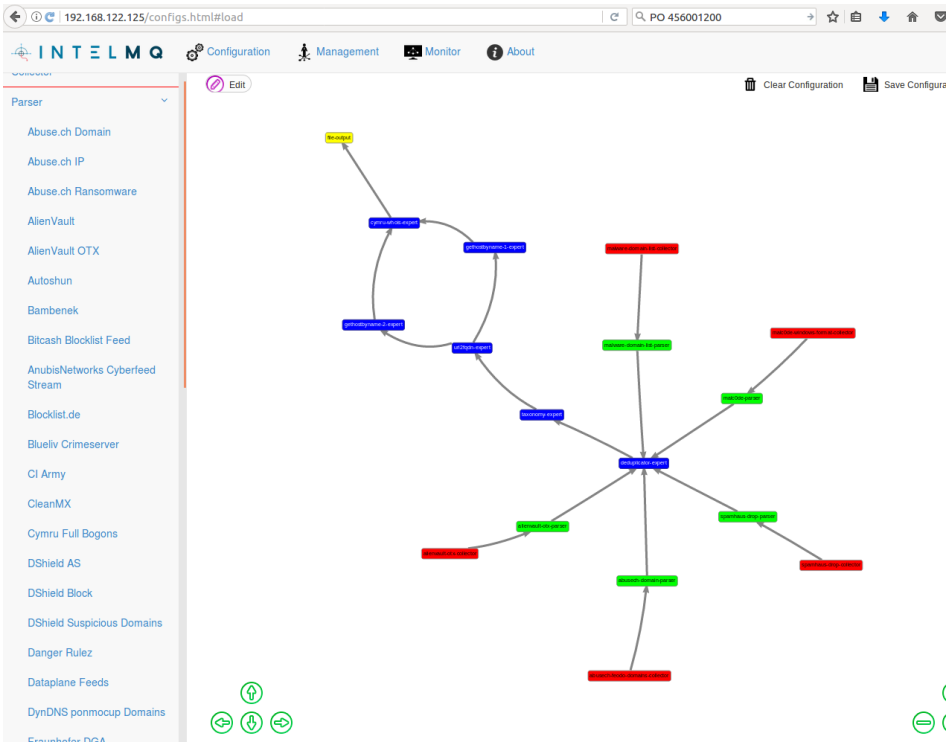
MISP posiada funkcję „feed", która pozwala na pobieranie bezpośrednio zdarzeń MISP z innych serwerów. Domyślnie włączane w MISP są dwa kanały OSINT - CIRCL (*The Computer Incident Response Center Luxembourg*) centrum reagowania na incydenty komputerowe w Luksemburgu - to inicjatywa kierowana przez rząd księstwa Luksemburg, mającą na celu gromadzenie, przeglądanie, raportowanie i reagowanie na zagrożenia i incydenty związane z bezpieczeństwem komputerowym oraz BOTVRIJ.EU projekt sponsorowany przez belgijską firmę *Cudeso* zajmującą się obsługa incydentów, przeprowadzaniem skanów bezpieczeństwa, testami podatności i szkoleniami z zakresu bezpieczeństwa. Dodatkowo dostawcy i partnerzy mogą łatwo udostępniać swoje kanały za pomocą prostego generatora PyMISP .

IV.4 IntelMQ

IntelMQ to rozwiązanie dla zespołów CERT służące do zbierania i przetwarzania informacji o zagrożeniach, danych z otwartych źródeł informacji o zagrożeniach (pastebin lub tweetera) i plikach dziennika systemu (logów) przy użyciu protokołu kolejkowania wiadomości. Jest to otwarta inicjatywa wspierana przez społeczność IHAP (Incident Handling Automation Project) a jej koncepcja została opracowana przez Europejski CERT – ENISA podczas kilku imprez InfoSec. Głównym celem jest zapewnienie, osobom reagującym na incydenty łatwy sposób na gromadzenie i przetwarzania informacji o rozpoznaniu zagrożeń poprawiając w ten sposób procesy obsługi incydentu (ENISA, 2017).

System nie wymaga specjalistycznej wiedzy do administrowania i obsługi, pozwala na łatwe dostosowanie agentów do nowych usług, pozwala na łączenie się z już działającymi systemami CIF, MISP, AbuseHelper. Zapewnia łatwy sposób przechowywania danych w kolektorach logów jak ElasticSearch, Splunk itd. Zapewnia łatwy sposób tworzenia własnych czarnych list. Zapewnia łatwą komunikację z innymi systemami za pośrednictwem HTTP RESTFUL API. Źródła danych dla IntelMQ to m.in. Abuse.ch, AlienVault, Autoshun, Bambenek, Bitcash Blocklist, Anubis, Blocklist.de, Blueliv Crimeserver, CI Army, CleanMX, Cymru Full Bogons, DShield AS, DShield Block, DShield Suspicious Domains, Danger Rulez,

Dataplane Feeds, DynDNS, Fraunhofer DGA, Generic CSV, HpHosts, JSON, MISP, Malc0de, Malware Domain List, Malware Domains, MalwarePatrol Dans Guardian, N6Stomp, Netlab 360, Nothink, OpenBL, OpenPhish, PhishTank, Proxyspy, ShadowServer, Spamhaus CERT, Spamhaus Drop, Taichung, Turris Greylist, URLVir, VXVault (ENISA, 2017).



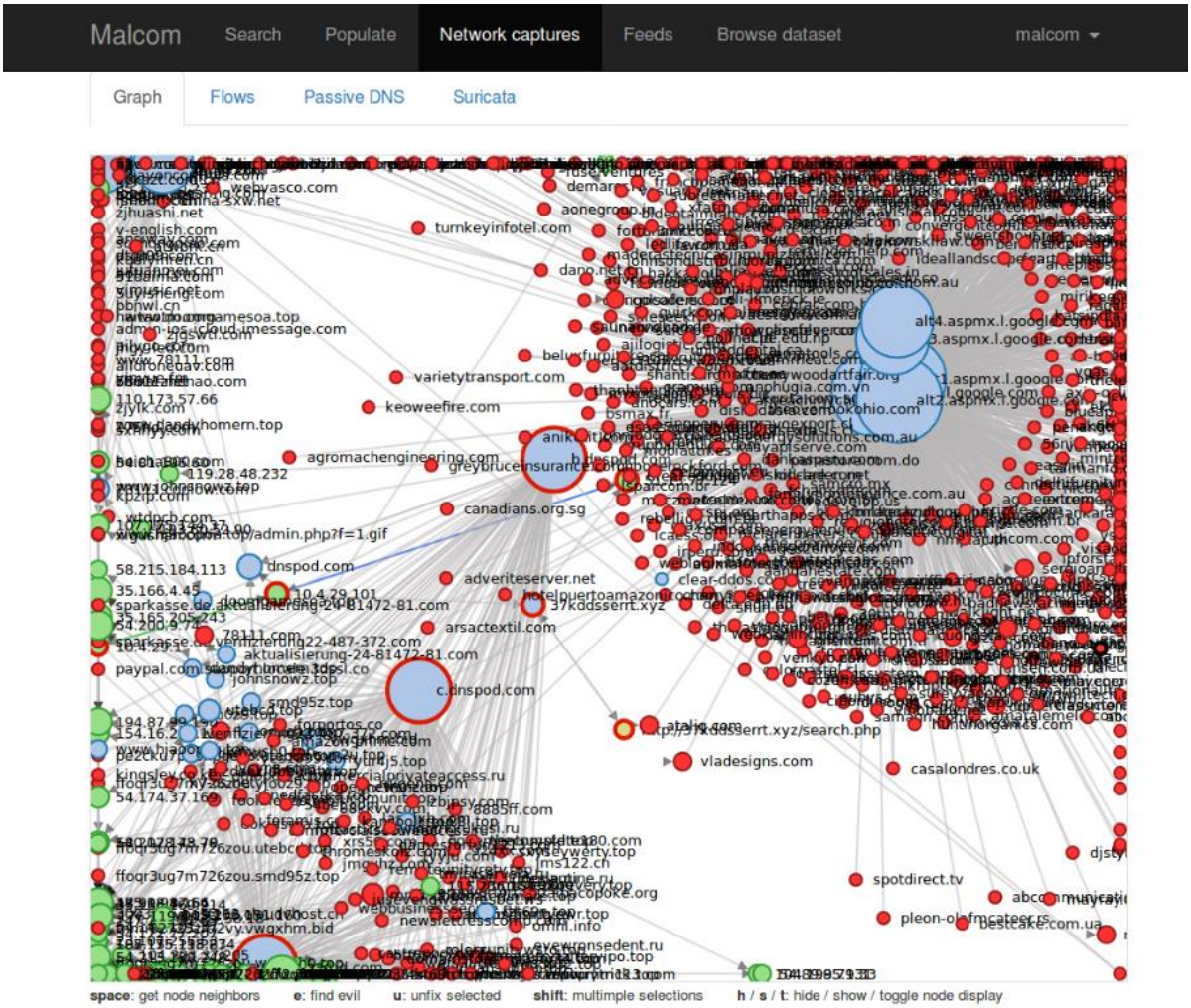
Rysunek 29. Przepływ danych w aplikacji IntelMQ. Źródło: opracowanie własne.

IV.5 Malcom

Malcom jest narzędziem służącym do analizy komunikacji sieciowej systemów za pomocą graficznego przedstawienia ruchu sieciowego a także do porównanie ruchu ze znanymi źródłami złośliwego oprogramowania. Jest to niezwykle przydatne przy analizowaniu sposobu, w jaki niektóre gatunki złośliwego oprogramowania próbują komunikować się ze światem zewnętrznym. Celem aplikacji jest przyśpieszenie analizy malware i rozpoznania zagrożeń poprzez dostarczenie ruchu sieciowego pochodzącego z danego hosta lub sieci w sposób czytelny dla człowieka. Malcom pomaga przy:

- wykrywaniu serwerów C&C.
- zrozumieniu komunikacji peer-to-peer.
- obserwacji infrastruktury DNS, fast-flux.
- szybkim stwierdzeniu, czy artefakt sieci jest „zły”
- analizie ruchu online.

- można pracować na aktywnym ruchu sieciowym, można także wczytać pliki PCAP.



Rysunek 30. Powiazanie pomiędzy serwerami dużego bota w sieci. Źródło: opracowanie własne.

Zaletą aplikacji jest przedstawienie ruchu sieciowego w postaci grafu powiązań, dzięki temu szybko możemy określić źródła ataku i zaproponować metody obrony, przykładowy graf dużego bota sieciowego przedstawia rysunek 30, rysunek 31 pokazuje próbę wyszukania złośliwych domen w otoczeniu sieciowym uczelni SGH. Jak widać jedyne domeny oznaczone w bazach jako złośliwe powiązane są z dostawcą domeny waw.pl lub dostawcami usługi DNS.

Rysunek 31. Niebezpieczne hosty powiązane z SGH. Źródło: opracowanie własne.

IV.6 LOKI

LOKI jest darmowym narzędziem na licencji OpenSource służącym do skanowania stacji roboczych serwerów pod kontem występowania wskaźników kompromitacji, stworzonym przez Floriana Rotha pracującego dla niemieckiej firmy BSK-Consulting i służy m.in. do wykrywania niebezpiecznych plików malware, trojanów typu RAT oraz różnych innych narzędzi hakerskich a także wszelkich ich śladów po włamaniach do systemów informatycznych. LOKI oferuje prosty skaner, który wykryje w systemie tego typu niebezpieczne pliki. Podobnie jak oprogramowanie antywirusowe, zawiera w sobie odpowiednie definicje złośliwych plików (IOC), trojanów i innych narzędzi do przejmowania kontroli nad systemami informatycznymi, wykorzystywanych przez hakerów a nawet zagraniczne służby specjalne (LOKI posiada m.in. definicje niektórych narzędzi wykorzystywanych przez GCHQ, NSA oraz Hacking Team. (Roth, 2015)

Aplikacja potrafi subskrybować wydarzenia i wskaźniki kompromitacji z serwera MISP opisywanego w rozdziale VI.3 a także z bazy OTX firmy Alienvault opisywanej

w rozdziale III.7 (jednego z najczęściej wybieranych dostawców baz służących rozpoznaniu zagrożeń cybernetycznych) w celu przeprowadzenia skanowania.

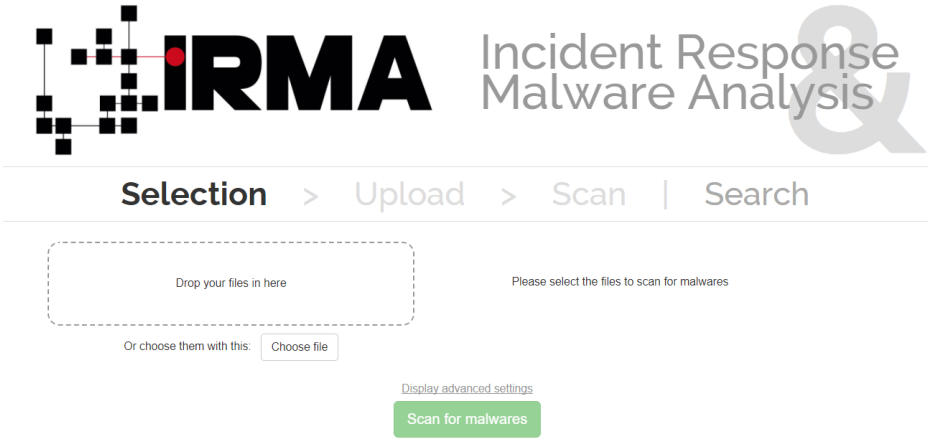
LOKI zawiera m.in. wskaźniki powiązane z:

- Malware grupy Equation (Hashe, sygnatury Yara od Kasperskiego oraz 10 autorskich reguł wygenerowanych przez autora narzędzia LOKI);
- Carbanak APT – (Hashe, nazwy plików IOCs);
- Arid Viper APT – (Hashe);
- Anthem APT Deep Panda (oficjalnie niepotwierdzone);
- APT jednostki 78020;
- Malware Regin (GCHQ / NSA / FiveEyes - w tym Legspin oraz Hopscotch);
- Five Eyes QUERTY Malware;
- Skeleton Key Malware;
- Lenovo Superfish (sygnatury Yara);
- Duqu 2 (sygnatury Yara);
- WoolenGoldfish – (hashe SHA1, sygnatury Yara);
- OpCleaver (kampania APT rodem z Iranu);
- Ransomware Locky;
- Narzędziami grupy Hacking Team - (sygnatury Yara);
- Ponad 180 narzędziami hakerskimi - (sygnatury Yara);
- Ponad 600 innymi złośliwymi plikami - (sygnatury Yara);
- Złośliwymi plikami malware - (ponad 10 000 hashy MD5, SHA1 i SHA256);
- Wieloma innymi podejrzanymi plikami - (ponad 1000 sygnatur regex) (Roth, 2017).
- możemy także dopisywać recznie swoje wskaźniki jeśli istnieje taka potrzeba

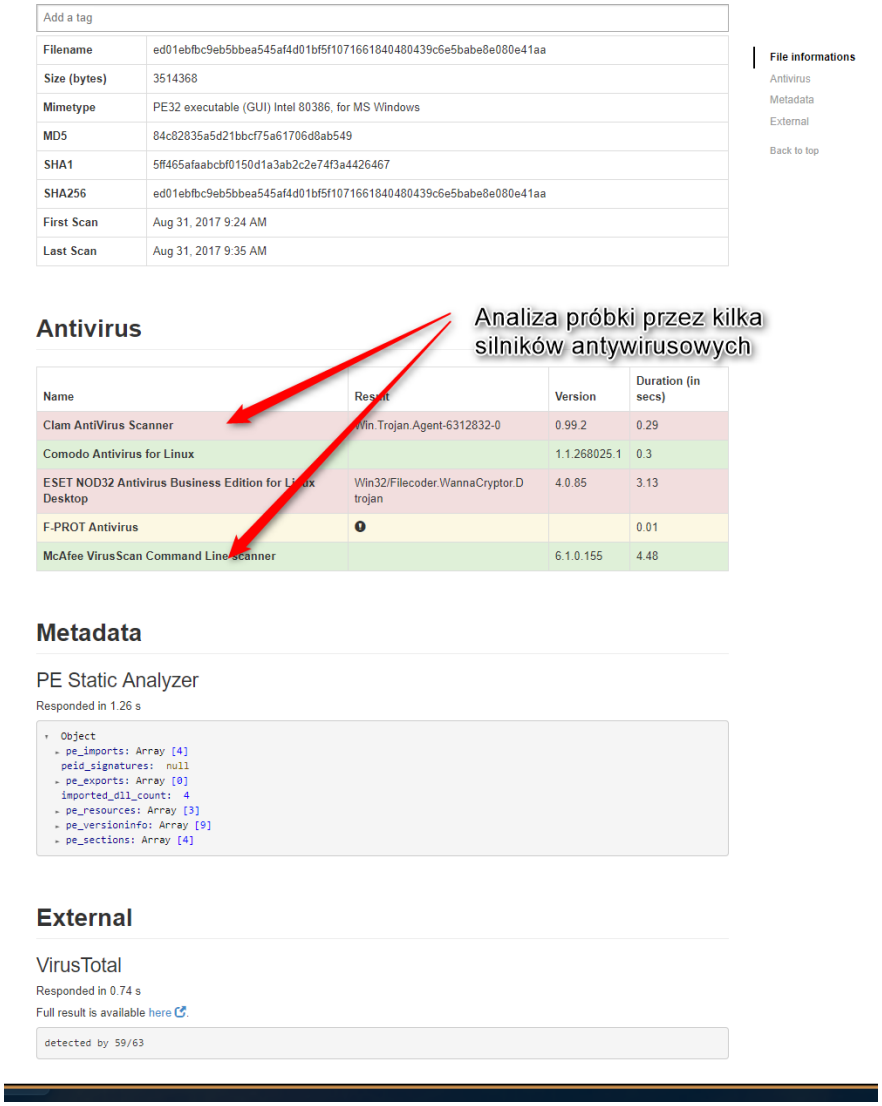
Darmowy skaner LOKI działa na systemach 32 oraz 64 bitowych i nie wymaga instalacji.

IV.7 IRMA

IRMA to platforma open source zaprojektowaną w celu ułatwienia identyfikacji i analizy złośliwych plików. celem aplikacji jest sprawdzenie próbki oprogramowania na kilku silnikach antywirusowych (podobnie jak to ma miejsce w serwisie Virustotal) jednakże próbka nie jest nigdzie wysyłana na zewnątrz. dzięki temu istnieje możliwość szybkiego przeskanowania próbki bez opuszczania jej wewnętrznej sieci organizacji. możemy sprawdzić dokumenty dostarczone przez partnerów i inne organizacje pod kątem zawartości złośliwego oprogramowania – dobrym przykładem jest sprawdzenie wpływających ofert na zamówienia publiczne. interfejs startowy aplikacji przedstawia rysunek 28, zaś przykładowa analizę malware „WannaCry” rysunek 32



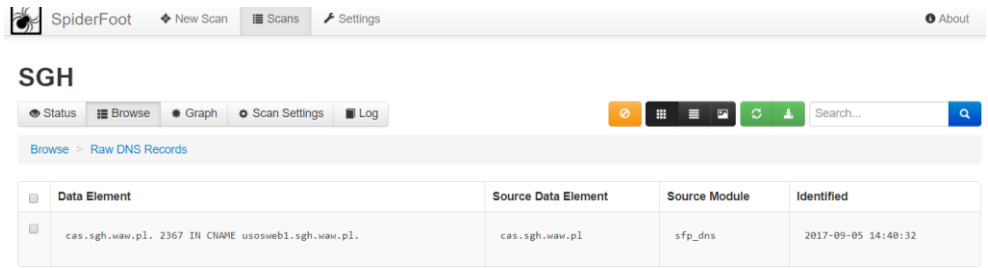
Rysunek 32. Interfejs aplikacji IRMA. Źródło: opracowanie własne.



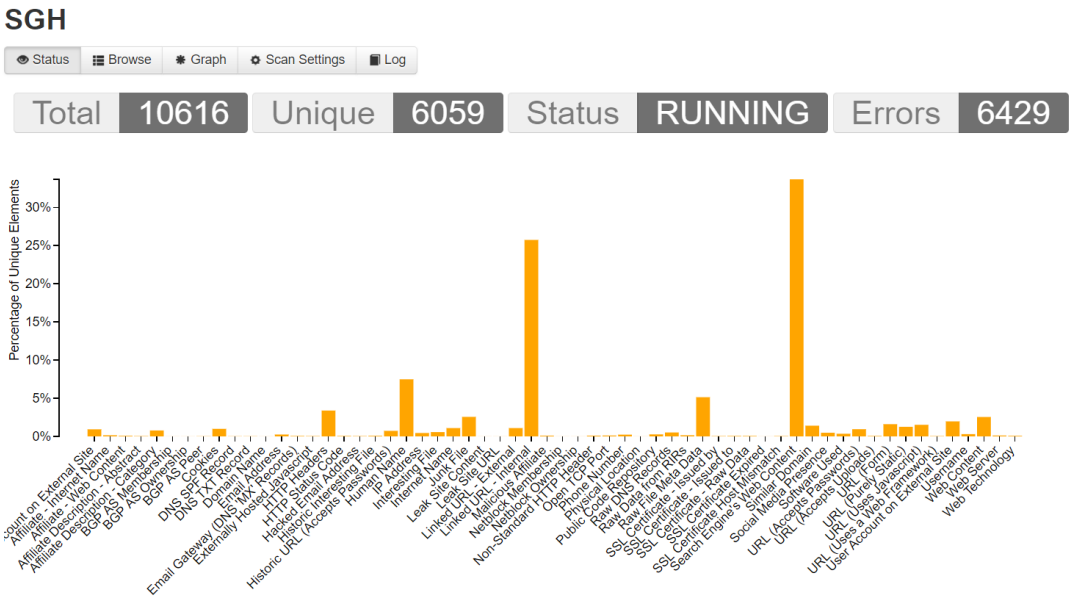
Rysunek 33. Analiza próbki malware WannaCry w aplikacji IRMA. Źródło: opracowanie własne.

IV.8 SpiderFoot

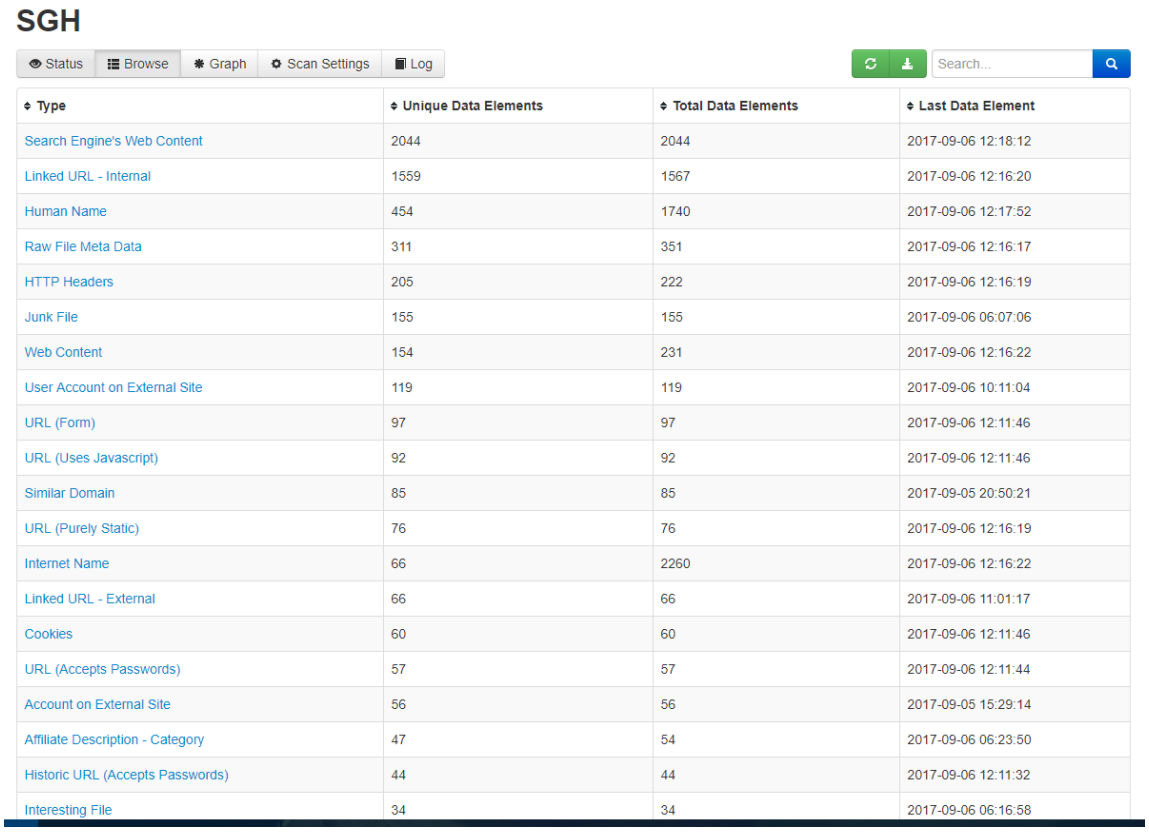
Podstawowym źródłem informacji o zagrożeniu cybernetycznym są jawne źródła dostępne w Intenecie. Jednym z narzędzi agregujących informacje z wielu źródeł jest SpiderFoot, największa jego zaleta jest pełna automatyzacja w wyszukiwaniu informacji. Dzięki tej aplikacji możemy sprawdzić reputacje źródeł ataków (domeny adresy IP, które odnaleźliśmy w dziennikach zdarzeń, czy adresy e-mailowe, z których przychodzą wiadomości phishingowe. Możemy także sprawdzić jakie dane o naszej organizacji mogą znaleźć cyberprzestępcy w otwartych źródłach informacji takich jak media społecznościowe czyli co publikują pracownicy naszej organizacji lub co publikuje się o naszej organizacji, czy jakiś nasz serwer nie jest wpisany na czarną listę przez organizacje monitorujące spam i cyberataki, czy dane opublikowane na serwerach do wymiany informacji takich jak PasteBin nie zawierają wpisów z nazwą naszej domeny, co świadczyło by o wycieku danych. Aplikacja stworzona jest w celu maksymalnej ekstrakcji informacji z kilkudziesięciu źródeł (ponad 50) takich jak SHODAN, RIPE, Whois, PasteBin, Google, SANS, Facebook, LinkedIn, Twitter, AdBlock, malcode, malwaredomainlist, SpamHaus, Tor i wielu innych. Aplikacja potrafi wyekstrahować dane z dostępnych dokumentów o aplikacjach na których były utworzone, skanerach, loginy i imiona i nazwiska, numery telefonów, technologie użyte na serwerach web i wiele innych danych. Przykładowa analiza ukazana jest na rysunkach 34, Rysunek 35 pokazuje graficzną reprezentację ilości odnalezionych informacji natomiast rysunek 36 pokazuje fragment listy informacji uzyskanych przez aplikację. Rysunek 37 pokazuje iż domene sgh.waw.pl próbowano używać przy tworzeniu wiadomości phisingowych.



Rysunek 34. SpiderFoot przykładowa analiza. Źródło: opracowanie własne.

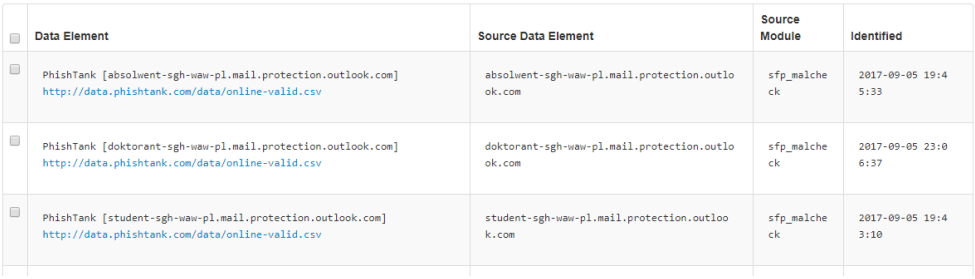


Rysunek 35. Graficzne przedstawienie danych uzyskanych przez SpiderFoot. Źródło: opracowanie własne.



Type	Unique Data Elements	Total Data Elements	Last Data Element
Search Engine's Web Content	2044	2044	2017-09-06 12:18:12
Linked URL - Internal	1559	1567	2017-09-06 12:16:20
Human Name	454	1740	2017-09-06 12:17:52
Raw File Meta Data	311	351	2017-09-06 12:16:17
HTTP Headers	205	222	2017-09-06 12:16:19
Junk File	155	155	2017-09-06 06:07:06
Web Content	154	231	2017-09-06 12:16:22
User Account on External Site	119	119	2017-09-06 10:11:04
URL (Form)	97	97	2017-09-06 12:11:46
URL (Uses Javascript)	92	92	2017-09-06 12:11:46
Similar Domain	85	85	2017-09-05 20:50:21
URL (Purely Static)	76	76	2017-09-06 12:16:19
Internet Name	66	2260	2017-09-06 12:16:22
Linked URL - External	66	66	2017-09-06 11:01:17
Cookies	60	60	2017-09-06 12:11:46
URL (Accepts Passwords)	57	57	2017-09-06 12:11:44
Account on External Site	56	56	2017-09-05 15:29:14
Affiliate Description - Category	47	54	2017-09-06 06:23:50
Historic URL (Accepts Passwords)	44	44	2017-09-06 12:11:32
Interesting File	34	34	2017-09-06 06:16:58

Rysunek 36. Dane, które udało się odnaleźć w sieci przez aplikację SpiderFoot.



Data Element	Source Data Element	Source Module	Identified
PhishTank [absolwent-sgh-waw-pl.mail.protection.outlook.com] http://data.phishtank.com/data/online-valid.csv	absolwent-sgh-waw-pl.mail.protection.outlook.com	sfp_malcheck	2017-09-05 19:45:33
PhishTank [doktorant-sgh-waw-pl.mail.protection.outlook.com] http://data.phishtank.com/data/online-valid.csv	doktorant-sgh-waw-pl.mail.protection.outlook.com	sfp_malcheck	2017-09-05 23:06:37
PhishTank [student-sgh-waw-pl.mail.protection.outlook.com] http://data.phishtank.com/data/online-valid.csv	student-sgh-waw-pl.mail.protection.outlook.com	sfp_malcheck	2017-09-05 19:43:10

Rysunek 37. Przykład użycia domeny SGH do ataku phisingowego. Źródło: opracowanie własne.

IV.9 Inne platformy do rozpoznania zagrożeń cybernetycznych

Pozostałe platformy i usługi do zbierania, analizowania, tworzenia i udostępniania informacji o zagrożeniach cybernetycznych to:

- **AbuseHelper** – open source'owy framework do odbierania i redystrybucji informacji o nadużyciach i gromadzeniu informacji o rozpoznaniu zagrożeń. dostępny na githubie https://github.com/abusesa/abusehelper.
- **AIS** – (Automated Indicator Sharing) stworzone przez Departament Bezpieczeństwa Wewnętrznego USA (DHS) wolne oprogramowanie (AIS) umożliwiające wymianę wskaźników zagrożenia cybernetycznego pomiędzy rządem federalnym USA a sektorem prywatnym https://www.dhs.gov/ais.
- **Barncat** – firma Fidelis Cybersecurity oferuje bezpłatny dostęp do swojej platformy Barncat po rejestracji. Platforma może być używana przez xespoły CERT, naukowców, dostawców usług internetowych oraz innych organizacji. Baza posiada elastyczny system konfiguracji https://www.fidelissecurity.com/resources/fidelis–barncat.
- **Bearded Avenger** testowa trzecia wersja następcy frameworku CIF https://github.com/csirtgadgets/bearded–avenger.
- **Blueliv Threat Exchange Network** – platforma pozwalająca uczestnikom dzielić się wskaźnikami zagrożeńa ze społecznością; https://community.blueliv.com.
- **Interflow** – to platforma bezpieczeństwa i wymiany informacji o zagrożeniach stworzona przez Microsoft dla specjalistów zajmujących się cyberbezpieczeństwem. Wykorzystuje rozproszoną architekturę, umożliwiającą wymianę informacji na temat bezpieczeństwa i zagrożeń wewnątrz i pomiędzy społecznościami celem wzmocnienia zbiorowego ekosystemu. Oferuje wiele opcji konfiguracyjnych, Interflow pozwala użytkownikom zdecydować, jakie tworzyć wspólnoty, jakie dane będą zasilać bazę jaki i z kim je dzielić https://technet.microsoft.com/en–us/security/dn750892.

- **Malstrom** – powstał jako repozytorium do śledzenia zagrożeń i artefaktów forensyki komputerowej, dodatkowo przechowuje reguły YARA oraz notatki do badań https://github.com/byt3smith/malstrom.

- **MANTIS** – (The Model–based Analysis of Threat Intelligence Sources) Platforma do zarządzania rozpoznaniem zagorżeń informatycznych, wspierająca wiele formatów danych takich jak STIX i Cybox. nie jest zaprojektowana do dużych rozwiązań http://django–mantis.readthedocs.io/en/latest/.

- **Megatron** – jest narzędziem realizowanym przez szwedzki CERT–SE, zbierającym i analizującym, szkodliwe adresy IP, może być także używany do obliczania statystyk, konwersji i analizy logów oraz zagrożeń i incydentów https://github.com/cert–se/megatron–java.

- **MineMeld** – Rozszerzalna platforma przetwarzania danych o rozpoznaniu zagrożeń stworzona przez Palo Alto Networks. Może być używana do manipulowania listami wskaźników i transformacji i / lub agregować je do spożycia przez infrastrukturę egzekwowania osoby trzeciej https://github.com/PaloAltoNetworks/minemeld/wiki.

- **OpenIOC** – to otwarty framework służący dzieleniu się rozpoznaniem zagrożeń. przeznaczony jest do wymiany informacji o zagrożeniach, zarówno wewnętrznych, jak i zewnętrznych w formie możliwej do automatycznej wymiany http://www.openioc.org/.

- **OpenTAXII** – to zralizowana w Pythonie implementacja TAXII, dostarczająca bogaty zestaw funkcji i przyjazny interfejs API dla różnych zewnętrznych aplikacji.

- **Ostrica** – (Open Source Threat Intelligence Collector) opensource'owy framework zorientowany na rozbudowę za pomocą wtyczek służacy do zbierania i wizualizacji za pomocą grafów informacji o rozpoznaniu zagrożeń informatycznych https://github.com/Ptr32Void/OSTrICa.

- **OpenTPX** – (Threat Partner eXchange) to opensource'owy system na który składają się format wymiany danych oraz narzędzia służące do automatycznej wymiany informacji o zagrożeniach i danych o bezpieczeństwie sieciowym. Format wymiany danych pomiędzy połączonymi systemami opiera się na lekkim tekstowym formacie JSON https://github.com/Lookingglass/opentpx.

- **PassiveTotal** – platforma oferowana przez firmę RiskIQ służąca do analizy zagrożeń, zapewniającą analitykom jak najwięcej danych, w celu zapobiegania atakom przed ich wystąpieniem. platforma oferuje interfejs API celem integracji z innymi systemami https://www.passivetotal.org/.

- **Recorded Future** - automatycznie łączy rozpoznanie zagrożeń ze źródeł otwartych, zamkniętych, a źródła technicznych w ramach jednego rozwiązania. Ich technologia wykorzystuje przetwarzanie języka naturalnego (NLP) i uczenia maszynowego do

dostarczenia tej informacji o zagrożeniach w czasie rzeczywistym – czyniąc Recorded Future popularnym wyborem dla zespołów IT bezpieczeństwa.

- **Scumblr** - to aplikacja internetowa, która umożliwia dokonywanie okresowych synchronizuje źródeł danych (takich jak repozytorium GitHub i adresów URL) i wykonywania analiz (takich jak analizy statycznej, kontroli dynamicznych i kolekcji metadanych) na określonych rezultatów. Scumblr pomaga usprawnić ochronę proaktywną przez inteligentną ramach automatyki pomóc identyfikować, śledzić i rozwiązywać problemy z bezpieczeństwem szybciej.

- **Soltra EDGE** - Podstawowa wersja Soltra EDGE jest dostępna za darmo, wsparcie jest realizowane na zasadzie społecznościowej, domyślnieobsługuje standardy STIX i TAXII.

- **STAXX (Anomali)** - pozwala na swobodny i łatwy sposób pobierania danych wysyłanych w postaci STIX / TAXII. Wystarczy pobrać klienta STAXX, i skonfigurować źródło a STAXX zajmie się resztą.

- **stoQ** - to framework, który pozwala analitycy Cyber organizować i automatyzacji powtarzalnych zadań, opartych na danych. Posiada wtyczki do wielu innych systemów interakcji z. Jeden przypadek użycia jest wydobycie IOCs z dokumentów, których przykładem jest pokazany tutaj , ale może być również używany do deobfuscationg i dekodowania treści i automatyczne skanowanie z YARA, na przykład.

- **TARDIS** – (Threat Analysis, Reconnaissance, and Data Intelligence System) jest platformą na licencji Open Source służącą do przeprowadzania analiz historycznych za pomocą sygnatur ataków.

- **ThreatCrowd** - to system do wyszukiwania i badania artefaktów związanych z zagrożeniami sieciowymi.

- **ThreatExchange** – system stworzony przez Facebook by organizacje wspólpracujące mogły udostępniać dane o zagrożeniach za pomocą wygodnego, uporządkowanego i łatwego w obsłudze interfejsu API, który zapewnia prywatność, i umożliwia dzielenie się informacjami tylko z pożądanymi grupami . Projekt jest jeszcze w fazie beta . Kod źródłowy można pobrać z GitHub.

- **X–Force Exchange (XFE) -** stworzona przez IBM XFE darmowa usługa typu SaaS, którą można użyć do wyszukiwania informacji o zagrożeniach , zbierania swoich spostrzeżeń i dziellenia się swoimi spostrzeżeniami z innymi członkami społeczności XFE.

IV.10 Instalacja, uruchomienie i działanie środowiska służącego rozpoznaniu zagrożeń informatycznych

Poszczególne aplikacje uruchomione są w środowisku wirtualnym Hyper-V na dwu-serwerowym klastrze. Przyjęto zasadę, iż każda aplikacja uruchomiona jest na osobnej maszynie, eliminuje to problemy z niezgodnością wersji bibliotek szczególnie przy aktualizacji poszczególnych aplikacji, początkowo środowisko było uruchomione w kontenerach Dockera jednakże nie było ono w pełni stabilne. Sandbox Cuckoo uruchomiony jest na oddzielnej fizycznej maszynie z racji konieczności kontrolowanie przez niego maszyn uruchomionych w środowisku wirtualnym KVM. Wszystkie aplikacje są bezpłatne, udostępnione na licencji Open Source, Większość (po za LOKI) posiada przyjazny interfejs webowy. Na środowisko składają się m.in.:

- **Cuckoo sandbox**– łatwo obsługiwany dzięki interfejsowi webowemu, i łatwo rozbudowywany dzięki interfejsowi API do współpracy z innymi aplikacjami, sandbox posiada kilka możliwości łączności z siecią Internet – brak połaczenia, emulator sieci INETSIM, tunel do sieci TOR, tunel VPN oraz łącze bezpośrednie (dirty line) zrealizowane za pomocą modemu LTE. Mnogość połączeń zapewnia badanie malware w szerszym spektrum, dzięki takiemu rozwiązaniu można zapewnić szczególne zachowanie bezpieczeństwa tak by malware nie mogło przeniknąć do sieci produkcyjnej organizacji. Sandbox komunikuje się z aplikacjami CRITS, MISP, Moloch (system analizy ruchu sieciowego).

- **MISP –** główne repozytorium informacji o rozpoznaniu zagrożeń cybernetycznych. Informacja o zagrożeniach z zewnątrz jest zasilana przez trzy instytucje CIRCL, Botvrij.eu oraz inThreat, spływające raporty o zagrożeniach przekazywane przez CERT.pl, RCB i Wydział Bezpieczeństwa Cyfrowego MS a także bieżące analizy w sandboxie i aplikacji CRITS. Wskaźniki kompromitacji i inne informacje o zagrożeniach pobierane jest przez aplikacje użytkowane w organizacji takie jak: Cuckoo, IntelMQ, Yeti, LOKI.

- **CRITS –** narzędzie do analizy próbek malware z połączeniem do kilkudziesięciu aplikacji (analizujących ruch sieciowy, zawartość plików, makra nagłówki) i serwisów (antywirusów, baz o zagrożeniach, skompromitowanych domenach lub adresach IP)

- **MALCOM** – narzędzie do badania głównie adresów IP i domen ujawnionych w kodzie malware, lub stwierdzenia czy serwisy instytucji współpracujących nie zostały skompromitowane.

- **SpiderFoot** - narzędzie do szybkiego wyszukiwania informacji Dzięki tej aplikacji możemy sprawdzić reputacje źródeł ataków (domeny adresy IP, które odnaleźliśmy w dziennikach zdarzeń, czy adresy e-mailowe, z których przychodzą wiadomości phishingowe. sprawdzana jest także reputacja

- **IntelMQ** – system szybko potrafi odnaleźć czy z danej domeny czy adresu IP nie był przeprowadzany już inny atak, czy dany adres nie jest już na „czarnej liście”.

- **LOKI** – narzędzie używane do skanowania stacji roboczych pod kątem występowania wskaźników kompromitacji publikowanych np. w alertach CERT.pl lub RCB. LOKI pobiera dane o wskaźnikach kompromitacji z lokalnego serwera MISP zasilanego przez bieżące analizy przychodzącego malware jak i różne instytucje i serwisy dlatego dużo szybciej niż antywirus może odnaleźć trwający atak lub występowanie świeżego malware

- **IRMA** – środowisko stworzone w celu dodatkowegobadania dokumentów np. przesyłanych na ogłoszenia przetargowe w celu dokładniejszej analizy na kilku silnikach i bazach antywirusowych. środowisko współpracuje z sandboksem Cuckoo.

- **AlienVault OSSIM** – darmowy system SIEM użytkowany w instytucji autora i jednostkach podległych. posiada skaner wykrywania podatności celem aktywnego skanowanie urxądzeń sieciowych i stałego monitorowanie zagrożeń (OpenVAS), aktywne i pasywne wykrywanie urządzeń w sieci (OCS-NG), IDS sieci i hosta, monitorowanie integralności plików (Snort, Suricata, OSSEC), analizę przepływu sieciowego, normalizacja logów oraz co najważniejsze, zarządzanie logami, korelacja zdarzeń SIEM, analiza i raportowanie.

ZAKOŃCZENIE

Niniejsza praca dyplomowa przedstawia jedną z propozycji stworzenia platformy do analizy gromadzenia i wymiany informacji o cyber-zagrożeniach. Jednym z głównych celów było stworzenie środowiska całkowicie opartego o oprogramowanie udostępniane na otwartej licencji czyli bezpłatne. Działające środowisko, utworzone przez autora opracowania, od blisko roku pomaga przy analizie zagrożeń w państwowej instytucji i informowaniu współpracujących podmiotów o zauważonych zagrożeniach. Przyjąć zatem można, iż teza o budowie działającego środowiska opartego o Open Source jest zasadna. Jednakże pamiętać należy, iż dynamika zmian w dziedzinie cyberbezpieczeństwa wymaga śledzenia nowych rozwiązań oraz rekonfiguracji czy dołożenia nowych elementów do istniejącego już systemu.

Bibliografia

1. ActiveResponse.org, 2016. *The Diamond Model.* [Online]
   Protokół dostępu: http://www.activeresponse.org/the-diamond-model/
   [Dostepne: 13 marzec 2017].

2. Alienvault, 2012. *About Open Threat Exchange (OTX).* [Online]
   Protokół dostępu: https://www.alienvault.com/documentation/otx/about-otx.htm
   [Dostepne: 18 marzec 2017].

3. Anty-Virus-Comparatives, 2016. *Malware emoval Test.* [Online]
   Protokół dostępu: https://www.av-comparatives.org/wp-content/uploads/2016/10/avc_rem_2016_en.pdf
   [Dostepne: 13 luty 2017].

4. AV-TEST, 2016. *Security Rreport 2015/2016.* [Online]
   Protokół dostępu: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2015-2016.pdf
   [Dostepne: 13 luty 2017].

5. AV-TEST, 2017. *Malware Statistics.* [Online]
   Protokół dostępu: https://www.av-test.org/en/statistics/malware/
   [Dostepne: 8 luty 2017].

6. Bank of England, 2016a. *An Introduction to Cyber Threat Modelling v2.0*, Londyn: BANK of England.

7. Bank of England, 2016b. *CBEST Implementation Guide,* Londyn: Bank of England.

8. Bank of England, 2016c. *CBEST Intelligence-Led Testing* , Londyn: Bank of England.

9. Bejtlich, R., 2010. *What Is APT and What Does It Want?.* [Online]
   Protokół dostępu: https://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html
   [Dostepne: 11 marzec 2017].

10. Bianco, D., 2014. *The Pyramid of Pain.* [Online]
    Protokół dostępu: http://detect-respond.blogspot.co.uk/2013/03/the-pyramid-of-pain.html
    [Dostepne: 22 luty 2017].

11. Bigo, Ł., 2006. *Prawo Moore'a - było, jest, nie będzie.* [Online]
Protokół dostępu:
http://www.pcworld.pl/news/Prawo.Moore.a.bylo.jest.nie.bedzie,92154.html
[Dostepne: 21 luty 2017].

12. Bińkowski, K., 2016. Automatyczna analiza złośliwego oprogramowania. *IT w Administracji*, Sierpień, pp. 52-54.

13. Caltagirone, S., Pendergast, A. & Betz, C., 2013. *The Diamond Model of Intrusion Analysis,* Hanover, MD: Center for Cyber Threat Intelligence and Threat Research.

14. Casey, E., 2001. *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet.* 3 ed. Baltimore: Academic Press.

15. Chuvakin, A., 2014. *On Threat Intelligence Management Platforms.* [Online]
Protokół dostępu: http://blogs.gartner.com/anton-chuvakin/2014/03/31/on-threat-intelligence-management-platforms/
[Dostepne: 2 marzec 2017].

16. CIRCL, 2016b. *Traffic Light Protocol (TLP) - Classification and Sharing of Sensitive Information.* [Online]
Protokół dostępu: https://www.circl.lu/pub/traffic-light-protocol/
[Dostepne: 2 wrzesień 2017].

17. CIRCL, 2016. *Malware Information Sharing Platform (MISP) - A Threat Sharing Platform.* [Online]
Protokół dostępu: https://www.circl.lu/services/misp-malware-information-sharing-platform/
[Dostepne: 3 wrzesień 2017].

18. CrySyS Lab, 2012. *sKyWIper (a.k.a. Flame a.k.a. Flamer):,* Budapest: Budapest University of Technology and Economics.

19. CSIRT Gadgets Foundation, 2015. *Collective Intelligence Framework.* [Online]
Protokół dostępu: http://csirtgadgets.org/
[Dostepne: 18 marzec 2017].

20. Cuckoo Fundation, 2017. *Automated Malware Analysis.* [Online]
Protokół dostępu: https://cuckoosandbox.org/
[Dostepne: 16 luty 2017].

21. Cyberdefence 24, Andrzej Kozłowski, 2016. *Szczyt NATO w Warszawie – konsekwencje dla polityki cyberbezpieczeństwa.* [Online]
Protokół dostępu: http://www.cyberdefence24.pl/406632,szczyt-nato-w-warszawie-konsekwencje-dla-polityki-cyberbezpieczenstwa
[Dostepne: 21 luty 2017].

22. Danyliw, R., Meijer, J. & Demchenko, Y., 2007. *The Incident Object Description Exchange Format.* [Online]
Protokół dostępu: https://www.ietf.org/rfc/rfc5070.txt
[Dostepne: 17 marzec 2017].

23. Data, G., 2017. *Cuckoo.* [Online]
Protokół dostępu: https://github.com/krishah/cuckoo/blob/master/install.sh

24. DHS, 2016. *DHS "Open for Business" to Receive Cyber Threat Indicators at Machine Spee.* [Online]
Protokół dostępu: https://www.dhs.gov/blog/2016/03/17/dhs-open-business-receive-cyber-threat-indicators-machine-speed
[Dostepne: 19 luty 2017].

25. Elisan, C. C., 2015. *Advanced Malware Analysis.* 1 ed. New York: McGraw-Hill.

26. ENISA, 2014. *ENISA Threat Landscape 2014,* Heraklion, Grecja: European Union Agency for Network and Information Security .

27. ENISA, 2017. *certtools/intelmq.* [Online]
Protokół dostępu: https://github.com/certtools/intelmq
[Dostepne: 2 wrzesień 2017].

28. ENISA, 2017. *Incident Handling Automation.* [Online]
Protokół dostępu: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[Dostepne: 2 wrzesień 2017].

29. EY, 2015. *Crreating trust in the digital world,* s.l.: EYGM.

30. Friedman, J. & Bouchard, M., 2015. *Definitive Guide to Cyber Threat Intelligence.* 1 ed. Annapolis: Cyberedge Press.

31. Gartner, 2014. *Threat intelligence what is it, and How Can it Protect You from Today's Advanced Cyber-Attack,* Broomfield: Webroot.

32. Goodman, M., 2016. *Zbordnie przyszłości.* 1 ed. Warszawa: Helion.

33. Hammel, M., 2014. *Understanding Online Threats with ThreatData.* [Online]
Protokół dostępu: https://www.facebook.com/notes/protect-the-graph/understanding-online-threats-with-threatdata/1438165199756960/
[Dostepne: 2 marzec 2017].

34. Herjavec, Steve Morgan, 2016. *Hackerpocalypse: A Cybercrime Revelation.* [Online]
Protokół dostępu: https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report#top
[Dostepne: 21 luty 2017].

35. Hutchins, E. M., Cloppert, M. & Amin, R., 2011. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,* s.l.: Lockheed Martin.

36. IMPERVA, 2012. *Hacker Intelligence Initiative, Monthly Trend Report #14.* [Online] Protokół dostępu: https://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf [Dostepne: 13 luty 2017].

37. INSA, 2015. *TACTICAL CYBER INTELLIGENCE,* Arlington: INTELLIGENCE AND NATIONAL SECURITY ALLIANCE.

38. inThreat, 2017. *Tthreat Intelligence.* [Online] Protokół dostępu: https://inthreat.com/threatintelligence [Dostepne: 2 wrzesień 2017].

39. Janusz, A., 2015. *Analiza malware w praktyce – procedury i narzędzia.* [Online] Protokół dostępu: https://sekurak.pl/analiza-malware-w-praktyce-procedury-i-narzedzia/ [Dostepne: 18 luty 2017].

40. Kaspersky, Lab, 2013. *Kaspersky Daily blog.* [Online] Protokół dostępu: https://plblog.kaspersky.com/robak-morris-konczy-25-lat/669/ [Dostepne: 11 luty 2017].

41. Konrad Rieck, P. T. C. W. i. H., 2011. Automatic Analysis of Malware Behavior. *The Journal of Computer Security,* Issue 19.

42. Kruegel, C., 2015. *Labs Report at RSA: Evasive Malware's Gone Mainstream.* [Online] Protokół dostępu: http://labs.lastline.com/evasive-malware-gone-mainstream [Dostepne: 12 luty 2017].

43. Krugel, C., 2015. *Labs Report at RSA: Evasive Malware's Gone Mainstream.* [Online] Protokół dostępu: http://labs.lastline.com/evasive-malware-gone-mainstream [Dostepne: 12 luty 2017].

44. Lawson, C. & McMillan, R., 2014. *Technology Overview for Threat Intelligence Platforms,* s.l.: Gartner.

45. Lehtinen, R., Russell, D. & Gangemi, G. T., 2007. *Podstawy ochrony komputerów.* Warszawa: Helion.

46. Liska, A., 2015. *Building an Intelligence-led Security Program.* Waltham: Syngress.

47. Luttgens, J., Pepe, M. i Mandia, K., 2016. *Incydenty bezpieczeństwa.* 3 red. Warszawa: Helion.

48. MacGregor, R., 2015. *Diamonds or chains.* [Online]
Protokół dostępu: http://pwc.blogs.com/cyber_security_updates/2015/05/diamonds-or-chains.html#_ftn2
[Dostepne: 13 marzec 2017].

49. Marks, P., 2011. Dot-dash-diss: The gentleman hacker's 1903 lulz. *New Scientist*, 24 12, pp. https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/.

50. McAfee, Vincent Weafer, 2016. *When It Comes To Cyberthreat Intelligence, Sharing Is Caring.* [Online]
Protokół dostępu:
https://www.google.pl/search?q=t%C5%82umacz&oq=tluma&aqs=chrome.1.69i57j0j69i59l2j0l2.3224j0j9&sourceid=chrome&ie=UTF-8
[Dostepne: 19 luty 2017].

51. McElroy, D. & Williams, C., 2012. Flame: world's most complex computer virus exposed. *The Telegraph*, 28 maj.

52. McMillan, R., 2010. Siemens: Stuxnet worm hit industrial systems. *Computerworld*, 14 wrzesień.

53. MEDIANT, 2013. *The OpenIOC Framework.* [Online]
Protokół dostępu: http://www.openioc.org/
[Dostepne: 17 marzec 2017].

54. MITRE Corporation, 2014a. *Cyber Observable eXpression (CybOX™).* [Online]
Protokół dostępu: https://cyboxproject.github.io/
[Dostepne: 17 marzec 2017].

55. MITRE Corporation, 2014c. *Trusted Automated eXchange of Indicator Information (TAXII™).* [Online]
Protokół dostępu: https://taxiiproject.github.io/
[Dostepne: 17 marzec 2017].

56. MITRE Corporation, 2014d. *Malware Attribute Enumeration and Characterization (MAEC™).* [Online]
Protokół dostępu: https://maecproject.github.io/
[Dostepne: 17 marzec 2017].

57. MITRE Corportion, 2014b. *Structured Threat Information eXpression (STIX™).* [Online]

Protokół dostępu: https://stixproject.github.io/
[Dostepne: 17 marzec 2017].

58. MITRE, 2008. *Common Attack Pattern Enumeration and Classification.* [Online] Protokół dostępu: https://capec.mitre.org/
[Dostepne: 22 marzec 2017].

59. MWR Infosecurity, 2015. *Threat Intelligence: Collecting, Analysing, Evaluating,* Londyn: MWR InfoSecurity .

60. National Cyber Security Centre, 2015. *An introduction to threat intelligence,* Londyn: CERT-UK Publication.

61. NATO Communications and Information Agency, 2015. *Malware Information,* Bruksela: NCI Agency.

62. OASIS, 2016. *OASIS Cyber Threat Intelligence TC Wiki.* [Online] Protokół dostępu: https://wiki.oasis-open.org/cti/Products
[Dostepne: 19 marzec 2017].

63. Oktavianto, D. & Muhardianto, I., 2013. *Cuckoo Malware Analysis.* I ed. Birmingham: Packt Publishing.

64. OPTIV, 2014. *Improving Reliability of Sandbox Results.* [Online] Protokół dostępu: https://www.optiv.com/blog/improving-reliability-of-sandbox-results
[Dostepne: 17 luty 2017].

65. Parnell, B.-A., 2011. *Cyber crime now bigger than the drugs trade.* [Online] Protokół dostępu: http://www.theregister.co.uk/2011/09/07/cost_is_more_than_some_drug_trafficking/
[Dostepne: 21 luty 2014].

66. PwC Polska, 2017. *Ochrona biznesu,* Warszawa: Price Waterhouse i Coopers & Lybrand.

67. Roth, F., 2015. *LOKI Free IOC Scanner.* [Online] Protokół dostępu: https://www.bsk-consulting.de/loki-free-ioc-scanner/
[Dostepne: 2 wrzesień 2017].

68. Roth, F., 2017. *Loki - Simple IOC and Incident Response Scanner.* [Online] Protokół dostępu: https://github.com/Neo23x0/Loki
[Dostepne: 2 wrzesień 2017].

69. Rutkowska, J., 2006. *Introducing Stealth Malware Taxonomy.* Singapur, COSEINC Advanced Malware Labs.

70. Sanger, D. e., 2012. *Obama Order Sped Up Wave of Cyberattacks Against Iran.* [Online]
Protokół dostępu: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all
[Dostepne: 30 sierpień 2017].

71. SANS Institute , 2013. *Tools and Standards for Cyber Threat Intelligence,* s.l.: SAns Institute.

72. SecureWorks, 2016. *Breaking the Kill Chain,* s.l.: SecureWorks.

73. Sikorski, M. & Honig, A., 2013. *PRACTICAL MALWARE ANALYSIS.* San Francisco: No Strach Press.

74. Simonite, T., 2012. *MIT Technology Review.* [Online]
Protokół dostępu: https://www.technologyreview.com/s/428166/the-antivirus-era-is-over/
[Dostepne: 13 luty 2017].

75. Smith, J., 2016. *Cyber threat intelligence sharing – understanding the technology.* [Online]
Protokół dostępu: https://blog.apnic.net/2016/06/24/cyber-threat-intelligence-sharing-understanding-the-technology/
[Dostepne: 19 marzec 2017].

76. Smol, W., 2013. *Sekurak.pl.* [Online]
Protokół dostępu: https://sekurak.pl/w-jaki-sposob-dzialaja-programy-antywirusowe/
[Dostepne: 12 luty 2017].

77. Soltra, 2015. *Hail a TAXII.* [Online]
Protokół dostępu: http://hailataxii.com/
[Dostepne: 19 marzec 2017].

78. Spengler, B., 2017. *Cuckoo Modified.* [Online]
Protokół dostępu: https://github.com/spender-sandbox/cuckoo-modified
[Dostepne: 17 luty 2017].

79. Symantec, 2011. *W32.Duqu The precursor to the next Stuxnet.* [Online]
Protokół dostępu: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
[Dostepne: 30 sierpień 2017].

80. The Economist,, 2015. *Sharing is caring.* [Online]
Protokół dostępu: http://www.economist.com/news/united-states/21639523-barack-obama-wants-congress-bolster-cyber-security-sharing-caring
[Dostepne: 19 luty 2017].

81. The Guardian, Ian Traynor , 2007. *Russia accused of unleashing cyberwar to disable Estonia.* [Online]
Protokół dostępu: https://www.theguardian.com/world/2007/may/17/topstories3.russia
[Dostepne: 2017 luty 21].

82. The New Yor Times, William Safire, 2004. *The Farewall Dosier.* [Online]
Protokół dostępu: http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?_r=1
[Dostepne: 19 luty 2017].

83. Trinius, P., Willems, C., Holz, T. & Rieck, K., 2009. *A Malware Instruction Set for Behavior-Based Analysis*, Mannheim: University of Mannheim.

84. U. S. Government Publishing Office, 1996. *IC21 THE INTELLIGENCE COMMUNITY IN THE 21ST CENTURY - STAFF STUDY PERMANENT SELECT COMMITTEE ON INTELLIGENCE.* [Online]
Protokół dostępu: https://www.gpo.gov/fdsys/pkg/GPO-IC21; https://www.gpo.gov/fdsys/pkg/GPO-IC21/html/figure1a.gif
[Dostepne: 25 marzec 2017].

85. US-CERT, 2014. *Information Sharing Specifications for Cybersecurity.* [Online]
Protokół dostępu: https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity
[Dostepne: 17 marzec 2017].

86. US-CERT, 2017. *Traffic Light Protocol (TLP) Definitions and Usage.* [Online]
Protokół dostępu: https://www.us-cert.gov/tlp
[Dostepne: 18 luty 2017].

87. Verizon, 2016. *2016 Data Breach Ivestigations Report ,* s.l.: Verizon Enterprise.

88. Virustotal, 2013. *YARA in a nutshell.* [Online]
Protokół dostępu: http://virustotal.github.io/yara/
[Dostepne: 18 marzec 2017].

89. VirusTotal, 2017. *About VirusTotal.* [Online]
Protokół dostępu: https://www.virustotal.com/pl/about/#avtesting
[Dostepne: 13 luty 2017].

90. WEBROOT, 2016. *2015 Threat brief.* [Online]
Protokół dostępu:

https://www.webroot.com/shared/pdf/Webroot_2015_Threat_Brief.pdf
[Dostepne: 12 luty 2017].

91. Wikipedia Fundation, 2017. *Złośliwe oprogramowanie.* [Online]
Protokół dostępu:
https://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie
[Dostepne: 11 luty 2017].

92. Worl Wide Web Consortium, 2017. *Internet Users.* [Online]
Protokół dostępu: http://www.internetlivestats.com/internet-users/
[Dostepne: 11 marzec 2017].

SPIS TABEL

SPIS RYSUNKÓW