Jerzy Surma[1]

Wybrane problemy budowy systemów rozpoznawania zagrożeń w cyberprzestrzeni

1. Wstęp

Ryzyko naruszenia bezpieczeństwa systemów informatycznych jest obecnie podstawowym ryzykiem operacyjnym w działalności opartej na technologiach cyfrowych. Z tego względu zarówno przedsiębiorstwa prywatne, jak i instytucje sektora publicznego ponoszą coraz większe koszty w zakresie zapewnienia odpowiedniej ochrony przed atakami w cyberprzestrzeni. Obecnie stosowane rozwiązania koncentrują się na ochronie przed atakami w momencie, kiedy nastąpiło już bezpośrednie działanie cyberprzestępcy. Praktyka pokazuje ograniczoną skuteczność tego typu podejścia i potrzebę systemowych rozwiązań proaktywnych, pozwalających antycypować działania przestępcze i skutecznie im zapobiegać. Na rysunku 1 przedstawiono zarys cyklu życia zaawansowanego ataku hackerskiego typu APT (ang. *Advanced Persistent Threat Attack*), który można podzielić na dwie fazy: przygotowanie ataku („Rozpoznanie celu ataku" oraz „Opracowanie uzbrojenia") oraz realizacja ataku (od „Dostarczenie uzbrojenia do środowiska docelowego" do „Realizacja ataku")[2]. Przygotowanie ataku typu APT to zwykle wielomiesięczna aktywność hakera, która powinna być przedmiotem rozpoznania i analiz. W tym nurcie w ostatnich latach podjęto wiele badań naukowych i prób budowania systemów informatycznych rozpoznania zagrożeń w cyberprzestrzeni (ang. *Cyber Threat Intelligence*), które są w stanie monitorować i analizować różnorodne źródła informacji z Internetu tak, aby identyfikować zagrożenia związane z cyberprzestępczością.

[1] Szkoła Główna Handlowa w Warszawie, Instytut Informatyki i Gospodarki Cyfrowej.

[2] Szczegółowy opis całego cyklu jest dostępny na: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (dostęp: 7.04.2018).

Rysunek 1. Cykl życia ataku cybernetycznego typu APT

Źródło: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pd (dostęp: 7.04.2018).

2. Klasyczne podejście do obrony przed atakami APT

Klasyczne podejście od obrony przed atakami APT dotyczy reaktywnego podejścia dopiero w fazie realizacji ataku. Jest to strategia „monitoruj i reaguj", która jest realizowana według następującego schematu[3]:

1) kolekcjonowanie opisów incydentów, sygnatur ataków, wskaźników zagrożeń itp.;
2) wykorzystanie danych zebranych w kroku 1. do:
   – zasilania systemów typu: *intrusion detection / prevention* (IDS/IPS), zaawansowanych zapór ogniowych, oprogramowania antywirusowego,
   – zaawansowanej analizy w celu ustalenia alertów i reguł wykorzystywanych przez systemy SIEM (ang. *Security Information and Event Management*), używanych w ramach SOC (ang. *Security Operation Center*);
3) zespół SOC, na podstawie analizy alertów otrzymanych z SIEM, dokonuje wyboru krytycznych incydentów, które są przekazywane do zespołu IR (ang. *Incident Response*) w celu pogłębionego rozpoznania i określenia planu reakcji;
4) dla wybranych incydentów zespół IR wykonuje działania naprawcze, „oczyszczenie" zainfekowanych systemów i zapobieżenie powtórzeniu się podobnych ataków.

Strategia „monitoruj i reaguj" zawiera kilka istotnych niedogodności; są to:

- trudność w analizie dużej liczby fałszywych alarmów (ang. *false positive*)[4],
- długi czas analizy nieznanego wcześniej zagrożenia w sytuacji potrzeby relatywnie szybkiej reakcji,
- ograniczona wiedza na poziomie zarządczym, co do potencjalnych inwestycji w kontekście antycypowanych zagrożeń cybernetycznych.

[3] J. Friedman, M. Bouchard, *Definitive Guide to Cyber Threat Intelligence*, Cyber Edge Press, Annapolis 2015.

[4] Zaklasyfikowanie zdarzenia nieistotnego jako zagrożenie.

3. Rola systemów rozpoznawania zagrożeń w cyberprzestrzeni

W kontekście problemów związanych z realizacją podejścia „monitoruj i reaguj" pojawiła się potrzeba prowadzenia działań wywiadowczych w cyberprzestrzeni. Systemy rozpoznawania zagrożeń w cyberprzestrzeni zbierają informacje o grupach przestępczych, ich motywacjach, intencjach oraz metodach działania. Informacja ta jest następnie analizowana oraz rozpowszechniana w taki sposób, aby zapewnić bezpieczne funkcjonowanie krytycznych zasobów teleinformatycznych oraz osób podlegających ochronie. Systemy tej klasy są w stanie, niejednokrotnie w czasie rzeczywistym, monitorować i analizować różnorodne źródła informacji z Internetu, aby identyfikować zagrożenia związane z cyberprzestępczością[5].

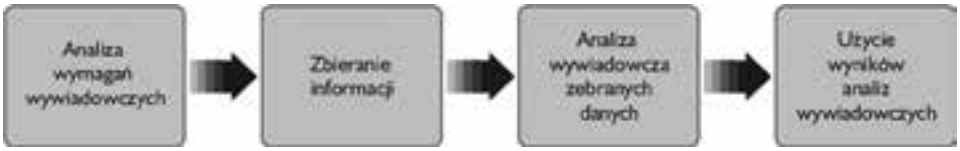
Korzyści związane z wykorzystaniem systemów rozpoznawania zagrożeń w cyberprzestrzeni są następujące:

- ograniczenie fałszywych alarmów poprzez eliminację nieistotnych incydentów,
- nadanie priorytetów do instalacji patch'y dla niebezpiecznych zagrożeń,
- ustalenie przepływu właściwych danych do SIEM, co umożliwia skuteczną korelację danych,
- identyfikacja zagrożeń i w tym kontekście możliwość zapobiegania atakom,
- określenie priorytetów alertów dla zespołu SOC, co umożliwia koncentrację na rzeczywistych zagrożeniach,
- dogłębne zrozumienie intencji i motywów działania grup przestępczych,
- umożliwienie decydentom zrozumienia aktualnych zagrożeń i w tym kontekście poprawną alokację budżetów i pracowników dla ochrony krytycznych zasobów,
- poprawne zarządzanie ryzykiem operacyjnym poprzez antycypację prawdopodobnych zagrożeń i komunikację ich do zarządu w celu podjęcia działań zapobiegawczych.

Funkcjonowanie systemów rozpoznawania zagrożeń w cyberprzestrzeni oparte jest zwykle na czterofazowym procesie pozyskiwania i analizy informacji wywiadowczych (rysunek 2).

I. Analiza wymagań wywiadowczych na podstawie poprawnej identyfikacji zagrożeń: sponsorzy, wykonawcy, motywacje, metody, techniki, podatności systemów na zagrożenia itp. Określenie źródeł pozyskiwanych danych. Nadanie priorytetów oraz eliminacja trywialnych źródeł danych.

[5] M.S. Collins, *Network Security through Data Analysis Building Situational Awareness*, O'Reilly Media, Austin 2014.



Rysunek 2. Proces pozyskiwania i analizy informacji wywiadowczych

Źródło: opracowanie własne na podstawie: J. Friedman, M. Bouchard, *Definitive Guide to Cyber Threat Intelligence*, Cyber Edge Press, Annapolis 2015.

II. Zbieranie danych, które obejmuje:
   - identyfikację zagrożeń (ang. *threat indicator*), wskazujących na potencjalne ataki czy zagrożenia; przykładami takich wskazań mogą być sygnatury plików, adresy IP związane z atakami;
   - dane o zagrożeniach (ang. *threat data feeds*), które uzupełniają wskazania zagrożeń o określony kontekst oraz umożliwiają korelowanie i analizowanie zagrożeń; dane tego typu umożliwiają identyfikację wzorców zachowań związanych z atakami;
   - strategiczne informacje wywiadowcze, tzn. informacje o osobach i organizacjach stanowiących zagrożenie oraz o potencjalnych działaniach przestępczych z ich strony;
   - monitorowanie podziemia, czyli zbieranie danych z tzw. darknet, obejmującego m.in. przestępcze fora internetowe w sieci Tor.

III. Analiza zebranych danych jest prowadzona na dwóch poziomach:
   - analiza automatyczna – wykorzystanie zaawansowanych metod analitycznych (patrz punkt 4).
   - analiza ekspercka – wykorzystanie wiedzy eksperckiej do pogłębionej analizy wybranych wyników, otrzymanych z automatycznej analizy danych.

IV. Użycie wyników analiz na poziomie:
   - operacyjnym – umożliwia zespołowi SOC podejmowanie działań zapobiegawczych w zakresie antycypowanych zagrożeń, rozpoznanych ataków APT, pogłębionej informatyki śledczej itp.,
   - strategicznym – odpowiednie podsumowanie umożliwia menedżerom racjonalne zarządzanie ryzykiem oraz podejmowanie decyzji inwestycyjnych w kontekście antycypowanych zagrożeń cybernetycznych.

4. Wykorzystanie metod eksploracji danych

Systemy rozpoznawania zagrożeń w cyberprzestrzeni analizują zbierane dane z wykorzystaniem metod eksploracji danych (ang. *Data Mining*), gdzie dane są pozyskiwanych z publicznie dostępnych źródeł (ang. *Open Source Intelligence*). Eksploracja danych jest to ekstrakcja interesujących (nietrywialnych, niejawnych, wcześniej nieznanych i potencjalnie użytecznych) wzorców (wiedzy) z dużych zbiorów danych[6]. Ze względu na format analizowanych danych, na potrzeby rozpoznania cyberprzestrzeni, metody eksploracji danych można podzielić na:

- standardową eksplorację danych – dla danych ilościowych (skala pomiarowa: interwałowa, ilorazowa) i jakościowych (skala pomiarowa: nominalna, porządkowa),
- eksplorację danych tekstowych i przetwarzanie języka naturalnego – dla danych typu ciąg znaków, tekst, tekst wygenerowany z pliku audio,
- eksplorację sieci społecznych i mediów społecznościowych – dla danych jakościowych, ilościowych, danych relacyjnych reprezentujących powiązania w sieci i ogólnie dla grafów,
- przetwarzanie i analizę multimediów – dla różnorodnych danych multimedialnych reprezentujących: zdjęcia, grafiki, dźwięki, filmy, animacje itp.

5. Podstawowe problemy związane z wykorzystaniem metod eksploracji danych

Na potrzeby tego artykułu ograniczymy się do standardowej eksploracji danych i zadania klasyfikacji[7], które jest najpopularniejsze w zakresie zastosowań w szeroko rozumianym cyberbezpieczeństwie[8]. Te metody mają ograniczone zastosowania w obszarze rozpoznania cyberprzestępczości z niżej omówionych powodów[9].

---

[6] G. Piatetsky-Shapiro, U. Fayyad, P. Smyth, R. Uthurusamy, *Advances in Knowledge Discovery and Date Mining*, AAAI/MIT Press, Boston 1996.

[7] Klasyfikacja polega na przyporządkowaniu obiektu do jednej z wcześniej określonych klas.

[8] J. Jonas, J. Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, „Policy Analysis" 2006, 584.

[9] J. Surma, *Cyfryzacja życia w erze Big Data*, Wydawnictwo Naukowe PWN, Warszawa 2017.

- Systemy klasyfikacji danych z definicji działają z relatywnie dużymi błędami, które są jak najbardziej akceptowalne w zastosowaniach biznesowych. Tego typu tolerancja jest dyskusyjna w sytuacji identyfikacji cyberprzestępczości. Znaczący błąd tzw. fałszywych alarmów będzie generował relatywnie wysokie koszty weryfikowania błędnych alertów. Ponadto istnieje poważny problem braku alarmu w sytuacji zagrożenia (ang. *false negative*)[10], który *de facto* oznacza uniemożliwienie identyfikacji realnego zagrożenia.
- Problem określony w punkcie powyżej wynika z tego, że systemy eksploracji danych działają poprawnie dla zadań strukturalizowanych, powtarzalnych, gdzie koszt błędnej decyzji jest relatywnie niski oraz gdzie poszczególne klasy do klasyfikacji mają w miarę zrównoważoną reprezentację w danych uczących. Aktywności cyberprzestępców są coraz częściej niestandardowe i unikalne. Koszt błędu jest niezwykle wysoki, a liczba przypadków rzeczywistej aktywności hackerskiej w całym ciągu uczącym jest relatywnie niska. W praktyce system klasyfikacji będzie generował olbrzymią liczbę fałszywych alarmów, co może uniemożliwić praktyczne wykorzystanie.
- Ostatni problem może wynikać z prostego powodu: braku danych. Wzrastająca świadomość techniczna cyberprzestępców implikuje ograniczenie korzystania z urządzeń elektronicznych, stosowanie kryptologii i technik dezinformacyjnych. Taki brak śladów elektronicznych albo naruszenie ich integralności może skutecznie sparaliżować działanie systemu wykorzystującego metody eksploracji danych.

6. Podsumowanie

Oczekiwania względem systemów rozpoznawania zagrożeń w cyberprzestrzeni są bardzo duże. Ich użycie w praktyce jest ograniczone z m.in. powodów przedstawionych w punkcie 5. Ponadto budowa systemów tego typu bazuje na złożeniu, że hackerzy wykorzystują powszechnie dostępne portale internetowe. W praktyce działalność „publiczna" profesjonalnych cyberprzestępców jest ograniczona do niezbędnego minimum. Zwykle ograniczają się do czytania treści oraz stosują metody maskowania swojej tożsamości. Po drugie, informacja o zagrożeniach jest rozproszona, co do lokalizacji i momentu publikacji. Wymaga to umiejętności rozpoznania i integrowania danych pochodzących

[10] Zaklasyfikowanie zagrożenia jako zdarzenia nieistotnego.

z różnych źródeł w różnym czasie. Po trzecie, możliwości w zakresie analizy semantycznej tekstów są obecnie mocno ograniczone, co uniemożliwia automatyczną analizę treści z mediów społecznościowych[11]. Z powyższych powodów budowane obecnie systemy komercyjne klasy Cyber Threats Intelligence, takie jak przykładowo Palantir[12], Recorded Future[13] czy ZeroFOX[14], mają bardzo ograniczoną użyteczność. Niemniej jednak ich popularność pokazuje wyraźnie, jak ważna jest próba systemowego przewidywania zagrożeń cyberprzestrzeni.

Bibliografia

Collins M.S., *Network Security through Data Analysis Building Situational Awareness*, O'Reilly Media, Austin 2014.

Friedman J., Bouchard M., *Definitive Guide to Cyber Threat Intelligence*, Cyber Edge Press, Annapolis 2015.

Jonas J., Harper J., *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, „Policy Analysis" 2006, 584.

Piatetsky-Shapiro G., Fayyad U., Smyth P., Uthurusamy R., *Advances in Knowledge Discovery and Date Mining*, AAAI/MIT Press, Boston 1996.

Surma J., *Cyfryzacja życia w erze Big Data*, Wydawnictwo Naukowe PWN, Warszawa 2017.

Źródła sieciowe

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (dostęp: 7.04.2018).

https://www.palantir.com/ (dostęp: 7.04.2018).

https://www.recordedfuture.com/ (dostęp: 7.04.2018).

https://www.recordedfuture.com/hacker-forum-traffic (dostęp: 7.04.2018).

https://www.zerofox.com/ (dostęp: 7.04.2018).

[11] Niemniej jednak istnieją przykłady bardzo udanych analiz wywiadowczych wyłącznie na poziomie metadanych bez odwoływania się do analizy treści, https://www.recordedfuture.com/hacker-forum-traffic (dostęp: 7.04.2018).

[12] https://www.palantir.com/ (dostęp: 7.04.2018).

[13] https://www.recordedfuture.com/ (dostęp: 7.04.2018).

[14] https://www.zerofox.com/ (dostęp: 7.04.2018).

* * *

Cyber Threat Intelligence Systems: problems and challenges

Abstract

Cyber Threat Intelligence is a component of cybersecurity intelligence and includes both the information relevant to protecting an organization from external and inside threats as well as the processes, policies and tools designed to gather and analyze that information. Cyber Threat Intelligence services provide organizations with current information related to potential attack sources relevant to their businesses. One of the main problems in implementing Cyber Threat Intelligence systems lies in applying advanced data mining techniques.

Keywords: Cyber Threat Intelligence, data mining, cybersecurity