FUNDACJA bezpieczna cyberprzestrzeń

WYKORZYSTANIE MODELI CYBER THREAT INTELLIGENCE JAKO ELEMENT SKUTECZNEGO REAGOWANIA NA INCYDENTY KOMPUTEROWE

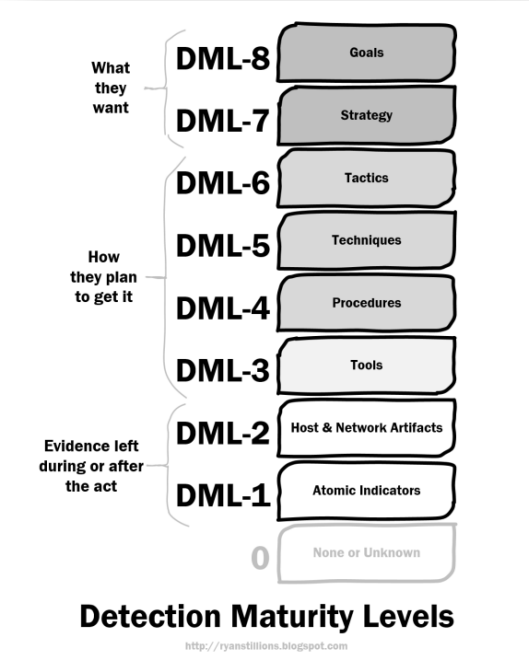
1312.2017

Specjaliści bezpieczeństwa teleinformatycznego nieustannie zmagają się z coraz bardziej wyrafinowanymi scenariuszami cyber ataków. Adwersarze, a zwłaszcza grupy hakerskie typu APT (*Advanced Persistent Threats)* dokonują czasochłonnych i skrupulatnych przygotowań, które z powodzeniem można przyrównać do planowania charakterystycznego dla operacji wojskowych. W cyberprzestrzeni na tej zasadzie funkcjonują chociażby takie organizacje jak APT28, Lazarus czy Butterfly. Ich działania bywają na tyle złożone, iż eksperci analizując poszczególne kampanie zaczęli opracowywać modele strukturalne, w których m.in. wyróżniają poszczególne fazy ataku (np. *Cyber Kill Chain* opracowany przez koncern Lockheed Martin).

Tradycyjnie uważa się, że strona atakująca (*red team*) zawsze posiada przewagę nad stroną utrzymującą bezpieczeństwo systemów (*blue team*). Wielopoziomowa analiza zagrożeń, zarówno techniczna, behawioralna czy kontekstowa (zawierająca także analizę typu INFOOPS) jest elementem budowy przewagi nad hakerami i może być wykorzystana jako czynnik zmieniający proporcje z korzyścią dla niebieskich. Działania te są przeprowadzane z użyciem profesjonalnych narzędzi informatycznych, choć warto zastrzec, że otrzymany z nich strumień danych jest tylko początkiem procesu analizy. Dopiero jego interpretacja może pomóc nam wzmocnić zdolności rozpoznawania zagrożeń, przewidywania postępowania hakerów i w końcu, reagowania na incydenty. Zbiór takich praktyk, będących pewnego rodzaju wywiadem w cyberprzestrzeni, określa się mianem *cyber threat intelligence*, właśnie z uwagi na podobieństwo do działalności instytucji wywiadowczych.

> WIELOPOZIOMOWA ANALIZA ZAGROŻEŃ, ZARÓWNO TECHNICZNA, BEHAWIORALNA CZY KONTEKSTOWA (ZAWIERAJĄCA TAKŻE ANALIZĘ TYPU INFOOPS) JEST ELEMENTEM BUDOWY PRZEWAGI NAD HAKERAM

Tak jak skuteczne reagowanie na incydenty komputerowe w cyberprzestrzeni, również i efektywne *cyber threat intelligence* jest oparte na procedurach i metodykach. Jednym z takich pomocniczych i aktualnych modeli jest Cyber Threat Intelligence Model (CTI) zaproponowany przez naukowców z Uniwersytetu w Oslo – V. Mavroeidisa oraz S. Bromander. Model CTI jest rozwinięciem prac Ryana Stillionsa, specjalisty bezpieczeństwa IT i autora m.in. modelu dojrzałości wykrywania zagrożeń (DML – *Detection Maturity Level Model*).



Rysunek 1. Detection Maturity Level Model.
Źródło: http://ryanstillions.blogspot.com

Podejście Norwegów jest o tyle innowacyjne, iż wraz z rozwinięciem i modyfikacją modelu Stillionsa, oprócz zdolności wykrywania (detective capabilities), dodali także zdolności prewencyjne (preventive capabilities), związane bezpośrednio z blokiem TTPs (tactics, techniques, procedures). Właśnie od strony technik, badacze wskazują na 3 główne elementy, które determinują zdolności prewencyjne, są nimi wzorce ataku, rodzaj użytego złośliwego oprogramowania oraz infrastruktura użyta do przeprowadzenia operacji (np. serwery *command & control* czy strony phishingowe)[1].

Kolejną nowością w stosunku do modelu Stillionsa jest potraktowanie jako osobno bloku wskaźników informujących o kompromitacji systemu (Indicators of Compromise). W tym przypadku analiza po stronie obrony powinna skupiać się na zebraniu i porównaniu tzw. wskaźników atomowych (artefakty takie jak

[1] https://www.duo.uio.no/bitstream/handle/10852/58492/CTI_Mavroeidis%25282017%2529.pdf?sequence=1

adresy e-mail, nazwy domen czy adresy IP), wskaźników behawioralnych (wskaźniki, które mogą być istotne w zakresie profilowania hakerów, czyli w jaki sposób zachowuje się przestępca) oraz takich wskaźników takich hashe zainfekowanych plików czy uzyskane dane z serwerów C2[2].

Specjaliści z Uniwersytetu w Oslo uzupełniają model DML także o blok „Identity", czyli dokładne (tożsamościowe) rozpoznanie atrybucji zagrożeń. Mimo, że w opiniach wielu ekspertów jest to element najtrudniejszy do ustalenia, staje się on bardzo pomocny, jeśli już poznamy aktora i chcemy przewidzieć jego dalszą aktywność (na których oparte są nazwy bloków poniżej „Identity"). Wiedza taka bezpośrednio przyczynia się do ulepszenia reakcji na incydenty. Jest też poniekąd dostępna publicznie – w sieci znajdują się raporty, które opisują działalność znanych grup cyberprzestępczych.

Model CTI może służyć jako podstawowy drogowskaz w procesie budowania uporządkowanej wiedzy o zagrożeniach. Pomaga w tym również hierarchiczność i ciąg logiczny schematu - od weryfikacji celu aż po ustalenie tożsamości cyberprzestępców. Na koniec, warto także wspomnieć o tym, że skuteczne budowanie zdolności threat intelligence nie może ograniczać się do wewnętrznych zasobów organizacji i własnych doświadczeń. Jako że współpraca jest kluczem co cyberbezpieczeństwa, dobrze jeśli kluczowe informacje o zagrożeniach, wraz z przypisanymi im artefaktami znajdą się na dedykowanych platformach, takich jak np. MISP opracowana przez zespół CIRCL.LU.

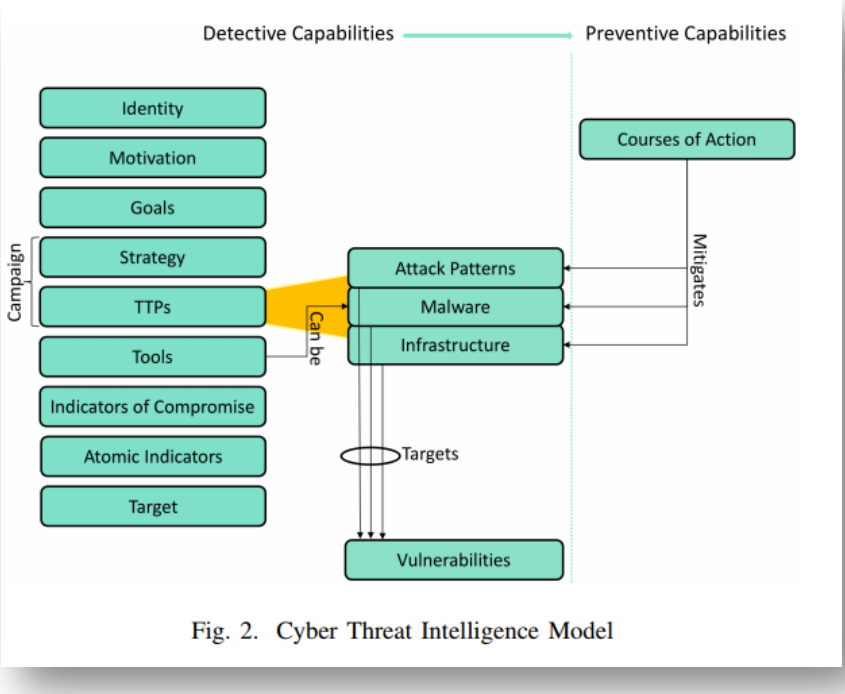


Fig. 2. Cyber Threat Intelligence Model

Rysunek 2. Cyber Threat Intelligence Model, źródło:
https://www.duo.uio.no/bitstream/handle/10852/58492/CTI_Mavroeidis%25282017%2529.pdf?sequence=1

[2] https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/

Z pewnością złośliwe kampanie będą coraz bardziej rozbudowane, a ich skutki dotkliwe, tak jak udowodnił mijający 2017 rok w przypadku robaków WannaCry czy NotPetya. Rozwijanie zdolności threat intelligence będzie zatem niezbędnym elementem wyścigu „cyber zbrojeń". Już teraz wiele podmiotów zauważa ten trend i wprowadza go w obszar działań obronnych. Rozwijanie tej wiedzy wpływa pozytywnie na ogólny poziom cyberbezpieczeństwa, jest także stymulatorem współpracy w branży. *Cyber Threat Intelligence* powoli staje się również stałą ofertą wśród producentów dostarczających usługi i produkty z zakresu cyberbezpieczeństwa. Niemal pewne jest też to, że modele typu CTI będą dalej ewoluowały, co będzie stanowić naturalną odpowiedź dla coraz bardziej wyrafinowanych zagrożeń w cyberprzestrzeni.

Autor: Kamil Gapiński

Kierownik Projektu
Fundacja Bezpieczna Cyberprzestrzeń

Śledź na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**