Romuald Hoffmann[1]

Markowowskie modele cykli życia ataku cybernetycznego

1. Wstęp

Obecnie jednym z głównych problemów wielu organizacji są cyberataki ukierunkowane[2], mające na celu ustanowienie niewykrywalnej i trwałej obecności atakującego w docelowej infrastrukturze informatycznej. Ataki takie mają charakter wieloetapowy i wraz z postępem technologicznym stają się coraz bardziej złożone, obejmując elementy zaatakowanej organizacji na wielu jej poziomach. Wbrew powszechnemu poglądowi ataki cybernetyczne APT wcale nie są procesem krótkotrwałym. W istocie jest to ciąg wykonywanych w odpowiedniej kolejności czynności, które łączy się w logiczne grupy i realizuje się etapowo, tworząc w ten sposób proces ataku cybernetycznego. Proces ataku cybernetycznego, podzielony na etapy (fazy) o relatywnie długim czasie trwania, można nazywać cyklem życia ataku cybernetycznego (ang. *cyber attack life cycle*)[3]. Analiza przypadków ataków komputerowych wskazuje, że proces ataku cybernetycznego nie jest z natury zdeterminowany. Do tej pory w dostępnych źródłach próżno szukać stochastycznych modeli cyklu życia ataku cybernetycznego. Celem artykułu jest zaproponowanie modeli wybranych cykli życia ataku cybernetycznego na bazie jednorodnych łańcuchów Markowa z ciągłym parametrem czasu.

---

[1] Wojskowa Akademia Techniczna, Wydział Cybernetyki, Instytut Systemów Informatycznych.

[2] APT, Advanced Persistent Threats.

[3] Zwany również „Cyber Kill Chain".

2. Fazy procesu ataku cybernetycznego w literaturze

W dostępnej literaturze fazy procesu cyberataku, ich liczba i role są różnie definiowane oraz opisywane. Według US Air Force Institute of Technology[4] proces ten składa się z pięciu etapów[5]:

1) rozpoznanie,
2) skanowanie,
3) dostęp do systemu,
4) instalacja kodu złośliwego,
5) eksploatacja kodu.

Firma Mandiant opublikowała w swoim raporcie[6] analitycznym, dotyczącym działalności chińskich jednostek cyberprzestępczych, opis procesu cyberataku APT, nazywając go cyklem życia ataku. W opisie wspomnianego cyklu wskazuje się na siedem etapów[7]:

1) wstępna kompromitacja systemu,
2) uchwycenie przyczółku,
3) eskalacja przywilejów,
4) wewnętrzne rozpoznanie,
5) penetracja horyzontalna,
6) utrzymanie kontroli (obecności),
7) zakończenie misji.

Firma Mandiant utrzymuje, że cykl ten w owym czasie był wykorzystywany przez chińskie jednostki szpiegostwa cybernetycznego do penetrowania zasobów wielu rządów i korporacji. Koncern Lockheed Martin[8] proces ataku cybernetycznego, tzw. Cyber Kill Chain®, definiuje jako ciąg siedmiu etapów[9]:

---

4 K.G.J. Coleman, *Aggresssion in Cyberspace*, w: *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, S. Jasper (red.), Georgetown University Press, Washington DC 2012, s. 105–119.

5 *Reconnaissance*, *scanning*, *system access*, *malicious activity*, *exploitation*.

6 Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (dostęp: 5.12.2013).

7 *Initial compromise*, *establish foothold*, *escalate privileges*, *internal reconnaissance*, *move laterally*, *maintain presence*, *complete mission*.

8 E.M. Hutchins, M.J. Cloppert, R.M. Amin, *Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, w: *Leading Issues in Information Warfare and Security Research*, J. Ryan (red.), t. 1, Academic Publishing International Ltd, Reading, UK 2011, s. 78–104.

9 *Reconnaissance*, *weaponization*, *delivery*, *exploitation*, *installation*, C2, *action*.

1) rozpoznanie,
2) uzbrojenie,
3) dostarczenie,
4) eksploracja,
5) instalacja,
6) kierowanie i dowodzenie,
7) akcja tzn. ostateczny atak celu.

Proces ten również opisują badacze J.M. Spring i E. Hatleback[10] oraz M.S. Khan, S. Siddiqui i K. Ferens[11]. Ci ostatni zauważają[12], że w zależności od typu ataku niektóre etapy procesu mogą zostać pominięte przez agresora. Inna firma, korporacja Dell[13], definiuje osiem faz cyklu życia ataku cybernetycznego[14]:
1) rozpoznanie,
2) przegląd stanu rozwoju infrastruktury otoczenia celu,
3) uzbrojenie,
4) dostarczenie,
5) eksploracja,
6) instalacja,
7) kierowanie i dowodzenie,
8) atak celu.

Propozycja firmy Dell, podobna w swojej istocie do podejścia Lockheed Martin, różni się od niego tylko dodatkową fazą przeglądu infrastruktury ofiary ataku[15]. Inni badacze, tacy jak: A. Hahn, R.K. Thomas, I. Lozano i A. Cardenas[16], wskazują na sześć faz:
1) rozpoznanie,
2) uzbrojenie,

---

[10] J.M. Spring, E. Hatleback, *Thinking about Intrusion Kill Chains as Mechanisms*, „Journal of Cybersecurity" 2017, vol. 3(3), s. 185–197.

[11] M.S. Khan, S. Siddiqui, K. Ferens, *A Cognitive and Concurrent Cyber Kill Chain Model*, w: *Computer and Network Security Essentials*, K. Daimi (red.), Springer, Cham, Switzerland 2018, s. 585–602.

[12] Ibidem, s. 585–602.

[13] Dell SecureWorks, *Advanced Threat Protection with Dell SecureWorks Security Services*, Dell 2014, https://www.secureworks.com/~/media/Files/US/Solution %20Briefs/DellSecureWorksNCO346NAdvancedThreatProtection.ashx (dostęp: 14.05.2018).

[14] *Reconnaissance*, *development*, *weaponization*, *delivery*, *exploitation*, *installation*, *command and control*, *action*.

[15] Faza w j. ang.: *development*.

[16] A. Hahn, R.K. Thomas, I. Lozano, A. Cardenas, *A Multi-layered and Kill-chain Based Security Analysis Framework for Cyber-physical Systems*, „International Journal of Critical Infrastructure Protection" 2015, vol. 11, s. 39–50.

3) dostarczenie,
4) eksploracja,
5) kierowanie i dowodzenie,
6) osiągnięcie celu.

Jednocześnie ci sami ww. autorzy[17] wskazują, że atak na infrastrukturę krytyczną należy rozpatrywać jako ciąg czterech następujących bezpośrednio po sobie podstawowych faz[18]:

1) rozpoznanie trzech warstw systemowych: systemów informatycznych, systemów sterowania automatyką i układów urządzeń fizycznych,
2) uzbrojenie,
3) dostarczenie kodu złośliwego,
4) realizacja (obejmująca trzy fazy tradycyjne: eksploracji, kierowania i dowodzenia, osiągnięcia celu)

oraz jako konsekwencję działań agresora dodatkowo dwóch faz:

5) zakłócenie sterowania automatyką,
6) atak na fizyczne urządzenia infrastruktury.

We wszystkich ww. podejściach do opisu procesu ataku nie wyszczególnia się etapu inicjacji procesu i jego zakończenia. Niedawno został zaproponowany[19] uogólniony cykl życia ataku cybernetycznego, zawierający dwie dodatkowe fazy: identyfikacji potrzeb atakującego oraz zakończenia ataku cybernetycznego połączonego z zatarciem śladów.

3. Przyjęte założenia i oznaczenia

Niezależnie od tego, jak dotychczas różni autorzy opisywali proces ataku cybernetycznego, jego cykl życia generalnie definiowany jest jako sekwencja od czterech do ośmiu faz. Zatem ogólnie możemy przyjąć, że mamy N faz cyklu życia ataku cybernetycznego ponumerowanych od 1 od N ($N \geq 4$). Zachowanie się procesu ataku pozwala przyjąć założenie spełnienia własności Markowa. Na potrzeby artykułu przyjmujemy czas ciągły i znajomość macierzy intensywności. Jednocześnie zakładamy, że poszczególne intensywności przejść pomiędzy

[17] Ibidem, s. 39–50.
[18] *Reconnaissance*, *weaponization*, *delivery*, *cyber execution*.
[19] R. Hoffmann, *Ogólny cykl życia ataku cybernetycznego i jego markowowski model*, „Ekonomiczne Problemy Usług" 2018, nr 2(131), t. 1, s. 121–130.

fazami są skończone i niezmienne w czasie. Wobec tego zachowanie się poszczególnych cykli ataku opisywać będziemy za pomocą jednorodnego łańcucha Markowa z czasem ciągłym[20]. Kolejnymi stanami procesu stochastycznego będą odpowiednie fazy cyklu życia ataku.

Zatem na potrzeby dalszych rozważań przyjmiemy następującą konwencję oznaczeń. Niech $X(t)$ dla $0 \le t \le +\infty$ będzie łańcuchem Markowa z ciągłym parametrem czasu t i ze skończoną liczbą stanów. Proces $X(t)$ będzie modelem opisującym zachowanie się rozważanego cyklu życia ataku cyberentycznego. Przez S_i przyjmujemy oznaczać stan procesu $X(t)$, gdzie i oznacza numer fazy $(i = 1,2,...,N)$. Stany $S_1, S_2, ..., S_N$ odpowiadają poszczególnym fazom cyklu życia ataku. Wobec tego zbiór $\{S_1, S_2, ..., , S_N\} = \{S_i\}_{i=\overline{1,N}}$ będzie zbiorem stanów procesu $X(t)$. Zdarzenie, że proces $X(t)$ w chwili $t \ge 0$ znajduje się w stanie S_i, zapisywać będziemy jako $\{X(t) = S_i\}$. Symbolem λ_{ij} $(i, j = 1,2,...,N)$ oznaczać będziemy intensywność przejścia procesu $X(t)$ ze stanu S_i do stanu S_j. Natomiast symbolem $P_i(t)$ przyjmujemy oznaczać prawdopodobieństwo przebywania w chwili $t \ge 0$ procesu $X(t)$ w stanie S_i, tzn. $P_i(t) = P\{X(t) = S_i\}$. Aby uprościć zapisy wzorów przyjmiemy, że wektor wierszowy prawdopodobieństw stanów oznaczymy przez $\boldsymbol{P}(t) = [P_1(t), P_2(t), \ ..., P_i(t), ..., P_N(t)]$ dla $t \ge 0$. Macierz intensywności przejść procesu $X(t)$ pomiędzy stanami przyjmujemy oznaczać przez $\boldsymbol{Q} = [\lambda_{ij}]_{N \times N}$ $(\lambda_{ij} < +\infty)$. Ponadto dla uproszczenia zapisów przez μ_i oznaczać będziemy intensywność przejścia λ_{iN} procesu $X(t)$ ze stanu S_i do stanu S_N dla $i = 1,2,...,N-1$, natomiast przez λ_i intensywność przejścia $\lambda_{i\,i+1}$ procesu $X(t)$ ze stanu S_i do stanu S_{i+1} dla $i = 1,2,...,N-2$.

4. Prosty cykl życia ataku cybernetycznego

Przy uwzględnieniu wcześniej przyjętych założeń i oznaczeń, bieżącym modelem cyklu życia ataku cybernetycznego będzie łańcuch Markowa $X(t)$ ze zbiorem faz (stanów) $\{S_i\}_{i=\overline{1,N}}$, który może przechodzić sekwencyjnie przez fazy od S_1 do S_{N-1} bez możliwości pominięcia jakiejkolwiek z faz i powrotu do poprzednich. Ponadto w chwili $t > 0$ proces $X(t)$ może przejść z dowolnej fazy $(S_i)_{i=\overline{1,N-1}}$ do fazy S_N. Przejście to odpowiada sytuacji zakończenia ataku z różnych powodów,

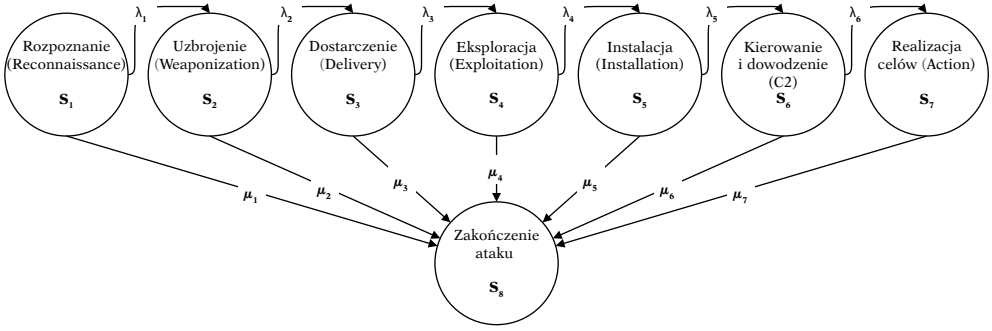
[20] I.N. Kowalenko, N.J. Kuzniecow, W.M. Szurienkow, *Procesy stochastyczne. Poradnik*, PWN, Warszawa 1989, s. 57–64; jednorodny proces Markowa dyskretny w stanach z ciągłym parametrem czasu.

np. z powodu zmiany zamiaru przez agresora, wykrycia i zablokowania jego działań przez mechanizmy obronne atakowanego systemu. Tak zdefiniowany model nazywać będziemy dalej prostym cyklem ataku cybernetycznego (rysunek 1).

W przykładowym modelu przyjmiemy fazy procesu ataku cybernetycznego zgodne z Cyber Kill Chain®[21]. Wobec tego modelem prostego cyklu życia ataku cybernetycznego odpowiadającego fazom ataku Cyber Kill Chain® jest łańcuch Markowa $X(t)$ określony przez macierz $\boldsymbol{Q}$ intensywności przejść:

$$Q = \begin{bmatrix} -\lambda_1 - \mu_1 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & \mu_1 \\ 0 & -\lambda_2 - \mu_2 & \lambda_2 & 0 & 0 & 0 & 0 & \mu_2 \\ 0 & 0 & -\lambda_3 - \mu_3 & \lambda_3 & 0 & 0 & 0 & \mu_3 \\ 0 & 0 & 0 & -\lambda_4 - \mu_4 & \lambda_4 & 0 & 0 & \mu_4 \\ 0 & 0 & 0 & 0 & -\lambda_5 - \mu_5 & \lambda_5 & 0 & \mu_5 \\ 0 & 0 & 0 & 0 & 0 & -\lambda_6 - \mu_6 & \lambda_6 & \mu_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & -\mu_7 & \mu_7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (1)$$

Na rysunku 1 umieszczono graf przejść dla procesu Markowa $X(t)$ z macierzą $\boldsymbol{Q}$ (wzór (1)) oraz siedem podstawowych faz Cyber Kill Chain®.



Rysunek 1. Graf Markowa prostego cyklu ataku cybernetycznego z etapami procesu ataku wg koncepcji Lockheed Martin Cyber Kill Chain®

Źródło: opracowanie własne.

[21] Wg koncepcji koncernu Lockheed Martin.

Układ równań różniczkowych Kołmogorowa[22], pozwalający na wyznaczenie wektora $\boldsymbol{P}(t)$ rozkładu prawdopodobieństw przebywania procesu $X(t)$ w chwili $t>0$ w poszczególnych stanach przy danej macierzy intensywności przejść $\boldsymbol{Q}$ danej wzorem (1) ma postać:

$$\frac{d}{dt}\boldsymbol{P}(t)=\boldsymbol{P}(t)\cdot\boldsymbol{Q} \tag{2}$$

z warunkiem początkowym $\boldsymbol{P}(0)=\left[P_1(0),\ P_2(0),\ldots,P_8(0)\right]=\left[1,0,\ldots,0\right]$.

Najprostszą metodą rozwiązania układu (2) jest wykorzystanie przekształcenia Laplace'a $\boldsymbol{P}^*(s)=\mathcal{L}\left[\boldsymbol{P}(t);s\right]=\int_0^{+\infty}\boldsymbol{P}(t)\cdot e^{-st}dt$. Zatem po dokonaniu przekształcenia Laplace'a ostatecznie uzyskujemy następującą postać operatorową:

$$\boldsymbol{P}^*(s)\cdot\left[s\cdot\boldsymbol{I}-\boldsymbol{Q}\right]=\boldsymbol{P}(0), \tag{3}$$

gdzie macierz $\boldsymbol{I}$ jest macierzą jednostkową, a macierz $s\cdot\boldsymbol{I}-\boldsymbol{Q}$ ma postać:

$$s\boldsymbol{I}-\boldsymbol{Q}=$$

$$=\begin{bmatrix}
s+\lambda_1+\mu_1 & -\lambda_1 & 0 & 0 & 0 & 0 & 0 & -\mu_1\\
0 & s+\lambda_2+\mu_2 & -\lambda_2 & 0 & 0 & 0 & 0 & -\mu_2\\
0 & 0 & s+\lambda_3+\mu_3 & -\lambda_3 & 0 & 0 & 0 & -\mu_3\\
0 & 0 & 0 & s+\lambda_4+\mu_4 & -\lambda_4 & 0 & 0 & -\mu_4\\
0 & 0 & 0 & 0 & s+\lambda_5+\mu_5 & -\lambda_5 & 0 & -\mu_5\\
0 & 0 & 0 & 0 & 0 & s+\lambda_6+\mu_6 & -\lambda_6 & -\mu_6\\
0 & 0 & 0 & 0 & 0 & 0 & s+\mu_7 & -\mu_7\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & s
\end{bmatrix}$$

W konsekwencji otrzymujemy rozwiązanie operatorowe:

$$\boldsymbol{P}^*(s)=\boldsymbol{P}(0)\cdot\left[s\cdot\boldsymbol{I}-\boldsymbol{Q}\right]^{-1}. \tag{4}$$

Stąd każda składowa $P_k^*(s)$ wektora $\boldsymbol{P}^*(s)$ wyraża się wzorem:

$$P_k^*(s)=\frac{1}{\det\left[s\cdot\boldsymbol{I}-\boldsymbol{Q}\right]}\sum_{i=1}^{8}P_i(0)\cdot D_{ki} \tag{5}$$

[22] I.N. Kowalenko, N.J. Kuzniecow, W.M. Szurienkow, op. cit., s. 60.

gdzie D_{ki} dopełnieniem algebraicznym wyznacznika macierzy $\left[s\cdot\boldsymbol{I}-\boldsymbol{Q}\right]$ powstałym przez skreślenie k-tego wiersza oraz i-tej kolumny macierzy. Zauważmy, że z powodu rozkładu początkowego $\boldsymbol{P}(0)=[1,0,\ldots,0]$ prawdopodobieństwo (5) redukuje się do postaci $P_k^*(s)=\dfrac{D_{k1}}{\det\left[s\cdot\boldsymbol{I}-\boldsymbol{Q}\right]}$. Stąd ostatecznie składowe wektora $\boldsymbol{P}^*(s)$ przyjmują postać:

$$\boldsymbol{P}^*(s)^T =$$

$$= \left[\begin{array}{c} \dfrac{1}{s+\lambda_1+\mu_1} \\ \dfrac{\lambda_1}{(s+\lambda_1+\mu_1)(s+\lambda_2+\mu_2)} \\ \dfrac{\lambda_1\lambda_2}{(s+\lambda_1+\mu_1)(s+\lambda_2+\mu_2)(s+\lambda_3+\mu_3)} \\ \dfrac{\lambda_1\lambda_2\lambda_3}{(s+\lambda_1+\mu_1)(s+\lambda_2+\mu_2)(s+\lambda_3+\mu_3)(s+\lambda_4+\mu_4)} \\ \dfrac{\lambda_1\lambda_2\lambda_3\lambda_4}{(s+\lambda_1+\mu_1)(s+\lambda_2+\mu_2)(s+\lambda_3+\mu_3)(s+\lambda_4+\mu_4)(s+\lambda_5+\mu_5)} \\ \dfrac{\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5}{(s+\lambda_1+\mu_1)(s+\lambda_2+\mu_2)(s+\lambda_3+\mu_3)(s+\lambda_4+\mu_4)(s+\lambda_5+\mu_5)(s+\lambda_6+\mu_6)} \\ \dfrac{\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5\lambda_6}{(s+\lambda_1+\mu_1)(s+\lambda_2+\mu_2)(s+\lambda_3+\mu_3)(s+\lambda_4+\mu_4)(s+\lambda_5+\mu_5)(s+\lambda_6+\mu_6)(s+\mu_7)} \\ \dfrac{1}{s}\cdot\sum_{k=1}^{7}\mu_k\cdot P_k^*(s) \end{array}\right] \quad (6)$$

Aby wyznaczyć rozwiązania w dziedzinie czasu poprzez dokonanie przekształcenia odwrotnego, zauważmy, że składowe $P_k^*(s)$ wektora operatorowych prawdopodobieństw $\boldsymbol{P}^*(s)$ dla stanów S_k $(k=1,\ldots 8)$ są funkcjami wymiernymi. W tym przypadku najefektywniejszą metodą przekształcenia odwrotnego jest wykorzystanie twierdzenia o residuach. W myśl tego twierdzenia rozwiązaniem dla $t\geq 0$ będzie wektor $\boldsymbol{P}(t)=\mathcal{L}^{-1}\left[\boldsymbol{P}^*(s);t\right]$ o składowych:

$$P_k(t)=\sum_j\frac{1}{(n_j-1)!}\lim_{s\to s_j}\frac{d^{n_j-1}}{ds^{n_j-1}}\left[\left(s-s_j\right)^{n_j}\cdot P_k^*(s)\cdot e^{st}\right], \quad (7)$$

gdzie s_j jest j-tym biegunem $P_k^*(s)$, n_j – krotnością j-tego bieguna.

Gdy wszystkie bieguny $P_k^*(s)$ są pojedyncze, wówczas wzór (9) upraszcza się do postaci:

$$P_k(t) = \sum_j \lim_{s \to s_j} (s - s_j) \cdot P_k^*(s) \cdot e^{st} \tag{8}$$

Ostatecznie w sytuacji, gdy intensywności przejść są różnowartościowe na podstawie wzorów (2) ÷ (8) otrzymujemy ogólne wzory na prawdopodobieństwa przebywania procesu $X(t)$ w poszczególnych stanach S_k ($k = 1,2,\ldots,8$):

$$P_1(t) = e^{-(\lambda_1+\mu_1)t}$$

$$P_k(t) = \prod_{j=1}^{k-1} \lambda_j \cdot \sum_{n=1}^{k} \frac{e^{-(\lambda_n+\mu_n)\cdot t}}{\prod_{\substack{i=1 \\ i\neq n}}^{k} (\lambda_n + \mu_n - \lambda_i - \mu_i)} \text{ dla } k = 2, \ldots, 6 \tag{9}$$

$$P_7(t) = \prod_{j=1}^{6} \lambda_j \cdot \left[\sum_{k=1}^{7} \frac{e^{-(\lambda_n+\mu_n)\cdot t}}{(\lambda_n + \mu_n - \mu_7) \prod_{\substack{i=1 \\ i\neq n}}^{6} (\lambda_n + \mu_n - \lambda_i - \mu_i)} + \frac{e^{-\mu_7 \cdot t}}{\prod_{i=1}^{6} (\lambda_i + \mu_i - \mu_7)} \right]$$

$$P_8(t) = \sum_{k=1}^{7} \mu_k \cdot P_k(t)$$

Na praktyczne potrzeby zobrazowania obliczeń, przyjmując intensywności przejść $(\mu_k = \mu)_{k=\overline{1,7}}$, rozpatrzymy dwa przypadki szczególne: $(\lambda_k = \lambda)_{k=\overline{1,6}}$ i $(\lambda_k = k \cdot \lambda)_{k=\overline{1,6}}$. W pierwszym, jeżeli $(\lambda_k = \lambda)_{k=\overline{1,6}}$, to na podstawie wzorów (4) ÷ (9) otrzymujemy następujący rozkład prawdopodobieństwa w chwili $t \geq 0$:

$$\boldsymbol{P}^{\boldsymbol{T}}(t) = \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \\ P_5(t) \\ P_6(t) \\ P_7(t) \\ P_8(t) \end{bmatrix} = \begin{bmatrix} e^{-(\lambda+\mu)t} \\ e^{-(\lambda+\mu)t} \lambda t \\ e^{-(\lambda+\mu)t} \frac{1}{2!} \lambda^2 t^2 \\ e^{-(\lambda+\mu)t} \frac{1}{3!} \lambda^3 t^3 \\ e^{-(\lambda+\mu)t} \frac{1}{4!} \lambda^4 t^4 \\ e^{-(\lambda+\mu)} \frac{1}{5!} \lambda^5 t^5 \\ e^{-\mu t} - e^{-(\lambda+\mu)t} \sum_{k=1}^{6} \frac{1}{(k-1)!} \lambda^{k-1} t^{k-1} \\ 1 - e^{-\mu t} \end{bmatrix} \tag{10}$$

W przypadku drugim, gdy $\left(\lambda_k = k \cdot \lambda\right)_{k=\overline{1,6}}$ rozkład prawdopodobieństwa procesu $X(t)$ w chwili $t \geq 0$ przyjmuje postać:

$$\boldsymbol{P}^{\boldsymbol{T}}\left(t\right) = \begin{bmatrix} e^{-(\lambda+\mu)t} \\ e^{-(\lambda+\mu)t} - e^{-(2\lambda+\mu)t} \\ e^{-(\lambda+\mu)t} - 2e^{-(2\lambda+\mu)t} + e^{-(3\lambda+\mu)t} \\ e^{-(\lambda+\mu)t} - 3e^{-(2\lambda+\mu)t} + 3e^{-(3\lambda+\mu)t} - e^{-(4\lambda+\mu)t} \\ e^{-(\lambda+\mu)t} - 4e^{-(2\lambda+\mu)t} + 6e^{-(3\lambda+\mu)t} - 4e^{-(4\lambda+\mu)t} + e^{-(5\lambda+\mu)t} \\ e^{-(\lambda+\mu)t} - 5e^{-(2\lambda+\mu)t} + 10e^{-(3\lambda+\mu)t} - 10e^{-(4\lambda+\mu)t} + 5e^{-(5\lambda+\mu)t} - e^{-(6\lambda+\mu)t} \\ e^{-\mu t} - 6e^{-(\lambda+\mu)t} + 15e^{-(2\lambda+\mu)t} - 20e^{-(3\lambda+\mu)t} + 15e^{-(4\lambda+\mu)t} - 6e^{-(5\lambda+\mu)t} + e^{-(6\lambda+\mu)t} \\ 1 - e^{-\mu t} \end{bmatrix} \tag{11}$$

Ostatecznie składowe wektora $P\left(t\right) = \left[P_1\left(t\right), \ldots, P_k\left(t\right), \ldots, P_8\left(t\right)\right]$ są następujące:

$$\begin{gathered} P_k\left(t\right) = e^{-(k\cdot\lambda+\mu)t}\left(-1+e^{\lambda t}\right)^{k-1} \text{ dla } k = 1, \ldots, 6, \\ P_7\left(t\right) = e^{-(6\lambda+\mu)t}\left(-1+e^{\lambda t}\right)^{6}, \\ P_8\left(t\right) = 1 - e^{-\mu t}. \end{gathered} \tag{12}$$

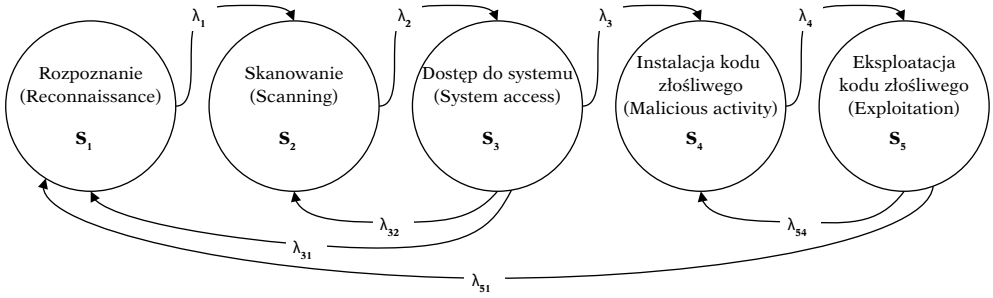
5. Cykl życia ataku cybernetycznego z iteracjami

Łańcuch Markowa $X(t)$ dla $t \geq 0$ ze zbiorem stanów $\left\{S_i\right\}_{i=\overline{1,N}}$, który może nie tylko przechodzić kolejno przez wszystkie fazy od S_1 do S_N, ale także ma możliwość w chwili $t > 0$ powrotu z bieżącej fazy do faz poprzedzających, nazywać będziemy cyklem życia ataku cybernetycznego z iteracjami. Jako przykład takiego modelu rozpatrzymy cykl ataku z iteracjami zgodny z etapami procesu ataku wg US Air Force Institute of Technology (rysunek 2).

W przykładowym modelu zakładamy, że proces ataku może być przeprowadzony sekwencyjnie, tzn. przejścia pomiędzy kolejnymi fazami ataku od S_1 do S_5 mogą nastąpić kolejno bez pominięcia jakiekolwiek fazy. Ponadto przyjmujemy, że proces może przejść z fazy S_5 do S_1 oraz z S_3 do S_1, co interpretujemy jako zakończenie (lub przerwanie) bieżącego ataku i rozpoczęcie nowego cyklu. Możliwe są iteracje z S_5 do S_4 oraz z S_3 do S_1, stanowiące korektę ataku. Pełną ilustrację rozpatrywanego w tym paragrafie cyklu stanowi rysunek 2, który

jednocześnie przedstawia graf Markowa jako ilustrację macierzy przejść procesu $X(t)$. W tym modelu macierz intensywności przejść $\boldsymbol{Q}$ ma postać:

$$\boldsymbol{Q} = \begin{bmatrix} -\lambda_1 & \lambda_1 & 0 & 0 & 0 \\ 0 & -\lambda_2 & \lambda_2 & 0 & 0 \\ \lambda_{31} & \lambda_{32} & -\lambda_3 - \lambda_{31} - \lambda_{32} & \lambda_3 & 0 \\ 0 & 0 & 0 & -\lambda_4 & \lambda_4 \\ \lambda_{51} & 0 & 0 & \lambda_{54} & -\lambda_{51} - \lambda_{54} \end{bmatrix} \tag{13}$$



Rysunek 2. Graf Markowa cyklu ataku cybernetycznego z iteracjami zgodny etapami procesu ataku wg koncepcji US Air Force Institute of Technology

Źródło: opracowanie własne.

Przy tak określonym cyklu ataku interesujące są dla nas graniczne rozkłady prawdopodobieństwa. Na podstawie ergodycznego twierdzenia Markowa wiemy, że jeżeli dla (jednorodnego) łańcucha Markowa z ciągłym parametrem czasu o skończonej liczbie stanów istnieje niezerowa macierz intensywności przejść $\boldsymbol{Q}$, to istnieją oraz są skończone i nie zależą od rozkładu początkowego $\boldsymbol{P}(0)$ granice $P_k = \lim_{t\to\infty} P_k(t)$, które nazywane są rozkładem granicznym lub stacjonarnym[23].

W rozpatrywanym modelu założenia ergodycznego twierdzenia Markowa są spełnione i istnieje rozkład graniczny.

Niech $\boldsymbol{P} = \left[P_1, P_2, P_3, P_4, P_5\right]$ będzie rozkładem granicznym (stacjonarnym), gdzie $\sum_{k=1}^{5} P_k = 1$. Zatem jeżeli $\lim_{t\to\infty} P_k(t) = P_k$, to $\lim_{t\to\infty} \frac{d}{dt} P_k(t) = 0$. Z tego wynika, że

[23] Ibidem, s. 77–80.

układ równań różniczkowych Kołmogorowa $\frac{d}{dt}\boldsymbol{P}(t) = \boldsymbol{P}(t)\cdot\boldsymbol{Q}$ przy $t \to \infty$ przyjmuje postać układu równań liniowych $\boldsymbol{P}\cdot\boldsymbol{Q} = 0$ ze względu na P_k.

Zauważmy, że układ równań[24] $\boldsymbol{P}\cdot\boldsymbol{Q} = 0$ jest nieoznaczony, dlatego aby wyznaczyć rozkład stacjonarny $\boldsymbol{P}$, zastąpimy jedno z równań[25] przez warunek normujący $\sum_{k=1}^{5} P_k = 1$. Wtedy otrzymamy następujący układ równań:

$$\boldsymbol{\Lambda}_1 \cdot \boldsymbol{P}^{\boldsymbol{T}} = \left[1,0,0,0,0,\right]^{\boldsymbol{T}} \tag{14}$$

gdzie

$$\boldsymbol{\Lambda}_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \lambda_1 & -\lambda_2 & \lambda_{32} & 0 & 0 \\ 0 & \lambda_2 & -\lambda_3 - \lambda_{31} - \lambda_{32} & 0 & 0 \\ 0 & 0 & \lambda_3 & -\lambda_4 & \lambda_{54} \\ 0 & 0 & 0 & \lambda_4 & -\lambda_{51} - \lambda_{54} \end{bmatrix} \tag{15}$$

Wyznacznik macierzy (15) $\det \boldsymbol{\Lambda}_1$ przyjmuje postać:

$$\det \boldsymbol{\Lambda}_1 = \lambda_2\lambda_4\left(\lambda_3 + \lambda_{31}\right)\lambda_{51} + \lambda_1\left(\lambda_4\left(\lambda_3 + \lambda_{31} + \lambda_{32}\right)\lambda_{51} + \lambda_2\left(\lambda_4\lambda_{51} + \lambda_3\left(\lambda_4 + \lambda_{51} + \lambda_{54}\right)\right)\right).$$

Jeżeli tylko wyznacznik $\det \boldsymbol{\Lambda}_1$ macierzy współczynników układu (14) ÷ (15) jest różny od zera, to wtedy otrzymujemy następujące rozwiązanie:

$$\boldsymbol{P}^{\boldsymbol{T}} = \frac{1}{\det \Lambda_1}\begin{bmatrix} \lambda_2\lambda_4\left(\lambda_3 + \lambda_{31}\right)\lambda_{51} \\ \lambda_1\lambda_4\left(\lambda_3 + \lambda_{31} + \lambda_{32}\right)\lambda_{51} \\ \lambda_1\lambda_2\lambda_4\lambda_{51} \\ \lambda_1\lambda_2\lambda_3\left(\lambda_{51} + \lambda_{54}\right) \\ \lambda_1\lambda_2\lambda_3\lambda_4 \end{bmatrix} \tag{16}$$

Przyglądając się uważnie we wzorze (16) wektorowi $\boldsymbol{P}^{\boldsymbol{T}}$, łatwo zauważyć, że jeżeli poszczególne intensywności λ_i i λ_{ij} będą wyrażone jako iloczyn $n_{ij}\cdot\lambda$, gdzie

[24] Podobnie $\boldsymbol{Q}^{\boldsymbol{T}}\cdot\boldsymbol{P}^{\boldsymbol{T}} = \boldsymbol{0}$ jest nieoznaczony.

[25] Będzie to pierwszy wiersz macierzy $\boldsymbol{Q}^{\boldsymbol{T}}$.

$\lambda > 0$ jest pewną stałą[26] i $n_{ij} > 0$, to poszczególne składowe wektora $\boldsymbol{P}$ nie będą zależeć od wielkości λ. Zobrazujemy to dwoma przykładami. W pierwszym przyjmiemy, że wszystkie niezerowe intensywności będą równe λ, tzn. $\left(\lambda_k = \lambda\right)_{k=\overline{1,6}}$ oraz $\lambda_{ij} = \lambda$. Wtedy na podstawie wzoru (16) otrzymujemy $\boldsymbol{P} = \left[\frac{2}{9}, \frac{1}{3}, \frac{1}{9}, \frac{2}{9}, \frac{1}{9}\right]$. W drugim przykładzie jeżeli przyjmiemy, że $\lambda_1 = \frac{\lambda}{2}, \lambda_2 = \lambda, \lambda_3 = 2\lambda, \lambda_4 = 3\lambda,\ \lambda_{31} = \frac{\lambda}{4}$, $\lambda_{31} = \frac{\lambda}{4}, \lambda_{32} = \frac{\lambda}{4}, \lambda_{51} = \frac{\lambda}{4}, \lambda_{54} = \frac{\lambda}{4}$, to uzyskujemy $\boldsymbol{P} = \left[\frac{27}{104}, \frac{15}{104}, \frac{3}{52}, \frac{1}{13}, \frac{6}{13}\right]$.

6. Podsumowanie i kierunki dalszych badań

W artykule przedstawiono dwa podstawowe modele: prosty cykl życia ataku cybernetycznego i cykl – z iteracjami, będące wycinkiem prac prowadzonych przez autora. Bardziej interesujące z teoretycznego i praktycznego punktu widzenia są modele cyklu życia ataku cybernetycznego z iteracjami. Iteracje bowiem występują faktycznie nader często w przypadku ponawiania ataków cybernetycznych tuż po zakończeniu wcześniejszego. Pojawiają się po dokonaniu korekty bieżącego ataku i również, gdy przeprowadza się wiele cyklicznie powtarzanych redundantnych wektorów ataków w celu zwielokrotnienia efektu uderzenia i utrudnienia ich analizy. Zatem dalsze prace należy prowadzić nad modelami cykli ataków cybernetycznych z iteracjami, uwzględniając również możliwości pominięcia niektórych faz ataku.

Cyberataki przeprowadzane w ostatnich latach, które były bardziej złożone i destrukcyjne od wcześniejszych, wykorzystywały m.in. nieopublikowane podatności oprogramowania, tzw. „Zero-day". W opinii autora ciekawym kierunkiem badań mogą być stochastyczne modele łączące cykle życia ataku cybernetycznego z cyklami życia podatności oprogramowania[27].

[26] Za stałą λ można przyjąć jedną z intensywności.

[27] R. Hoffmann, *Stochastyczne modele cyklu życia podatności oprogramowania*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2018, z. 49, s. 271–285.

Bibliografia

Coleman K.G.J., *Aggression in Cyberspace*, w: *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, S. Jasper (red.), Georgetown University Press, Washington DC 2012.

Hahn A., Thomas R.K., Lozano I., Cardenas A., *A Multi-layered and Kill-chain Based Security Analysis Framework for Cyber-physical Systems*, „International Journal of Critical Infrastructure Protection" 2015, vol. 11, s. 39–50.

Hoffmann R., *Ogólny cykl życia ataku cybernetycznego i jego markowowski model*, „Ekonomiczne Problemy Usług" 2018, nr 2(131), t. 1, s. 121–130.

Hoffmann R., *Stochastyczne modele cyklu życia podatności oprogramowania*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2018, z. 49, s. 271–285.

Hutchins E.M., Cloppert M.J., Amin R.M., *Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, w: *Leading Issues in Information Warfare and Security Research*, J. Ryan (red.), t. 1", Academic Publishing International Ltd, Reading, UK 2011.

Khan M.S., Siddiqui S., Ferens K., *A Cognitive and Concurrent Cyber Kill Chain Model*, w: *Computer and Network Security Essentials*, K. Daimi, Springer, Cham, Switzerland 2018, s. 585–602.

Kowalenko I.N., Kuzniecow N.J., Szurienkow W.M., *Procesy stochastyczne. Poradnik*, PWN, Warszawa 1989.

Spring J.M., Hatleback E., *Thinking about Intrusion Kill Chains as Mechanisms*, „Journal of Cybersecurity" 2017, vol. 3(3), s. 185–197.

Źródła sieciowe

Dell SecureWorks, *Advanced Threat Protection with Dell SecureWorks Security Services*, Dell 2014, https://www.secureworks.com/~/media/Files/US/Solution %20Briefs/DellSecureWorksNCO346NAdvancedThreatProtection.ashx (dostęp: 14.05.2018).

Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (dostęp: 05.12.2013).

* * *

The Markov models of cyber-attack life cycles

Abstract

Like never before, a better understanding of the nature of cyber-attack processes which are conducted is needed to make informed defensive decisions and actions. Generally, the process by which cyber-attacks are conducted is described as a cyber-attack

lifecycle. The lifecycle is named in military manners as a cyber kill chain as well. Despite of the fact that in their nature cyber-attack processes are stochastic, no models of the lifecycles based on the theory of stochastic processes have been proposed and published practically so far. This work has addressed this deficiency by applying Homogeneous Continuous Time Markov Chain methods to descriptions of observed cyber-attack lifecycles. In this paper two types of models are proposed which have been named as: the simple cyber-attack lifecycle model and the model of cyber-attack lifecycle with iterations.

Keywords: cyber-attack lifecycle with iterations, simple cyber-attack lifecycle, cyber-attack process, cyber kill chain, Homogeneous Continuous Time Markov Chain