Identifikácia fáz útoku v počítačovej sieti

Analýza a návrh riešenia

Bc. Marek Dorko

1Im 2022 – 2023

Abstrakt. Činnosť útočníkov v rámci kybernetických útokov je možné rozdeliť do niekoľkých fáz, resp. krokov. V rámci tomto článku sa bližšie venujeme identifikácie jednotlivých fáz útoku. Podstatná časť článku sa venuje popisom prístupu k jednotlivým fázam útoku. Pre tento popis sa zameriavame na najčastejšie využívané rámce, ako je Cyber kill chain, Mandiant model a Mitre ATT&CK. Súčasne v rámci článku bližšie popisujeme skryté Markovove modely, ktoré predstavujú jeden z možných prístupov, ako riešiť identifikáciu fáz útoku v počítačovej sieti.

Kľúčové slová: kybernetická bezpečnosť, fázy útoku, Mitre ATT&CK, skryté Markovove modely

Úvod

Kybernetické útoky ohrozujú používateľov a organizácie už od vzniku internetu. Spolu s počítačovými sieťami sa však stali oveľa viac zložitejšími. V dnešnej dobe potrebujú útočníci vykonať aj niekoľko krokov, aby dosiahli svoj konečný cieľ. Množinu takýchto krokov označujeme ako viacstupňový útok alebo scenár útoku. Ich viacstupňový charakter bráni detekcii narušenia systému, keďže na pochopenie stratégie útoku a identifikáciu hrozby je potrebná korelácia viac ako jednej akcie. Od začiatku roku 2000 sa komunita výskumníkov v oblasti bezpečnosti pokúsila navrhnúť riešenie na detekciu tohto druhu hrozby a predikovať ďalšie kroky útoku.

Pokročilí útočníci postupujú krok za krokom pri ich pokusoch o vykonanie útoku na systém. Je to hlavne z dôvodu, že obete zvolené útočníkmi sú zvyčajne stredné alebo veľké organizácie so zložitou topológiou siete a rôznymi vrstvami zabezpečenia. Vzhľadom na to, že najdôležitejšie dáta z hľadiska hodnoty informácie sú umiestnené v menej dostupných častiach siete, bolo by viac-menej nemožné uskutočniť úspešný prienik do systému pomocou jednokrokového útoku. Ďalším dôvodom je to, že ak sa útok rozloží na niekoľko krokov, tak je nenápadnejší a ťažšie identifikovateľný obeťou, najmä ak niektoré z krokov sami o sebe nepredstavujú riziko pre systém.

V rámci práce budeme uvažovať o reprezentácii postupu útočníka pomocou MITRE ATT&CK rámca [1]. Tento rámec obsahuje taktiky a v rámci nich jednotlivé techniky. Hlavnou myšlienkou práce je uľahčiť prácu forenznému a inému analytikovi, ktorý dostane k dispozícii údaje z jednotlivých zariadení v rámci počítačovej siete organizácie. Jeho úlohou je rekonštruovať činnosť útočníka. Inými slovami, identifikovať jednotlivé fázy. Táto úloha je reprezentovaná v rámci cieľa práca - navrhnúť a implementovať model identifikácie fáz útoku v počítačovej sieti vrátane vyhodnotenia efektívnosti tohto modelu.

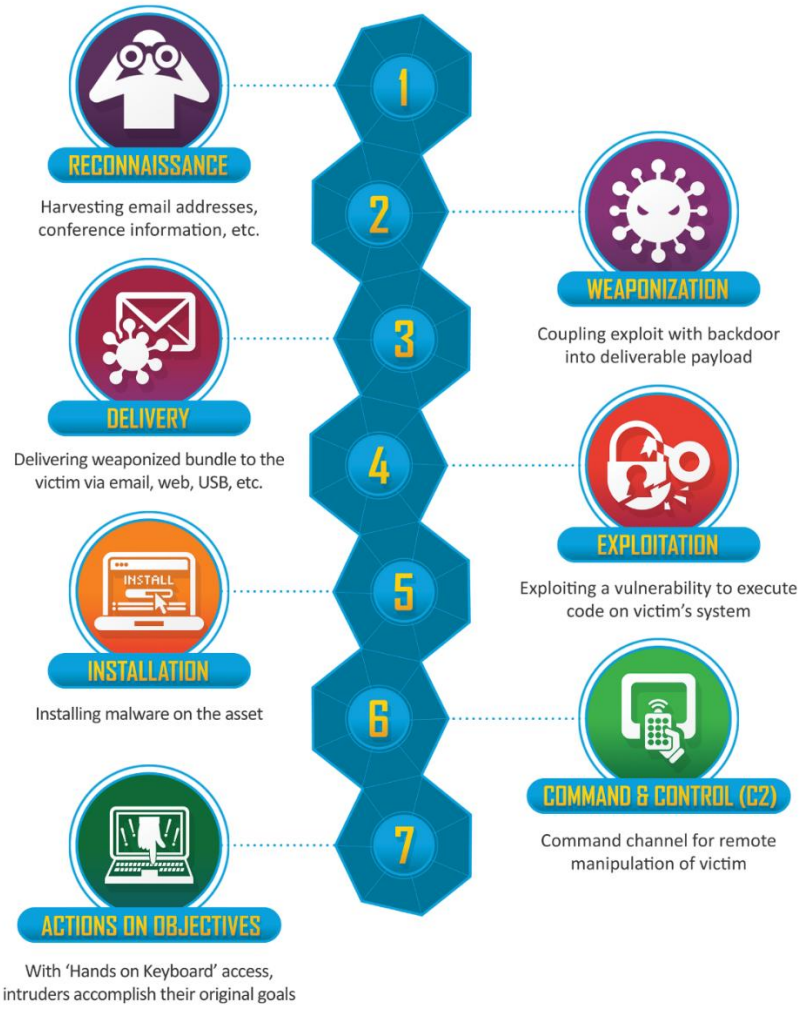
Aby sme vedeli navrhnúť a implementovať vyššie uvedený cieľ, je potrebné analyzovať jednotlivé prístupy k identifikácii fáz útokov v počítačovej sieti. Vyššie sme uviedli jeden z týchto prístupov (MITRE ATT&CK rámec), od ktorého budeme vychádzať. V rámci práce chceme porovnať viacero týchto prístupov (napr. Kill chain model). V tejto práci budeme pracovať s dátami zozbieranými v rámci súťaže Guardians 2021 [2]. Tento dataset predstavuje reálne zozbierané dáta zo stredne veľkej organizácie (vydavateľstvo novín), na ktorú bol odsimulovaných niekoľko útokov vrátane viacstupňových útokov. Dataset obsahuje dáta z koncových staníc, emailového servera, webového servera a ďalších zdrojov. Cieľom práce je prostredníctvom tohto datasetu identifikovať konkrétne digitálne stopy (najmä záznamy), ktoré reprezentujú jednotlivé fázy/kroky útočníka v čase. Zároveň by sme takto chceli zistiť, akú taktiku a techniky spadajúce pod túto taktiku, útočník využil.

1 Modely životného cyklu útoku

Jedným z cieľovej tejto práce je analyzovať prístupy k identifikácii fáz útoku v počítačovej siete. V tejto časti si jednotlivé prístupy bližšie popíšeme.

1.1 Cyber kill chain

Rámec Cyber kill chain, vyvinutý spoločnosťou Lockheed Martin, je súčasťou Intelligence Driven Defense modelu na identifikáciu a prevenciu kybernetických útokov. Model identifikuje, čo všetko musia útočníci splniť, aby dosiahli svoj cieľ. Pozostáva zo siedmich krokov: prieskum, zbrojenie, doručenie, zneužitie, inštalácia, velenie a riadenie a pôsobenie na ciele, ktoré zvyšujú viditeľnosť útoku a umožňujú analytikom lepšie pochopiť taktiky, techniky a postup útočníka. Jednotlivé fázy tohto modelu popisuje nasledujúci obrázok [3].



Obr. 1 Cyber kill chain model

Prvým krokom je prieskum, v ktorom sa primárne zameriava na zhromažďovanie informácií. To môže byť vykonávané na vyhľadávaním na konkrétnom cieli, zbieraním a kompilovaním údajov z online dostupných zdrojov, ako sú napríklad stránky sociálnych sietí.

V tejto fáze je tiež možné zbierať technické údaje spustením skenovania portov na cieľovej webovej lokalite a odhaliť tak potenciálne zastarané bežiace služby. Ďalšou možnosťou ako zozbierať údaje je zvyčajne pomocou phishingových emailov.

Po zozbieraní údajov nasleduje fáza zbrojenia, v ktorej môže útočník vytvoriť potenciálny malvér na základe analýzy zhromaždených dát. Napríklad, ak útočník vie, že v prostredí organizácie beží zraniteľná verzia Adobe Reader, môže vytvoriť malvér, ktorý túto zraniteľnosť bude zneužívať.

Fáza doručenia zvyčajne zahŕňa špeciálne vytvorené phishingové emaily, ktoré sa posielajú konkrétnym zamestnancom v organizácii. Takéto emaily často obsahujú priložené dokumenty programu Word s makrami alebo PDF súbory, ktoré obsahujú vložený odkaz, ktorý presmeruje obete na webové stránky útočníka, následne z ktorých je možné automaticky stiahnuť malvér.

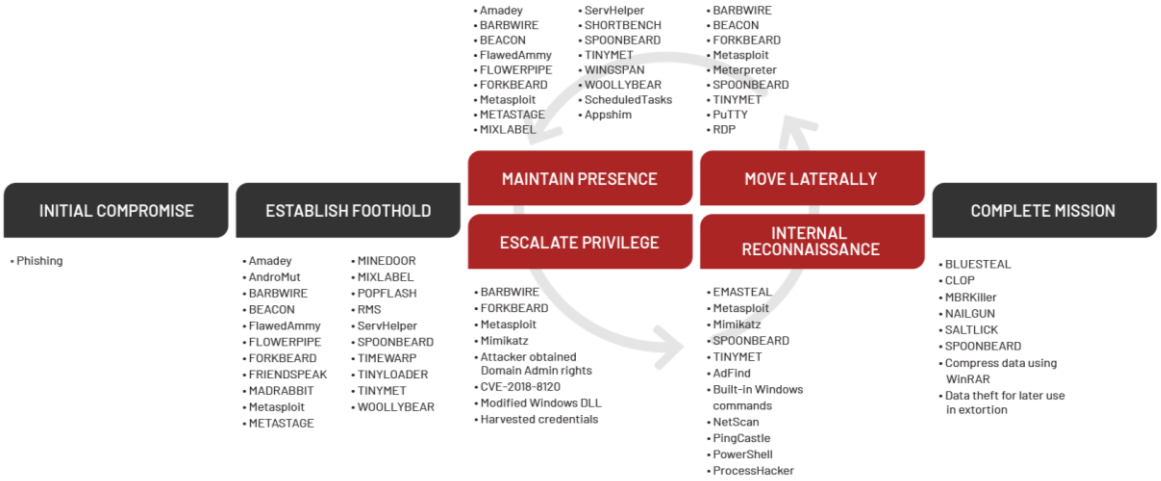
Zneužitie je štvrtou fázou v útočnom cykle a kde sa vypláca fáza zbrojenia. Priložený súbor zvyčajne využije cielenú zraniteľnosť a môže sa pokúšať o stiahnutie ďalšieho softvéru na zariadenie obete pre vytvorenie perzistencie, čo už môžeme hovoriť o fáze inštalácie. Tá zahŕňa aj eskaláciu privilégií, interné skenovania na nájdenie špecifických nainštalovaných aplikácií, vytváranie naplánovaných úloh, registráciu služieb či úpravu registrov na zabezpečenie, že aplikácia prežije reštart zariadenia. Útočníci potom nastavia spojenie so serverom velenia a riadenia (Command and Control), kde budú pokračovať vo svojej činnosti.

Po dokončení týchto šiestich fáz, útočníci prejdú k exfiltrácii údajov na ich servery. Nie je neobvyklé, že útočníci pokračujú vykonaním „bočného“ pohybu (Lateral Movement) s cieľom nájsť ďalšie systémy na kompromitáciu a zopakovať ich fázy znovu.

1.2 Mandiant model

Firma Mandiant pre kybernetickú bezpečnosť vytvorila model životného cyklu útoku, ktorý zahŕňa podrobné fázy o tom, ako fungujú APT (Advanced Persistent Threats) útočníci, resp. skupiny a ako sa pohybujú v sieti s cieľom exfiltrácie údajov. Na účely „lovu“ hrozieb poskytuje jedinečné príklady správania a nástrojov, na ktoré sa APT útočníci spoliehajú pri útoku na cieľ. Mandiant model je znázornený na Obr. 2 [4].

APT skupina [5] je zoskupenie kybernetických útočníkov, ktorí sa zameriavajú na pokročilé pretrvávajúce hrozby. Obvykle ide o ľudí z radov štátnych organizácií alebo organizácií, ktoré pracujú na objednávku štátu. Zameriavajú sa na cielené a sofistikované kybernetické operácie v snahe preniknúť do systémov vysoko postavených cieľov (vládne organizácie, korporácie) a nepozorovane v nich ostať dlhší čas. Účelom je zvyčajne dlhodobá kybernetická špionáž a odcudzenie citlivých údajov. APT skupiny disponujú širokou škálou poznatkov, pokročilými nástrojmi a technikami, vďaka ktorými dokážu zneužívať zero-day zraniteľnosti.



Obr. 2 Mandiant model

Mandiant model začína fázou počiatočnej kompromitácie (initial compromise), v ktorej sa zvyčajne vyskytuje phishingový email so škodlivou prílohou alebo odkazom. V porovnaní s predchádzajúcim modelom (Cyber kill chain), Mandiant model konsoliduje fázy zbrojenie, doručenie, zneužitie a inštalácia do fázy počiatočnej kompromitácie.

Zriadenie opory (establish foothold) je druhou fázou v tomto modeli, ktorá zahŕňa inštaláciu zadných dvierok (backdoor) po tom, čo doručený email bol spustený obeťou. Účelom zadných dvierok je vytvorenie spojenia s koncovým bodom.

Vo fáze eskalácie privilégií (escalate privileges) útočník získava ďalší prístup k podnikovým systémom a dátam. Útočníci často eskalujú svoje privilégiá prostredníctvom získavania poverení, zaznamenávania stlačenia kláves alebo rozvrátenia autentifikačných systémov.

Ďalším krokom je interný prieskum (internal reconnaissance), kde útočník skúma prostredie organizácie, aby lepšie porozumel infraštruktúre, ukladaniu informácií, ktoré ho zaujímajú a rolám a zodpovednostiam kľúčových jednotlivcov. V tomto čase útočníci minimalizujú akékoľvek abnormálne aktivity, a preto využívajú primárne vstavané príkazy operačného systému na preskúmanie kompromitovaných systémov.

Nasleduje fáza „bočný“ pohyb (move laterally), v ktorej útočník používa účty získané v predchádzajúcej fáze a presúva sa na ďalšie systémy v rámci kompromitovaného prostredia. Bežné techniky bočného pohybu zahŕňajú prístup k sieťovým zdieľaným súborom, vzdialené vykonávanie príkazov alebo prístup k systémom prostredníctvom protokolov vzdialeného prihlásenia, ako sú Remote Desktop Services (RDS) alebo Secure Shell (SSH).

Vo fáze udržiavania prítomnosti (maintain presence) útočník zabezpečuje nepretržitý prístup k prostrediu inštaláciou viacerých variantov zadných vrátok alebo prístupom k službám vzdialeného prístupu, ako je napríklad podniková virtuálna privátna sieť (VPN).

Poslednou fázou je dokončenie misie (complete mission), kde útočník dosiahne ciele, ako je krádež duševného vlastníctva, finančných údajov alebo informácií umožňujúcich identifikáciu osôb. V iných prípadoch môže byť cieľom misie narušenie systémov alebo služieb alebo zničenie údajov v prostredí.

Pochopenie krokov, ktoré útočníci podniknú, je dôležité na vytvorenie plánu na predchádzanie takýmto útokom a na zmiernenie rizík.

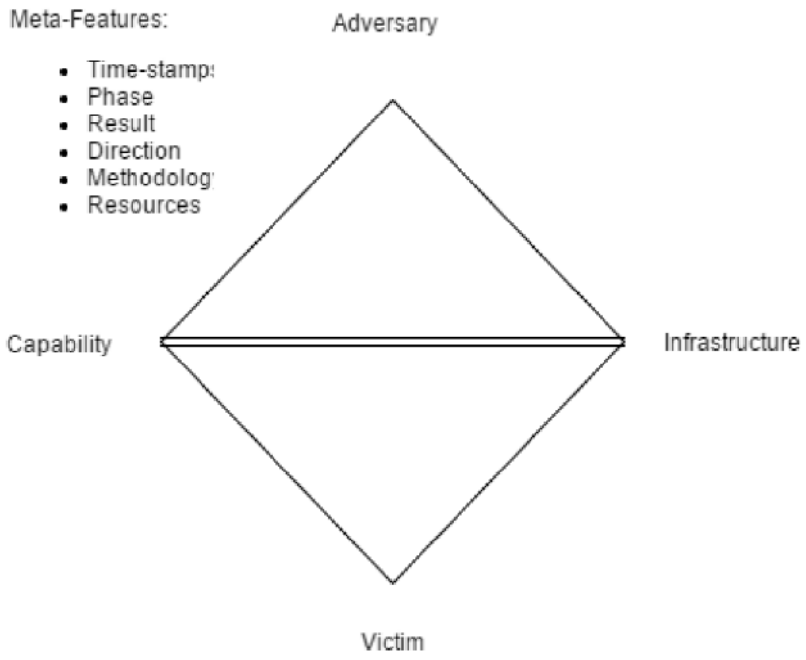
1.3 Diamantový model

Diamantový model [8] je jedným z nových modelov pre analyzovanie narušenia systému, kde útočník útočí na obeť prioritne v závislosti od dvoch kľúčových motivácií, na rozdiel od používania sérii krokov, ako je Kill chain model alebo graf útoku.

Tento model pozostáva zo štyroch základných prvkov, ako sú útočník, infraštruktúra, schopnosti a obeť. Útočník je herec (alebo skupina hercov), ktorí zaútočia na obeť po analýze ich schopnosti proti obeti. Spočiatku útočník začína so žiadnymi znalosťami o schopnostiach obete. Po analýze schopnosti obete, útočník môže zistiť, že on/ona má väčšiu schopnosť ako obeť, a teda či zaútočiť alebo nie. Tento model je dôležitý pri riešení pokročilejších útočníkov

ako sú tí, ktorí už získali určitú kontrolu nad sieťou. Útočník tiež analyzuje infraštruktúru technických a logických schopností veliť a ovládať ktorúkoľvek sieť obete.

Diamantový model môžeme vidieť na nasledujúcom obrázku.



Obr. 3 Diamantový model

1.4 MITRE ATT&CK model

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) [1] je celosvetovo dostupná základňa obsahujúca taktiky a techniky protivníkov. Je založená na pozorovaniach z reálneho sveta. Používa sa ako základ pre vývoj rôznych modelov hrozieb a metodológií v súkromnom sektore, vo vláde a v komunite produktov a služieb kybernetickej bezpečnosti.

ATTA&CK organizuje techniky do súboru taktík, ktoré pomáhajú vysvetliť a poskytnúť kontext pre techniku. Každá technika obsahuje informácie, ktoré sú relevantné pre červený tím (red team) alebo penetračného testera na pochopenie podstaty toho, ako technika funguje a tiež pre obrancu na pochopenie kontextu alebo artefaktov generovaných používanou technikou.

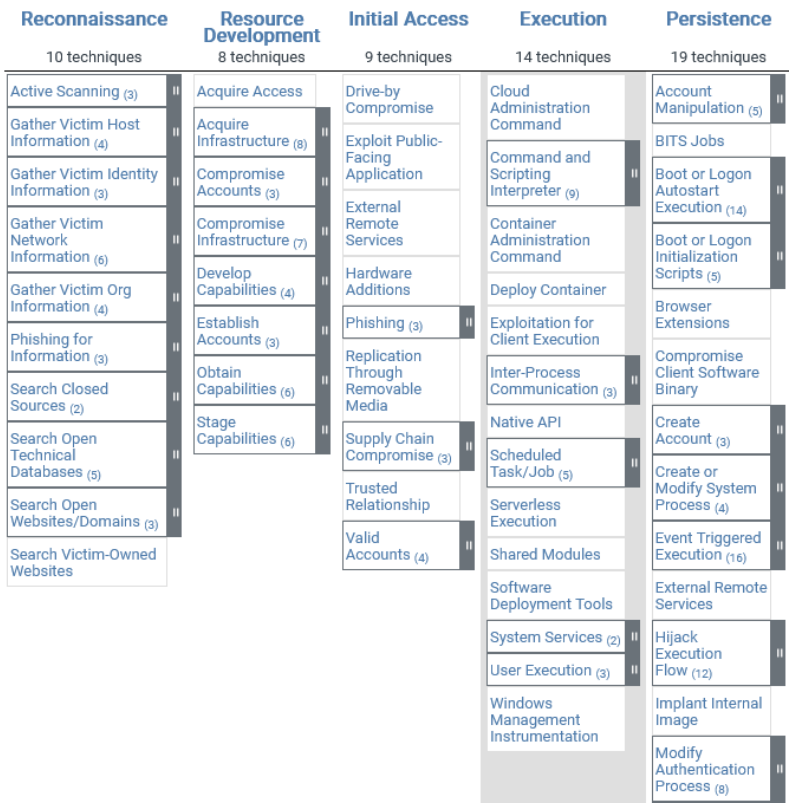
Taktika je taktickým cieľom útočníka. Taktiky slúžia ako užitočné kontextové kategórie pre jednotlivé techniky a pokrývajú štandardné zápisy vyššej úrovne pre veci, ktoré robia

útočníci počas operácie, ako je pretrvávanie, objavovanie informácií, „bočný“ pohyb, spúšťanie súborov a exfiltrácia údajov.

Techniky predstavujú „ako“ útočník dosiahne taktický cieľ vykonaním akcie. Napríklad, útočník môže získať prístupové údaje, aby získal prístup k užitočným prístupovým údajom v rámci siete, ktoré možno neskôr použiť na bočný pohyb. Techniky môžu tiež predstavovať „čo“ útočník získa vykonaním akcie. Spôsobov alebo techník na dosiahnutie taktických cieľov môže byť veľa, takže v každej kategórii taktiky existuje viacero techník.

2.3.1 ATT&CK rámec

Vzťah medzi taktikou a technikami je možné vizualizovať v ATT&CK rámci. Napríklad pod taktikou pretrvávanie (toto je cieľ útočníka – zotrvať v cieľovom prostredí) existuje séria techník vrátane Manipulácia s účtom (Account manipulation), Rozšírenia prehliadača (Browser extensions) či Naplánovaná úloha (Scheduled task/job). Každá z nich je samostatnou technikou, ktorú môžu útočníci použiť na dosiahnutie cieľa vytrvalosti/pretrvávania. Časť ATT&CK matice je možné vidieť na Obr. 3.



Obr. 4 Časť ATT&CK rámca

ATT&CK rámec je pravdepodobne najrozšírenejším aspektom ATT&CK, pretože sa bežne používa na zobrazenie vecí, ako je obranné pokrytie prostredia, detekčné schopnosti v bezpečnostných produktoch, výsledky incidentu a pod. Rámec pozostáva z nasledujúcich štrnástich taktík:

- Prieskum (Reconnaissance),
- Rozvoj zdrojov (Resource Development),
- Počiatočný prístup (Initial Access),
- Spustenie (Execution),
- Pretrvávanie (Persistence),
- Eskalácia privilégií (Privilege Escalation),
- Obranný únik (Defense Evasion),
- Prístup k prihlasovacím údajom (Credential Access),
- Objavenie (Discovery),
- „bočný pohyb“ (Lateral Movement),
- Zbierka (Collection),
- Príkaz a ovládanie (Command and Control),
- Exfiltrácia (Exfiltration),
- Dopad (Impact).

Pri každej technike v rámci ATT&CK rámca je tiež uvedené aké skupiny túto techniku využívajú. Skupiny [6] sú klastre aktivít, ktoré sú v bezpečnostnej komunite sledované pod spoločným názvom. Analytici sledujú tieto klastre pomocou rôznych analytických metodológií a pojmov, ako sú skupiny hrozieb, skupiny činností a aktéri hrozieb. Niektoré skupiny majú viacero mien spojených s podobnými aktivitami, pretože rôzne organizácie sledujú podobné aktivity pod rôznymi názvami. Definície skupín organizáciami sa môžu čiastočne prekrývať so skupinami určenými inými organizáciami a môžu sa nezhodovať v konkrétnej činnosti. Príklad takejto skupiny uvádzame na Obr. 4.

G0073	APT19	Codoso, C0d0so0, Codoso Team, Sunshop Group	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.

Obr. 5 Skupina APT19

Jednotlivé stĺpce predstavujú ID skupiny, názov, pridružené skupiny a popis na čo sa skupina zameriava.

Ďalšou veľmi užitočnou informáciou, ktorá je pri jednotlivých technikách uvedená je softvér [7], ktorý útočníci využívajú. Softvér je rozdelený na:

- Nástroj – komerčný, open-source, verejne dostupný softvér, ktorý by mohol byť použitý obrancom, penetračným testerom alebo útočníkom. Táto kategória zahŕňa softvér, ktorý sa nenachádza v podnikovom systéme, ako aj softvér bežne dostupný ako súčasť operačného systému. Ako príklady takýchto nástrojov môžeme uviesť PsExec, Metasploit, Mimikatz, ako aj nástroje systému Windows, ako sú Net, netstat, Tasklist, atď.
- Malvér – komerčný softvér s vlastným uzavretým zdrojovým kódom alebo aj softvér s otvoreným zdrojovým kódom, ktorý je určený na použitie útočníkmi na škodlivé účely. Príklady takéhoto škodlivého softvéru zahŕňajú PlugX, CHOPSTICK, atď.

Pri technikách sú uvádzané aj zmiernenia. Tie predstavujú bezpečnostné koncepty a triedy technológií, ktoré môžu byť použité na zabránenie úspešnému vykonaniu techniky alebo podtechniky.

2 Návrh riešenia

Dôležitou časťou pri riešení je výber modelu životného cyklu útoku. V predchádzajúcej kapitole sme tieto modely uviedli a ich jednotlivé kroky popísali. Myšlienkou tejto práce je identifikovať podozrivé záznamy v dátach a previesť ich na konkrétne fázy daného modelu. Najvhodnejším sa zdá byť ATT&CK model od neziskovej organizácie MITRE, keďže tento rámec je v bezpečnostnej komunite veľmi používaný a okrem vyššie zmieneného je možné

použiť aj ďalšie nástroje ako napríklad ATT&CK Navigator, v ktorom je možné použité techniky označovať a identifikovať tak napríklad skupinu, ktorá útok vykonala.

Pri analýze podobných prác sme objavili riešenie, ktoré identifikuje fázy útoku pomocou Skrytých Markovových reťazcov, teda metódy strojového učenia. Tie sú založené na pravdepodobnosti. Našim najbližším cieľom je otestovať či riešenie pomocou týchto reťazcov pripadá do úvahy aj v našom prípade, teda na dátach uložených v ElasticSearch databáze a prípadne navrhnúť inú metódu.

2.1 Skrytý Markovov model (Hidden Markov Model – HMM)

Skryté Markovove modely [9] sa vo veľkej miere používajú na určovanie počítačových systémov, ktoré sú pod viacnásobným Multi-Stage Network Attack (MSA), avšak získanie optimálnych parametrov tréningu modelu zostáva výzvou.

Markovove modely fungujú lepšie pre nepozorovateľné stavy a prechody, čím sa eliminuje potreba úplných informácií pri predikcii a detekcii útoku. Markovove reťaze a Hidden Markov Models (HMM) sú dva hlavné príklady Markovových modelov.

V kontexte sieťových útokov je útočná plocha modelovaná na základe Markovovej vlastnosti, ktorá definuje budúci stav ako funkciu len aktuálneho stavu. V praxi HMM vyžaduje dataset na trénovanie.

Skrytý Markovov Model je dvojúrovňový stochastický proces, kde prvá úroveň predstavuje stavy modelovaného systému, ktoré nie sú pozorovateľné. Druhá úroveň predstavuje pozorovania/emisie získané zo systému, čo v sieti môžu byť výstrahy IDS indikujúce stav systému. HMM je bežne reprezentovaný ako trojica (A, B, π), kde A je matica prechodu stavov, B je matica pravdepodobnosti pozorovania a π je počiatočný vektor pravdepodobnosti. Autori v [10, 11] dokonca definujú 6-ticu (Q , V , A, B, π, O). Tri dodatočné parametre sú množina systémových stavov, S, množina odlišných symbolov pozorovania, V a sekvencia pozorovaní, O.

Stručný popis šiestich HMM parametrov:

1. Množina systémových stavov. Je to konečná množina N stavov reprezentovaná ako: S = {s1, s2, . . . , sN }. Stav v čase t je označovaný ako qt

2. Množina odlišných pozorovaní. Množina V obsahuje M odlišných symbolov pozorovania a je daná ako: V = {v1, v2, . . . , vM }

3. Sekvencia pozorovaní O. Táto množina má premenlivú dĺžku T a predstavuje sekvenciu pozorovaní, ktorej prvky patria do množiny symbolov odlišných pozorovaní V. Množina je označená ako:
   O = {o1, o2, . . . , oT }

4. Matica prechodov stavov A. Je to matica rozmeru NxN, v ktorej súčet riadkov je rovný jednej, teda ∑ aij = 1 , ∀ i, j ∈ [1, N].

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ a_{21} & a_{22} & \dots & a_{2N} \\ \dots & \dots & \dots & \dots \\ a_{N1} & a_{N} & \dots & a_{NN} \end{bmatrix}$$

   Každý prvok A, aij označuje pravdepodobnosť prechodu zo stavu, i do j, teda ∀ t ∈ [1, T], aij = P(qt+1 = sj|qt =si).

5. Matica pravdepodobností pozorovaní B. Táto matica má rozmer NxN.
   ∑ bj(vk) = 1, ∀ j ∈ [1, N] a k ∈ [1, M].

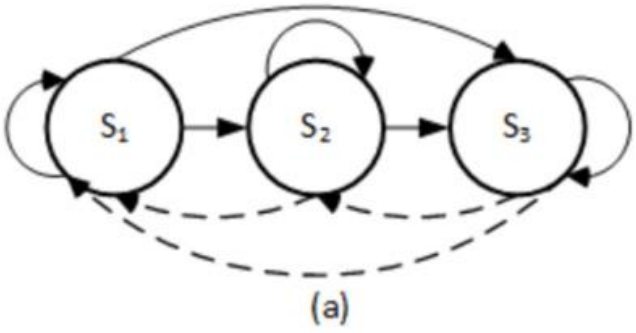
$$B = \begin{bmatrix} b_1(1) & b_1(2) & \dots & b_1(M) \\ b_2(1) & b_1(2) & \dots & b_2(M) \\ \dots & \dots & \dots & \dots \\ b_N(1) & b_N(2) & \dots & b_N(M) \end{bmatrix}$$

   Každý prvok B, bj(vk) označuje pravdepodobnosť pozorovania symbolu vk v stave j, teda ∀t, bj(vk) = P(ot =vk|qt = sj).

6. Vektor pravdepodobností počiatočného stavu π. Toto je reprezentované ako riadková matica pravdepodobností úvodných stavov v čase t=1, napríklad πi = P(q1 = si). Podobne ako A a B, ∑ πi = 1, ∀ i ∈ [1, N].
   π = [π1, π2, . . . , πN]

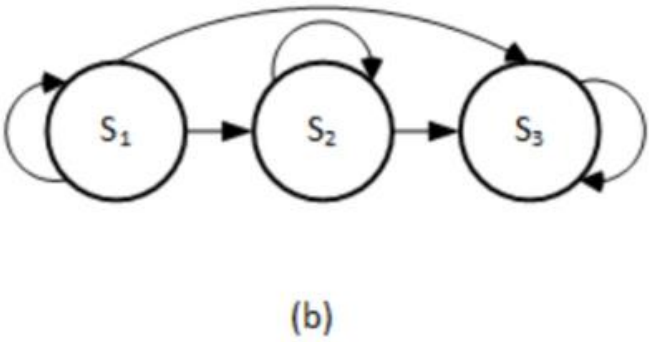
2.1.1 Typy HMM

Vo všeobecnosti existujú dva typy HMM: ergodic a left-right. Autori v [12] definujú ergodic HMM ako plne prepojený HMM, kde každý stav môže prejsť do akéhokoľvek možného stavu ako je znázornené na Obr. 6a. Tento typ sa konkrétne nevzťahuje na MSA, keďže sa len zriedka očakáva, že by útočník kompromitoval, resp. ohrozoval cieľ návratom do predchádzajúceho stavu alebo stavov, a nie pokračovaním smerom k cieľu.



Obr. 6a Ergodic HMM

Left-right typ HMM, znázornený na Obr. 6b, nepovoľuje prechody do predchádzajúcich stavov, čo je typické v MSA. Problém s týmto typom je, že aij = 0, ∀ j < i a nulové hodnoty sú obmedzením pre Baum-Welch algoritmus a Viterbiho implementáciách dekódovania, pretože sa očakáva, že prechod stavu bude 0 < aij ≤ 1. Tento problém možno vyriešiť priradením veľmi malých hodnôt namiesto núl a následne škálovanie každého riadku tak, aby súčet riadku bol rovný nule.



Obr. 6b Left-right HMM

2.1.2 Tri základné problémy HMM

Trénovanie (učenie), dekódovanie a hodnotenie sú tri základné problémy HMM, ako boli pôvodne opísané v [18]. Prvý z nich je najnáročnejším problémom, pretože zohráva kľúčovú úlohu pri definovaní HMM. Nasleduje stručný popis týchto problémov a ako sa bežne riešia:

1. Trénovanie (Učenie): Toto nastaví všetky parametre HMM λ, na maximalizovanie pravdepodobnosti pozorovania P (O|λ). Baum-Welch algoritmus sa najčastejšie používa na riešenie tohto problému.
2. Dekódovanie: Stavy HMM nie sú pozorovateľné; avšak pozorovania, ktoré sú generované v stave, sú evidentné. Problém dekódovania sa snaží nájsť najviac pravdepodobnú cestu stavov (Viterbiho cesta), ktorá môže byť prechodná vzhľadom na sekvenciu pozorovaní O a HMM parametre λ. Na vyriešenie tohto problému sa zvyčajne používa Viterbiho dekódovanie.
3. Hodnotenie: Vzhľadom na HMM je nevyhnutné určiť pravdepodobnosť generovanej pozorovanej sekvencie podľa toho modelu. Dopredné a spätné algoritmy sú bežne používané na túto úlohu.

Záver

V článku sme sa zamerali na analýzu a porovnanie prístupov na identifikáciu fáz útoku. Uviedli sme Cyber kill chain, Mandiant model a napokon ATT&CK rámec a v každom popísali jednotlivé kroky. Načrtli sme základný návrh riešenia pomocou metódy strojového učenia a teda pomocou Skrytých Markovových reťazcov.

Najbližšími krokmi bude otestovanie vhodnosti použitia spomínanej metódy. To môže byť vykonané na testovacích dátach menšieho rozsahu. Ak bude táto metóda použiteľná a dostačujúca, prejdeme na implementáciu na našom datasete.

Použitá literatúra

1. ATT&CK rámec [online]. [cit. 2023-06-23]. Dostupné na: https://attack.mitre.org/
2. Guardians [online]. [cit. 2023-06-23]. Dostupné na: https://www.guardians.sk/

3. Cyber kill chain [online]. [cit. 2023-06-23]. Dostupné na: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

4. Mandiant model [online]. [cit. 2023-06-23]. Dostupné na: https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

5. APT skupina [online]. [cit. 2023-06-23]. Dostupné na: https://www.eset.com/cz/aptskupina/

6. ATT&CK skupiny [online]. [cit. 2023-06-23]. Dostupné na: https://attack.mitre.org/groups/

7. ATT&CK softvér [online]. [cit. 2023-06-23]. Dostupné na: https://attack.mitre.org/software/

8. AL-MOHANNADI, Hamad, et al. Cyber-attack modeling analysis techniques: An overview. In: 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW). IEEE, 2016. p. 69-76.

9. CHADZA, Timothy; KYRIAKOPOULOS, Konstantinos G.; LAMBOTHARAN, Sangarapillai. Analysis of hidden Markov model learning algorithms for the detection and prediction of multi-stage network attacks. Future generation computer systems, 2020, 108: 636-649.

10. THANTHRIGE, Udaya Sampath K.; SAMARABANDU, Jagath; WANG, Xianbin. Intrusion alert prediction using a hidden Markov model. *arXiv preprint arXiv:1610.07276*, 2016.

11. BROGI, Guillaume; BERNARDINO, Elena Di. Hidden Markov models for advanced persistent threats. *International Journal of Security and Networks*, 2019, 14.4: 181-190.

12. SHAWLY, Tawfeeq, et al. Architectures for detecting interleaved multi-stage network attacks using hidden Markov models. *IEEE Transactions on Dependable and Secure Computing*, 2019, 18.5: 2316-2330.