Полювання на здобичників

Threat Hunting – це активний пошук кіберзлочинців у мережі. Якщо вчасно натрапити на їхній слід, можна добряче зекономити на усуненні наслідків.

«Полювання на загрози» – перспективний напрямок, який стає важливою ланкою у побудові кіберзахисту. Threat Hunting є певною мірою відповіддю на цільові атаки (APT), які завжди є складними операціями, що включають тривалу розвідку і підготовку. Замість того, щоб боротися з атаками на їхній фінальній стадії (наприклад, коли відбувається шифрування, виведення даних або руйнування), «мисливці» превентивно шукають ознаки сторонньої присутності. Окрім того, отримані «мисливцями» дані використовуються аналітиками для визначення конкретних загроз і розслідування інцидентів.

Для цього перевіряють як інформацію з мережі, так і розвідувальні дані про нові загрози, отримані з відкритих джерел або спеціалізованими каналами. Тут потрібен досвідчений персонал, що вміє розпізнавати складні атаки: аналітики, які висувають гіпотези, і власне «мисливці», завдання яких полягає у пошуку даних.

Практична модель SANS

Для початку полювання потрібна якась підозра (розуміння того, що щось не так), інакше «мисливець» не зможе взагалі визначити, з чого починати пошуки. За загальноприйнятою практикою, процес починається з висунення гіпотези, наприклад: «чи може атакуюча сторона використовувати якусь нову вразливість?» або «чи не потрапила якась з кінцевих точок під віддалене управління хакерів?». Гіпотеза є певним абстрактним припущенням, яке є основою для подальшого розслідування. Опрацювання гіпотези полягає в обробленні отриманих вже конкретних даних. Наприклад, якщо досліджується припущення про віддалений контроль робочої станції, можна почати з пошуку аномалій у мережевому трафіку, таких як збільшення DNS-запитів з певного комп'ютера. У разі, якщо гіпотеза підтверджується, потрібно встановити факт атаки, визначити її масштаб і можливі наслідки і негайно братися до знешкодження.

Мисливці беруть участь і в подоланні наслідків атаки, визначаючи, як саме відбулося проникнення в мережу (наприклад, через вразливість нульового дня або неправильне налаштування мережевого екрану), чи це окрема атака чи частина більш масштабної кампанії, а також чи є нові індикатори компрометації, які необхідно відстежувати надалі.

Відповідно до формалізованої моделі, розробленої організацією «інститут SANS», яка займається дослідженнями і освітою в галузі кібербезпеки, процес полювання на загрози складається з шістьох етапів (**рис. 1**).

На першому («Мета») визначаються цілі і очікувані наслідки полювання, які може задавати керівництво компанії в рамках більш загальної бізнес-стратегії. Причиною полювання може бути, наприклад, приєднання нової мережі після корпоративного злиття, повідомлення кіберрозвідки про можливу присутність злочинців у мережі або прагнення краще дослідити середовище і впевнитись у його захищеності. Результатом же полювання може бути як виявлення

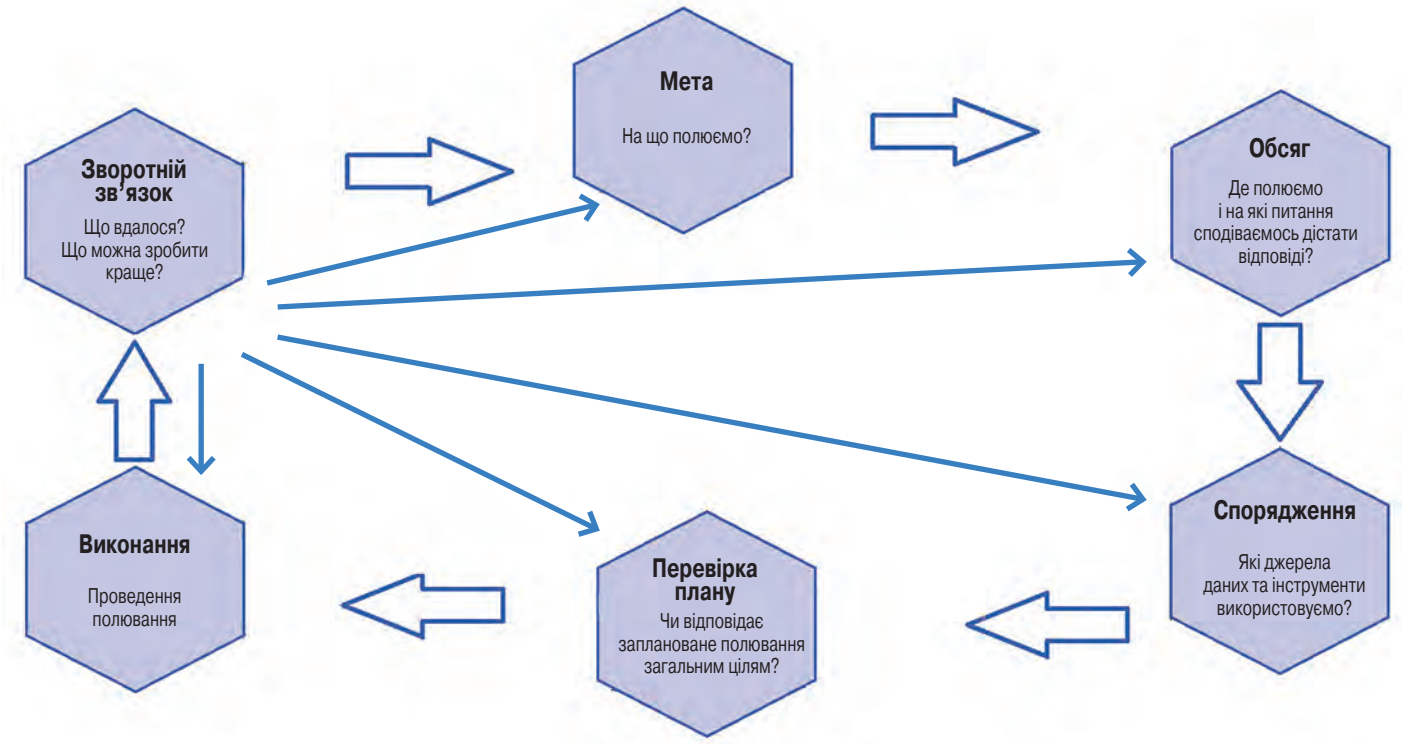

Рис. 1. Модель полювання на загрози інституту SANS

злочинців, так і ідентифікація недоліків у процесах реагування на інциденти.

На другому етапі («Обсяг») формується детальний план пошуку даних, складається перелік мереж та систем, які необхідно перевірити, а також підмереж та комп'ютерів, дані з яких потрібні для успішного пошуку. Після цього формулюють гіпотезу, яка має дати відповіді на аналітичні питання, що визначають напрямок пошуку. Гіпотеза може враховувати наявну інформацію про тактики, техніки і процедури, якими послуговуються злочинці, а також передбачає, які явища можуть спостерігатися у ході пошуку. Гіпотез може бути декілька, кожна для свого напрямку пошуку в рамках однієї визначеної цілі.

Етап спорядження в основному полягає у виробленні детального плану збирання й аналізу даних, а також у визначенні тактик, технік і процедур, за допомогою яких перевірятиметься гіпотеза. Для визначення джерел даних, які можуть допомогти підтвердити або спростувати гіпотезу, враховуються такі характеристики, як розташування джерела, його роль у послідовності атаки (Kill Chain), метод отримання даних, тривалість їх зберігання тощо (наприклад, якщо для аналізу потрібен архів за півроку, а журнали містять дані лише за місяць, таке джерело не є релевантним). При цьому SANS радить не будувати гіпотезу на базі якогось конкретного джерела, оскільки це може призвести до упередженості.

Під час **перевірки плану** менеджер проєкту може доповісти про план полювання власникам бізнесу. Також відбувається виділення потрібних ресурсів. Якщо їх недостатньо, приймається рішення про залучення додаткових (придбання інструментів, наймання працівників ззовні) або ж про перегляд обсягу операції. Також визначається, скільки часу займе полювання – його повинно бути достатньо, щоб накопичити необхідні дані.

Власне **виконання плану** полювання складається з багатьох ітерацій збирання даних і їх аналізу для підтвердження або спростування гіпотези. За потреби залучають інші доступні дані і використовують усі необхідні інструменти аналізу. Після закінчення полювання складають звіт, який містить результати роботи і відповіді на поставлені запитання.

Вкрай важливим є **етап зворотного зв'язку**, коли ставляться питання щодо усіх попередніх етапів. Приміром, чи адекватним був обсяг завдання і чи відповідала гіпотеза меті полювання; чи достатньо було зібраних даних і чи не оминули бува якоїсь важливої інформації (через упередженість або помилки), а також чи були обрані аналітичні засоби достатньо потужними і всеосяжними, щоб підтвердити або спростувати гіпотезу. Оцінювання етапу перевірки визначає, чи було вжито всіх заходів, щоб знайти й виправити недоліки в плані операції, а етапу виконання – чи з достатньою науковою строгістю було використано інструменти аналізу для викриття явищ, пов'язаних з присутністю атакуючої сторони. Уся ця інформація служить для виправлення помилок і вдосконалення процесу полювання у майбутньому.

Полювання на природі

Як може виглядати процес полювання на загрози, також змальовує у своєму документі SANS. Припустимо, керівник з інформаційної безпеки електростанції дає вказівку провести пошук на понижувальних і проміжних підстанціях, мета – виявити присутність групи ELECTRUM, а також визначити, що необхідно придбати для протидії цим злочинцям (саме ця група стояла за

атаками на українські електромережі у 2016 році, тож сценарій не такий вже й абстрактний). На етапі визначення обсягу полювання встановлюються об'єкти, що підлягають тестуванню: система управління та інтерфейси «людина-машина». Провідну роль відіграє інформація про тактики, техніки і процедури ELECTRUM, отримана з каналів даних про загрози (Threat Intelligence) та з відкритих джерел. Відомо, що під час атаки 2016 року злочинці продемонстрували вміння впливати на пристрої, що використовують протокол обміну IEC 60870–5-104. Тому гіпотеза формулюється таким чином: «Якщо ELECTRUM застосовує проти підстанції свій інструмент атаки на IEC 60870–5-104, повинен бути присутній набір ознак, що узгоджується з поведінкою зловмисного ПО CRASHOVERRIDE». Цю гіпотезу можна довести, знаючи, які артефакти полишає по собі дане ПО.

Етап спорядження полягає у визначенні джерел даних, необхідних для підтвердження гіпотези, і найкращого інструментарію для аналізу цих даних. Мережевий трафік можна дослідити, скориставшись якимось комерційним продуктом або й відкритою програмою на кшталт Wireshark. Інший засіб, IDS-система Snort, допоможе у виявленні артефактів виконання CRASHOVERRIDE, а в журналі подій Windows варто пошукати завершення легітимного процесу комунікації і перехоплення контролю над портом з боку модуля зловмисної програми.

На етапі перегляду визначаються додаткові ресурси, необхідні для закриття потреб. Наприклад, винаймають стороннього фахівця з протоколу IEC 60870–5-104. Під час власне виконання плану мисливці збирають дані з журналів подій Windows на всіх машинах, які комунікують за допомогою IEC 60870–5-104, а також з усіх підмереж, де передається відповідний трафік. Мисливці шукають ознаки незвичної поведінки у процесах, пов'язаних з цим протоколом. Аналітики шукають у журнальних даних комп'ютерів і мереж ознаки тактик, технік і процедур, що застосовуються групою ELECTRUM. Після завершення полювання складають звіт, що містить результати роботи і умови, які могли вплинути на чистоту експерименту. Після перегляду результатів полювання приймаються рішення щодо усунення виявлених недоліків процесу – наприклад, розроблення або придбання додаткових інструментів аналізу IEC 60870–5-104.

Що шукати?

ITWorld радить шукати декілька простих ознак, які можуть свідчити по присутність злочинців у мережі і, відповідно, заслуговують на увагу. Серед іншого, це однакові байтові послідовності, які передаються щодня і сигналізують, що ПО встановлено і чекає на команди; сайти, які регулярно відвідує незначна кількість робочих станцій; невдалі спроби входження в облікові записи, які можуть бути ознакою використання раніше вкрадених паролів; спроби входу з використанням облікових даних іншого або неіснуючого користувача (це може свідчити про спроби бічного руху, тобто поширення атаки мережею після успішного проникнення); спроби підвищення привілеїв; популярні програми-завантажувачі вірусів.

В Інтернеті можна зустріти й інші поширені ознаки компрометації. Ними можуть бути, наприклад, незвично великий вихідний трафік, доступ до пошти або корпоративних ресурсів з нехарактерних географічних локацій або обмін даними з країнами, у яких компанія не веде бізнес, дивна поведінка облікових записів з привілеями адміністратора (великий обсяг отриманої або зміненої інформації, доступ до систем, у які раніше з того запису не входили, тощо), різке збільшення активності запитів до бази даних.

Незвичайно великі розміри HTML-відповідей (десятки мегабайтів замість кілобайтів) можуть свідчити про спробу крадіжки даних за допомогою SQL-ін'єкції, а велика кількість запитів – про намагання скористатися якоюсь вразливістю, надсилаючи різні варіанти команд. Якщо програма обмінюється інформацією через незвичний порт, це може бути зв'язок зі злочинним центром управління. Нерідко злочинці змінюють системний реєстр і конфігурацію. Великі обсяги даних, що зберігаються у незвичних місцях (кореневий каталог, сміттєвий кошик тощо), а тим більше заархівовані в форматі, який компанія не використовує, напевне є «посилкою», підготовленою для виведення назовні.

Threat Hinting і Threat Intelligence

Мисливці на загрози, зокрема, послуговуються ідентифікаторами компрометації (IOC). Згідно з визначенням, яке є на сайті інституту Infosec, це «дані, отримані в ході розслідування, зокрема знайдені у системних журналах і файлах, які вказують на можливу діяльність зловмисників у системі або мережі». Іншими словами, це ознаки того, що якась атака вже відбулась або відбувається. Вони можуть свідчити про присутність злочинців у мережі і підготовку до основного етапу атаки (крадіжки даних або руйнування). Поширеними індикаторами компрометації є зловмисні IP-адреси і доменні імена, хеш-суми шкідливих файлів, адреси електронної пошти, імена файлів і бібліотек.

Пошуком індикаторів компрометації займаються, зокрема, розробники рішень у галузі кібербезпеки, які постійно мають справу з атаками і самі відслідковують діяльність угруповань зловмисників, аналізують зразки шкідливого ПО і виявляють тенденції у світі кіберзлочинності. Цей напрямок діяльності зветься Threat Intelligence (кіберрозвідка). Інформація Threat Intelligence видається у вигляді потоків даних (feeds), які містять індикатори компрометації, правила виявлення у популярному форматі формалізованого опису YARA або ж у формі комплексних текстових звітів, що включають у себе опис і обшир злочинної кампанії, аналіз її тактик, технік і процедур.

Для прикладу можна згадати такі відомі дослідницькі підрозділи й сервіси, як ***Cisco Talos***, ***FortiGuard Labs (Fortinet)***, ***Mandiant Threat Intelligence (FireEye)***, ***AutoFocus (Palo Alto Networks)***. Їхні дані розвідки частково доступні у відкритому доступі, решта – як платна підписка.

Існують і цілком відкриті (шерингові) ресурси обміну інформацією Threat Intelligence, наприклад MISP. Окремо

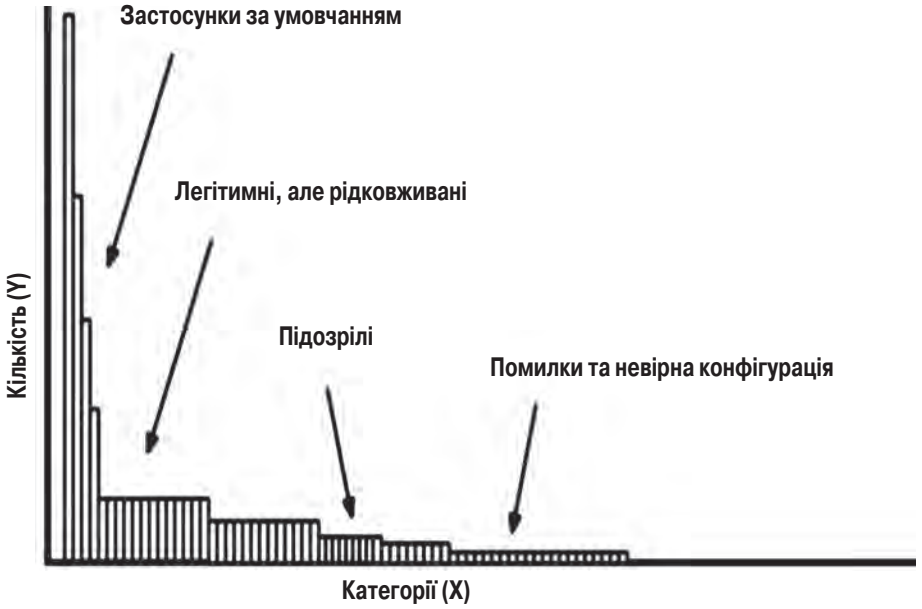

Рис. 2. Приклад результатів Stack Counting (за книгою М. Коллінза)

варто згадати базу знань MITRE ATT&K, яка являє собою структурований перелік відомих тактик і методів зловмисників, розділений на матриці для різних ситуацій. Матриці описують усі етапи атаки і види діяльності зловмисного ПО, як то проникнення, здобуття привілеїв, ухилення від засобів захисту тощо. Також ця інформація доступна у форматах машинного читання STIX та TAXII. До бази MITRE ATT&K автоматично передають дані інструменти безпеки багатьох виробників («пісочниці», SIEM, EDR тощо). Важливо, що обраний поведінковий підхід дозволить у майбутньому описувати нові прийоми зловмисників по мірі того, як ті адаптуватимуться до нових способів захисту.

Зброя і снасті

Щодо самого пошуку даних, то тут є різні методи, починаючи з найпростіших ручних. Майкл Коллінз у своїй книжці Threat Hunting (вона частково опублікована в Інтернеті) наголошує, що, оскільки мисливці на загрози мають справу з доволі нечіткими даними і малозрозумілими явищами, краще зосередитися не на виявленні загроз, а на їх ранжируванні, тобто складанні списку явищ, впорядкованого за ступенем підозрілості. Метою є фіксація підозрілих явищ з одночасним відсіюванням нешкідливих і регулярно повторюваних. Наприклад, якщо відбувається пошук спроб крадіжки даних, то замість критерію «понад 50 ГБ на адресу зі списку» можна скласти список адрес, впорядкований за обсягами даних.

Окрім пошуку даних в журналах, дампах пам'яті, архівах подій тощо, мисливець проводить кореляцію явищ, зафіксованих у різних джерелах. Наприклад, якщо відомо про комунікацію між двома IP-адресами у певний час, варто пошукати інформацію про схожі події деінде. У 9 випадків з 10, пише Коллінз, кореляція даних з різних джерел – процес доволі одноманітний, проте трапляється, що зв'язок виглядає досить непевно, і тут рішення мусить прийняти мисливець.

Для кореляції використовуються різні методи автоматизованої обробки, зазвичай їх три.

Кластерний аналіз – форма машинного навчання без учителя, яка дозволяє знаходити кореляції у великих масивах і виокремлювати кластери подібних даних за заданими характеристиками. Штучний інтелект здатний обробляти терабайти інформації, що для людини може бути надто складно або довго. Кластерний аналіз дозволяє виявляти закономірності й кореляції у непов'язаних між собою даних, а результати надалі служать основою для пошуку загроз. Окрім того, різні алгоритми, застосовані до одного масиву, можуть давати відмінні результати.

Метод групування може застосовуватись після кластеризації для дослідження виявлених підозрілих даних. Цей метод полягає у просіюванні виявлених артефактів через фільтри, що також дозволяє виявляти неочевидні зв'язки між ними.

Пакетний обрахунок (Stack Counting) – це визначення кількості елементів однакового значення (наприклад, виходів в Інтернет з різних браузерів) і виявлення тих, що трапляються рідко, а тому можуть являти собою підозрілі аномалії (**рис. 2**).

Інструменти, які мають стосунок до Threat Hunting, можна розділити на три категорії. По-перше, це системи, які здійснюють моніторинг і збирають інформацію (мережеві екрани, антивіруси тощо). SIEM і SOAR впорядковують «сирі» дані, а засоби аналізу (які й є інструментами полювання у вузькому сенсі) забезпечують кореляцію і візуалізацію отриманих даних і допомагають визначати тенденції.

Infosec радить, щоб аналітичні системи були достатньо потайними та їхня робота залишалася непомітною для злочинців, інакше ті діятимуть ще обережніше і виявити їх стане важче. Також необхідна інтеграція з іншими засобами безпеки – зокрема, з SIEM, щоб можна було одразу прописувати коригуючи дії. Нарешті, аналіз повинен бути автоматизованим, щоб розвантажити аналітиків від одноманітної роботи і підвищити їхню ефективність. До засобів аналізу, наприклад, належать рішення ***IBM i2 Enterprise Insight Analysis***, ***Exabeam threat hunter***, ***Sqrrl Enterprise***, ***VMware Carbon Black Cloud Enterprise EDR*** та інші.

Взагалі ж існує безліч корисних інструментів, які так чи інакше можуть використовуватися у процесі полювання на загрози: програми для одночасного пошуку в різних каналах Threat Intelligence, бази сигнатур, засоби розслідування (digital forensics), програми для виявлення аномальних даних і багато іншого.

Щоб дати цьому всьому раду, потрібен неабиякий хист, але це той випадок, коли краще вкластися в профілактику, аніж в ліквідацію наслідків.

Василь ТКАЧЕНКО, **СиБ**