УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Лекція 10. Цифрова експертиза та аналіз інцидентів

1. Робота з доказами та визначення причетних до атаки.
2. Модель Cyber Kill Chain.
3. Ромбоподібна модель аналізу вторгнень.

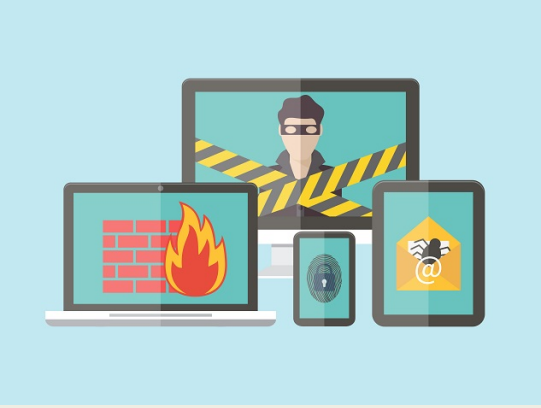
Цифрова експертиза

- Після того, як досліджено та визначено достовірні попередження, що потрібно робити з доказами? Аналітик з кібербезпеки неминуче виявлятиме докази злочинної діяльності. Щоб захистити організацію та запобігти кіберзлочинам, необхідно визначити суб'єкти загрози, повідомити про них відповідним органам та надати докази для підтримки звинувачення.

- Аналітики з кібербезпеки 1-го рівня часто першими виявляють протиправні дії. Аналітики з кібербезпеки повинні знати, як правильно обробляти докази та встановлювати їх взаємозв'язок із суб'єктами загроз.

- **Цифровою експертизою** називається процес відновлення та дослідження знайденої на цифрових пристроях інформації, яка стосується злочинної діяльності. Індикатори компрометації є доказом того, що стався кіберінцидент. Цією інформацією можуть бути дані на пристроях зберігання даних, дані в енергонезалежній пам'яті комп'ютера, або сліди кіберзлочинів можуть зберігатися в мережних даних, наприклад, у файлах pcap та журналах. Важливо, щоб всі індикатори компрометації зберігалися для подальшого аналізу та визначення причетних до атаки.

Цифрова експертиза



- Загалом кіберзлочинну діяльність можна охарактеризувати, як таку, що відбувається всередині або ззовні організації.

- Внутрішні розслідування стосуються осіб всередині організації. Ці особи можуть порушувати користувацькі угоди або здійснювати інші дії некримінального характеру. Коли люди підозрюються у причетності до злочинної діяльності, пов'язаної з крадіжкою або знищенням інтелектуальної власності, організація може залучати правоохоронні органи і у такому випадку розслідування стає відкритим. Внутрішні користувачі також можуть використовувати мережу організації для вчинення інших злочинних дій, які не пов'язані з місією організації, але порушують різні юридичні закони. У цьому випадку слідчі проведуть розслідування.

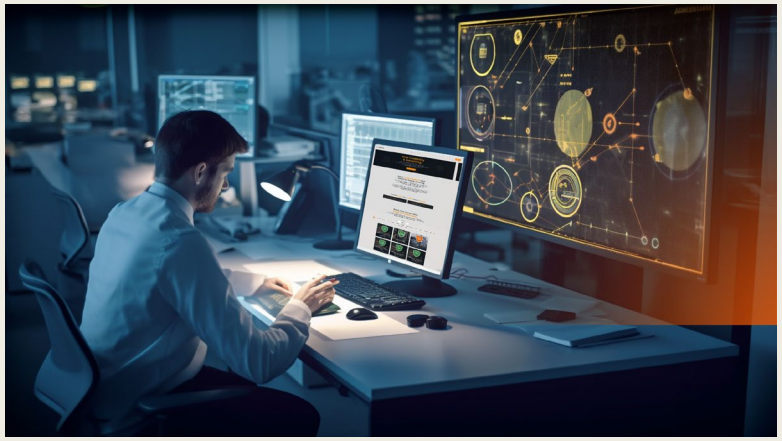
- Коли зловмисник проникає в мережу ззовні та викрадає чи змінює дані, потрібно зібрати докази, щоб задокументувати масштаб проникнення. Різні регулюючі органи визначають низку кроків, які організація повинна виконати у випадку компрометації даних різних типів. Результати експертних досліджень можуть допомогти визначити заходи, які необхідно вжити.

Цифрова експертиза

- Наприклад, згідно HIPAA, якщо виник витік даних, які містять інформацію про пацієнта, то має бути надіслано повідомлення про порушення постраждалим особам. Якщо витік даних стосується більше 500 осіб, то повинні бути сповіщені органи державної юрисдикції, засоби масової інформації, а також постраждалі особи. Необхідно провести цифрову експертизу для визначення кола постраждалих осіб, засвідчити їх кількість для того, щоб можна було зробити належне оповіщення відповідно до правил HIPAA.

- Цілком можливо, що сама організація може стати предметом розслідування. Аналітики з кібербезпеки можуть безпосередньо контактувати із доказами, виявленими під час цифрової експертизи, які детально описують поведінку членів організації. Аналітики повинні знати вимоги щодо зберігання та обробки таких доказів. Невиконання вимог може призвести до застосування кримінального покарання для організації та навіть аналітика з кібербезпеки, якщо буде встановлено намір знищити докази.

HIPAA – це закон, який врегульовує мобільність та підзвітність медичного страхування і встановлює стандарти захисту медичної звітності та особистих медичних даних пацієнтів. HIPAA визначає, які дані пацієнтів захищаються (англ. "protected health information" або "PHI"), а також хто повинен дотримуватись вимог HIPAA при роботі з PHI.

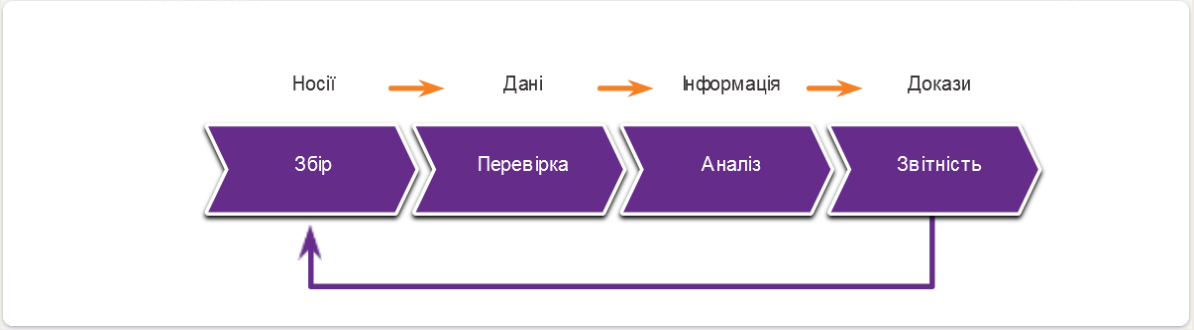


Процес цифрової експертизи

- Важливо, щоб організація розробила належно задокументовані процеси та процедури для проведення цифрової експертизи. Наявність цієї документації може вимагати законодавство, а сама документація може бути перевірена органами влади у випадку публічного розслідування.

- Спеціальна публікація NIST 800-86 (NIST SP 800-86) *«Керівництво з інтеграції методів експертизи у реагування на інциденти» (Guide to Integrating Forensic Techniques into Incident Response)* є цінним ресурсом для організацій, яким необхідні рекомендації щодо розробки планів цифрової експертизи. Наприклад, вона рекомендує проводити експертизу за допомогою чотирьохетапного процесу.

Чотири основні етапи процесу експертизи цифрових доказів



Процес цифрової експертизи

Крок 1 - Збирання: виявлення потенційних джерел даних для експертизи та їх збір, обробка та зберігання. Цей етап є надзвичайно важливим, оскільки потрібно бути особливо обережним, щоб не пошкодити, не втратити чи не пропустити важливі дані.

Крок 2 - Перевірка: передбачає оцінку зібраних даних та добування з них цінної інформації. Може включати розпаковування або розшифровку даних. Інформація, яка не стосується розслідування, може бути видалена. Ідентифікація реальних доказів у великих масивах даних може бути дуже складною та довготривалою.

Крок 3 - Аналіз: передбачає формування висновків на основі вивчених даних. Характерні особливості, такі як: люди, місця, час, події тощо, мають бути задокументовані. Цей крок може також включати кореляцію даних з різних джерел.

Крок 4 - Звітування: передбачає підготовку та подання інформації, яка одержана за результатами аналізу. Звіт повинен бути неупередженим і, якщо доречно, повинні бути запропоновані альтернативні пояснення. Необхідно включити обмеження та проблеми, що виникли під час аналізу. Також слід внести пропозиції щодо подальшого розслідування та наступних кроків.

Типи доказів

У судочинному процесі докази широко класифікуються на ***прямі*** та ***опосередковані***. Прямі докази – це докази, які безперечно перебували в обвинуваченого, або свідчення очевидця, що безпосередньо спостерігав злочинну поведінку.

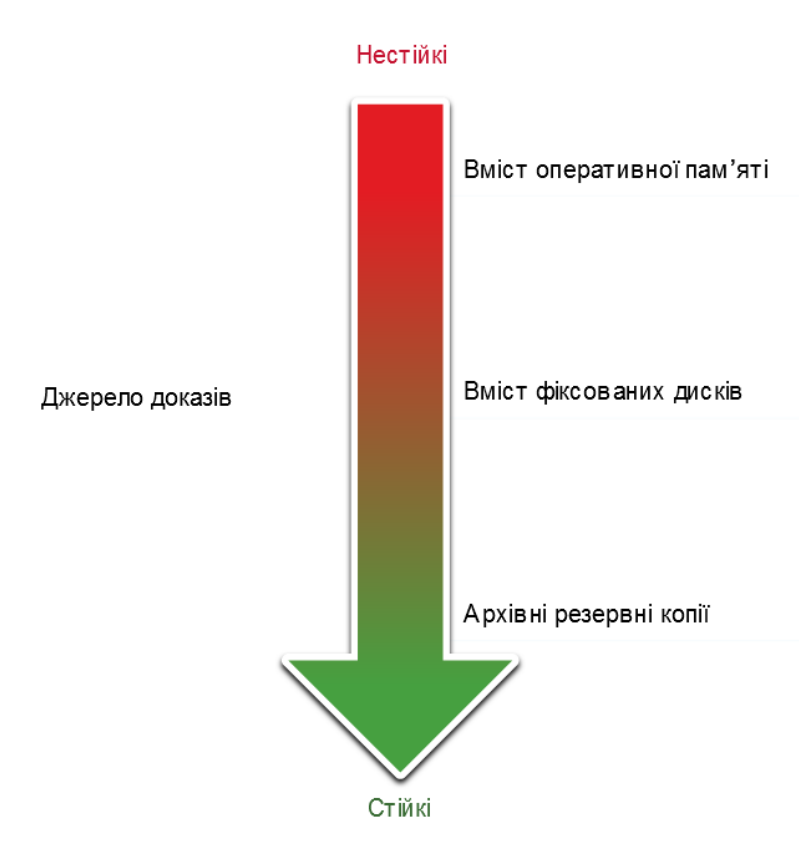
Докази також поділяються на:

- **Найкращі докази (Best evidence):** Це докази, що перебувають у первісному стані. Цими доказами можуть бути пристрої для зберігання, які використовував обвинувачений, або архіви файлів, якщо може бути доведено, що їх не змінювали.

- **Підтверджуючі докази:** це докази, які підтримують твердження, що зроблено на основі найкращих доказів.

- **Опосередковані докази:** це докази, які в поєднанні з іншими фактами формують гіпотезу. Їх також називають непрямими доказами. Наприклад, свідчення про те, що особа вже вчиняла подібні злочини, може підтвердити твердження, що ця особа вчинила злочин, у якому звинувачується.

Послідовність збору доказів



Документ IETF RFC 3227 містить рекомендації для збору цифрових доказів. Цей документ описує послідовність збору цифрових доказів з урахуванням нестабільності даних.

Дані, що зберігаються в оперативній пам'яті, є найбільш нестабільними і вони будуть втрачені під час вимкнення пристрою. Крім того, важливі дані, що знаходяться в енергонезалежній пам'яті, можуть бути перезаписані стандартними процесами, що виконуються на комп'ютері.

Тому збір цифрових доказів повинен починатися з найбільш нестабільних доказів і переходити до найбільш стабільних, як показано на рисунку.

Послідовність збору доказів

Приклад збору доказів від найбільш нестабільних до найбільш стабільних:

- Регістри пам'яті, кеші
- Таблиця маршрутизації, ARP-кеш, таблиця процесів, статистика ядра, оперативна пам'ять
- Тимчасові файли системи
- Енергонезалежні носії, фіксовані та знімні
- Віддалене журналювання і дані моніторингу
- Фізичні взаємозв'язки та топології
- Архівні носії, стрічки або інші резервні копії

Докладні відомості про системи, з яких були зібрані докази, включно з тим, хто має доступ до цих систем і на якому рівні дозволів, повинні бути записані. Такі деталі повинні включати в себе апаратні та програмні конфігурації систем, з яких отримано дані.

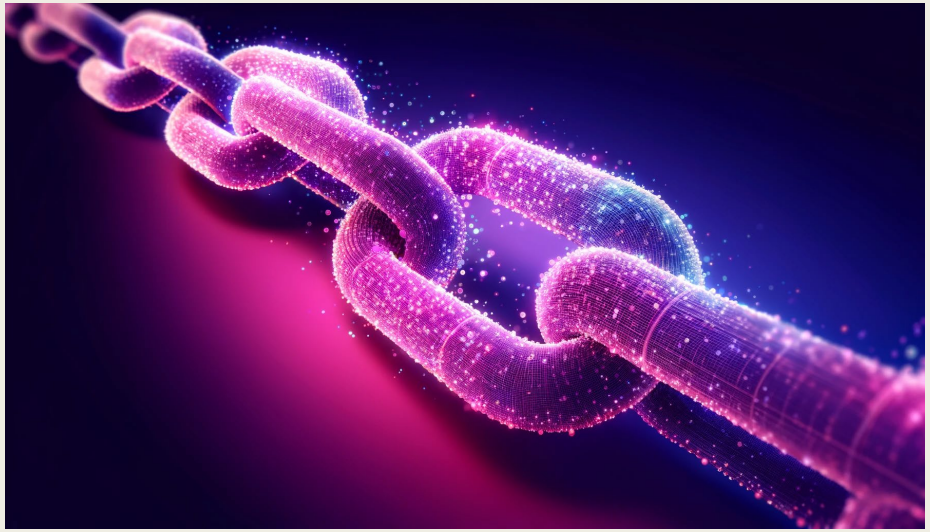
Ланцюг опіки (Chain of Custody)

Хоча докази можуть бути зібрані з джерел, які підтверджують провину обвинуваченої особи, можна стверджувати, що докази могли бути змінені або сфабриковані після їх збору. Щоб спростувати цей аргумент, необхідно визначити і суворо дотримуватися **ланцюга забезпечення збереження доказів** (ланцюга опіки).

Це криміналістична техніка, яка документує частину доказу з моменту його отримання до моменту його знищення. Він забезпечує чіткий запис про те, хто мав до нього доступ, куди і коли його транспортували, а також про будь-які зміни в статусі.

Ланцюг опіки передбачає збір, обробку та безпечне зберігання доказів. Необхідно зберігати детальні записи про наступне:

- Хто виявив і зібрав докази?
- Усі подробиці щодо роботи з доказами, включаючи час, місце та задіяний персонал.
- Хто несе основну відповідальність за докази, коли відповідальність була покладена, і коли вона була змінена?
- Хто має фізичний доступ до доказів під час їх зберігання? Доступ має обмежуватися лише найнеобхіднішим персоналом.



Цілісність та збереження даних

- Під час збору даних важливо зберегти їх у первісному стані. Часові мітки файлів повинні бути збережені. З цієї причини, оригінальні докази повинні бути скопійовані, і аналіз слід проводити ***лише на копіях оригіналу***. Це необхідно для уникнення випадкової втрати чи підміни доказів. Оскільки часові мітки можуть бути частиною доказів, слід уникати відкриття файлів з оригінального носія.

- Процес створення копій доказів, який застосовується під час розслідування, повинен бути записаний. За можливості, копії повинні бути прямими побітовими копіями оригінального носія. Має бути можливість порівняти архівований образ диска і досліджуваний образ диска, щоб можна було визначити, чи було підроблено вміст досліджуваного диска. З цієї причини важливо заархівувати і захистити оригінальний диск, щоб зберегти його в початковому, оригінальному стані.

- Енергозалежна пам'ять може містити кримінальні докази, тому спеціальні інструменти повинні використовуватися для збереження цих доказів, перш ніж пристрій буде вимкнено, а дані втрачені. Користувачі не повинні від'єднувати, відключати або вимикати живлення заражених комп'ютерів, доки співробітники служби безпеки не дадуть вказівку це зробити.

- Дотримання цієї послідовності забезпечить збереження будь-яких доказів правопорушень та виявлення будь-яких показників компрометації.

Визначення причетних до атаки

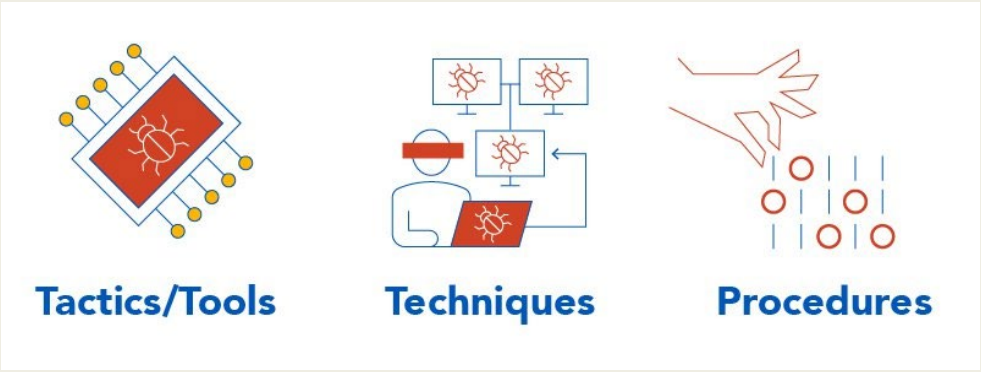
- Після того як масштаб кібератаки був оцінений, зібрано та збережено докази, група реагування на інциденти може перейти до виявлення джерела атаки. Як ми знаємо, існує широкий спектр зловмисників, починаючи від незадоволених осіб, хакерів, кіберзлочинців до кримінальних угрупувань або навіть держав.

- Деякі злочинці діють зсередини мережі, інші можуть знаходитись і в іншій частині світу. Витонченість та складність кіберзлочинів також відрізняється. Держави можуть використовувати великі групи висококваліфікованих фахівців для здійснення нападу та приховування своїх слідів, тоді як інші нападники можуть відкрито вихвалятися своїми злочинними діями.

- **Атрибуція атаки** (threat attribution) – це процес встановлення особи, організації або країни, відповідальної за успішне вторгнення або атаку.

- Встановлення причетних зловмисників має відбуватися шляхом принципового та систематичного вивчення доказів. Можливо корисно буде зробити припущення щодо джерела атаки, шляхом визначення потенційних мотивів інциденту, але важливо не допускати цього упередження під час розслідування. Наприклад, приписування атаки комерційному конкуренту може відвести розслідування далеко в сторону від версії, що можливим ініціатором злочину є кримінальна група або інша держава.

Визначення причетних до атаки



- У розслідуванні, що базується на фактичних доказах, команда реагування на інциденти порівнює **тактику, методи та процедури** (Tactics, Techniques, and Procedures – TTP), які мали місце в інциденті з іншими відомими проникненнями. Кіберзлочинці, як і інші злочинці, мають специфічні ознаки, що характерні для більшості їх злочинів. За допомогою джерел інформації про загрози можна співставити TTP, що ідентифіковані під час розслідування, з відомими джерелами подібних атак.

- Деякі аспекти загрози, які можуть допомогти у визначенні причетних, – це *місцезнаходження вихідних вузлів* або доменів, *особливості коду*, що використовується в шкідливих програмах, *використані інструменти* та інші методи. Іноді на рівні національної безпеки, визначення причетних до атак не можна здійснювати відкрито, оскільки це призведе до виявлення методів та можливостей, які необхідно захистити.

- Для усунення внутрішніх загроз велике значення має **управління ресурсами**. Виявлення пристроїв, з яких було запущено атаку, може безпосередньо визначити нападника. IP-адреса, MAC-адреса та логи DHCP можуть допомогти відстежити адреси, що використовувались під час атаки, і на їх основі визначити відповідний пристрій. Журнали AAA (Authentication, Authorization and Accounting) дуже корисні в цьому відношенні, оскільки вони відстежують, хто, коли і які ресурси мережі переглядав.

База знань MITRE ATT&CK

- Один із способів виявлення причетних до атаки – це моделювання поведінки нападника. База знань тактик, технік та загальновідомих знань про зловмисників **MITRE** (MITRE Adversarial Tactics, Techniques & Common Knowledge – ATT&CK) дозволяє виявляти тактику, методи та процедури (tactics, techniques, and procedures – TTP) зловмисника в рамках захисту від загроз і визначення причетних до атаки.
- Це робиться шляхом відображення кроків атаки на матрицю узагальненої тактики і опису методів, які використовуються в кожній тактиці. Тактика складається з технічних цілей, яких зловмисник повинен досягти для виконання атаки, а технічні методи є засобами, за допомогою яких тактика виконується. Зрештою, процедури – це конкретні дії, що здійснюються зловмисниками в методах, які були виявлені. Процедури – це документально підтверджене реальне використання зловмисниками певних методів.
- База знань MITRE ATT&CK є глобальною базою знань про поведінку зловмисників. Вона базується на спостереженнях і аналізі реальних проникнень з метою опису поведінки зловмисника, а не самої атаки. Вона призначена для автоматизованого обміну інформацією шляхом визначення структури даних для обміну інформацією між спільнотою користувачів і MITRE.

База знань MITRE ATT&CK

- На рисунку показано аналіз експлойта-вимагача у онлайн пісочниці ANY.RUN. У стовпцях матриці вказано тактику і методи атаки на підприємство, які використовувалися зловмисним програмним забезпеченням, що розташовані під стовпцями. Якщо натиснути мишкою на метод, з'явиться докладна інформація про процедури, які використовувалися конкретним екземпляром зловмисного програмного забезпечення, з визначеннями, поясненнями і прикладами техніки.

Модель Cyber Kill Chain

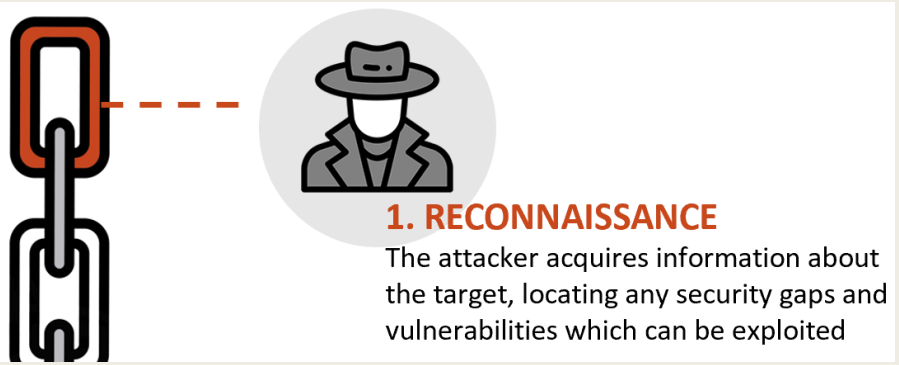
- **Модель Cyber Kill Chain** була розроблена компанією Lockheed Martin для виявлення та запобігання кібервторгненням.
- Модель Cyber Kill Chain складається з семи кроків. Ці кроки допомагають аналітикам зрозуміти методи, інструменти та процедури, які використовують зловмисники.
- Метою реагування на інциденти є виявлення і зупинка атаки на якомога ранніх кроках моделі. Чим раніше атака буде зупинена, тим меншим буде збиток і тим менше зловмисник дізнається про цільову мережу.

Кроки в моделі Cyber Kill Chain

Модель Cyber Kill Chain визначає, які саме дії зловмисник повинен виконати, щоб досягти своєї мети. Кроки, описані в моделі Cyber Kill Chain, показані на рисунку.

Якщо зловмисника буде зупинено на будь-якому з етапів, ланцюжок атаки буде розірвано. Розрив ланцюжка означає, що захисник успішно зірвав загрозу вторгнення нападника. Напад буде успішним тільки тоді, коли зловмисники виконають сьомий крок.

Розвідка



- Розвідка відбувається тоді, коли нападник виконує дослідження, збирає розвідувальні дані і вибирає цілі для нападу. На основі цих даних зловмисник зможе прийняти рішення про початок атаки.

- Будь-яка загальнодоступна інформація може допомогти визначити, коли, де і як можна здійснити атаку. Існує великий обсяг загальнодоступної інформації, особливо у великих організаціях, включно зі статтями в новинах, веб-сайтами, матеріалами конференцій та загальнодоступними мережними пристроями. Постійно зростаючі обсяги інформації про співробітників можна отримати в соціальних мережах.

- Нападник обирає як цілі занедбані або незахищені об'єкти, оскільки ймовірність проникнення в них та їх зламу є вищою. Вся інформація, отримана нападником, аналізується, щоб визначити її важливість та виявити додаткові можливі шляхи атаки.

Розвідка

У таблиці узагальнено деякі тактичні прийоми зловмисників та засоби захисту, які використовуються на етапі розвідки.

Тактика противника	Дії операційного центру безпеки
Планування та проведення дослідження: • Збір поштових адрес • Пошук робітників у соціальних мережах • Збір усієї інформації про зв'язки з громадськістю (прес-релізи, нагороди, відвідування конференцій тощо) • Визначення доступних ззовні серверів • Проведення сканування мережі для визначення IP-адрес та відкритих портів	Визначення намірів зловмисника: • Сповіщення з веб-журналів та історія пошуку • Аналітика даних браузера • Створення посібників з виявлення поведінки, яка вказує на розвідувальну діяльність • Пріоритет захисту технологій та людей, на яких спрямована розвідувальна діяльність

Озброєння

- Метою цього кроку є використання інформації, розвіданої раніше, для розробки зброї проти конкретних цільових систем або окремих осіб в організації. Для розробки цієї зброї проектувальник буде використовувати виявлені вразливості ресурсів і вбудовує їх у інструмент, який можна буде розгорнути.

- Очікується, що після використання інструменту нападник досягне своєї мети – отримає доступ до цільової системи чи мережі, тому працездатність цієї системи (або всієї мережі) знизиться.Нападник буде додатково вивчати мережу та захист ресурсів, щоб виявити додаткові слабкі місця, отримати контроль над іншими ресурсами або розгорнути нові атаки

- Вибрати зброю для нападу не складно. Нападник повинен переглянути, які атаки можна застосувати для виявлених вразливостей. Існує багато атак, які вже були створені та повністю випробувані. Одна з проблем полягає в тому, що оскільки ці атаки настільки добре відомі, вони, швидше за все, також відомі захисникам. Часто більш ефективним є використання атаки нульового дня (zero-day attack), щоб уникнути методів виявлення.

- Атака нульового дня (zero-day attack) використовує зброю, невідому захисникам і мережним системам безпеки. Зловмисник може створити власну зброю, спеціально розроблену для того, щоб уникнути виявлення, використовуючи зібрану інформацію про мережу та системи. Зловмисники навчилися створювати численні варіанти своїх атак, щоб ухилятися від мережного захисту.

Озброєння

У таблиці узагальнено деякі тактики і методи захисту, які використовуються на цьому етапі.

Тактика зловмисника	Дії операційного центру безпеки
Підготовка операції: • Отримання автоматизованого інструменту для доставки шкідливого ПЗ (засіб озброєння). • Обрання або створення документу для надання жертві. • Обрання або створення бекдору та інфраструктури керування та контролю.	Виявлення та збір ознак озброєння: • Правила IDS і сигнатури актуальні. • Проведення повного аналізу шкідливих програм. • Створення способів виявлення поведінки відомих засобів озброєння. • Визначення того, чи зловмисне ПЗ застаріле, готове чи нове, що може свідчити про спеціальну атаку? • Збір файлів та метаданих для майбутнього аналізу. • Визначення, які ознаки засобів озброєння є спільними для яких операцій.

Доставка

- Під час цього кроку зброя передається до цілі за допомогою вектора доставки. Це може бути зроблено завдяки використанню веб-сайту, USB-носія або вкладення електронної пошти. Якщо зброю **не буде доставлено**, то атака завершиться **невдачею**.

- Нападник використовуватиме багато різних методів, щоб збільшити шанси на доставку корисного навантаження, а саме шифрування повідомлень, надання коду вигляду легітимної програми або маскування (обфускація) коду.

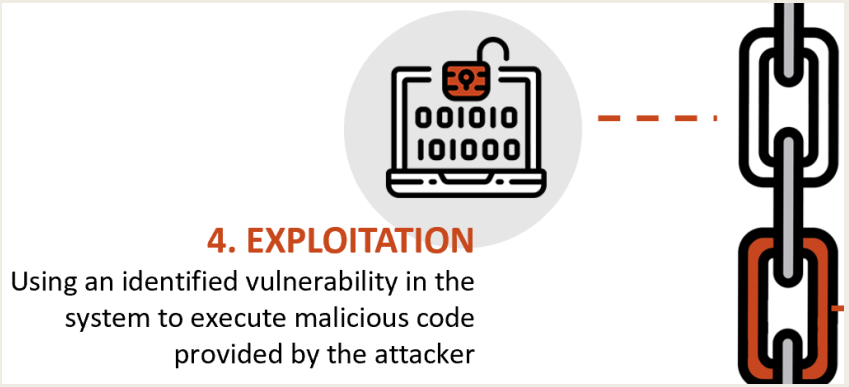
- Сенсори безпеки настільки чутливі, що вони будуть ідентифікувати код як зловмисне ПЗ, якщо в нього не внести зміни, щоб уникнути виявлення. Код може бути змінено таким чином, щоб він виглядав безпечним, але все ж при цьому виконував необхідні дії, навіть якщо це потребує більше часу для виконання.

Доставка

У таблиці узагальнено деякі тактики і методи захисту, які використовуються під час цього кроку.

Тактика зловмисника	Дії операційного центру безпеки
Запуск зловмисного ПЗ на цілі: • Безпосередньо на веб-серверах • Непряма доставка через: ○ Шкідливий електронний лист ○ Зловмисне ПЗ на USB-накопичувачі ○ Взаємодія в соціальних мережах ○ Зламані сайти	Блокування доставки шкідливого програмного забезпечення: • Аналіз шляху до інфраструктури, який використовується для доставки. • Розуміння цільових серверів, людей і даних, доступних для атаки. • Формування висновків про наміри зловмисника на основі націлювання. • Збір електронної пошти та веб-журналів для експертизи та реконструкції.

Проникнення



- Після того як зброя була доставлена, нападник застосовує її для використання вразливості та отримання контролю над ціллю. Найпоширеніші цілі використання експлойту – це застосунки, вразливості операційної системи та користувачі.

- Зловмисник повинен використовувати експлойт, який дасть змогу отримати бажаний для нього ефект. Це дуже важливо, оскільки, якщо проводиться неправильне застосування експлойту, очевидно, що атака не спрацює, а непередбачені побічні ефекти, такі як: DoS або перезавантаження декількох систем, призведуть до надмірної уваги в результаті чого аналітики з кібербезпеки зможуть одержати інформацію про атаку та наміри зловмисника.

Проникнення

У таблиці узагальнено деякі тактики і методи захисту, які використовуються на етапі проникнення

Тактика зловмисника	Дії операційного центру безпеки
Використання вразливості для отримання доступу: • Використання ПЗ, обладнання або вразливості людини • Придбання або розробка експлоіту • Використання ініційованих зловмисником експлоітів для виявлення вразливостей сервера • Використання експлоіту, ініційованого жертвою, як-от відкриття вкладення електронного листа або зловмисного веб-посилання	Навчання співробітників, захист коду і зміцнення захисту пристроїв: • Навчання працівників щодо безпеки та періодичне тестування електронною поштою • Навчання веб-розробника щодо безпечного коду • Регулярне сканування вразливостей і тестування на проникнення • Заходи зміцнення безпеки кінцевої точки • Аудит кінцевої точки для експертизи та визначення походження експлоіту

Встановлення

- На цьому етапі зловмисник встановлює **«чорний хід» (backdoor)** в системі, щоб забезпечити постійний доступ до цілі. Щоб зберегти цей бекдор, важливо, щоб віддалений доступ не привертав увагу аналітиків з кібербезпеки чи користувачів.

- Цей спосіб доступу повинен залишатись непомітним і витримувати сканування програмами виявлення шкідливого ПЗ та перезавантаження комп'ютера, що є необхідним, щоб бекдор запрацював.

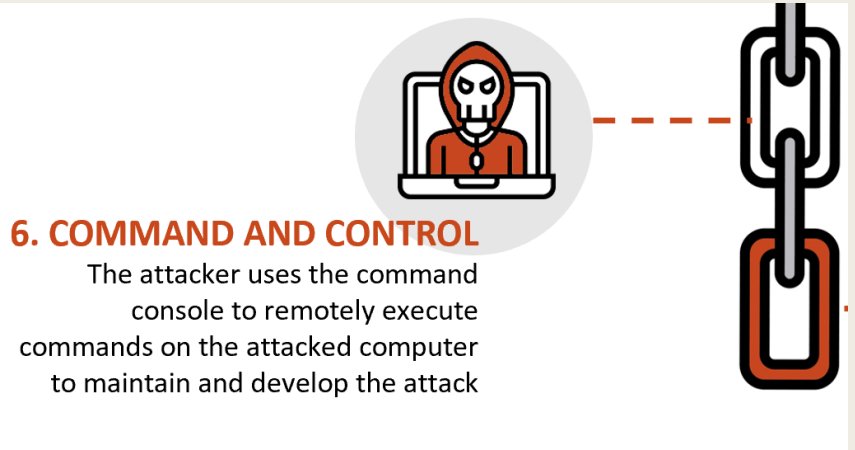
- Цей стійкий доступ також може забезпечити автоматичне з'єднання, що є особливо ефективним, коли під час керуванням ботнетом потрібно декілька каналів зв'язку.

Встановлення

У таблиці узагальнено деякі тактичні прийоми та методи захисту, які використовуються на цьому етапі.

Тактика зловмисника	Дії операційного центру безпеки
Встановлення постійного бекдору: • Встановлення webshell на веб-сервер для постійного доступу. • Збереження стану шляхом додавання служби, ключів автозапуску тощо. • Деякі зловмисники змінюють позначку часу зловмисного ПЗ, щоб воно відображалося як частина операційної системи.	Виявлення, реєстрація та аналіз процесу інсталяції: • HIPS для попередження або блокування загальних шляхів встановлення. • Визначення того, чи зловмисне ПЗ вимагає підвищених привілеїв чи прав користувача. • Проведення аудиту кінцевої точки для виявлення ненормального створення файлів. • Визначення того, чи зловмисне ПЗ є відомою загрозою чи новим варіантом.

Керування та контроль



- **Мета цього кроку** – встановити керування та контроль (CnC або C2) над системою жертви.
- Зламані хости, як правило, підключаються до контролера в Інтернеті. Це пов'язано з тим, що більшість зловмисних програм вимагає ручної взаємодії, щоб отримати дані з мережі.
- CnC канали використовуються нападником для того, щоб посилати команди програмному забезпеченню, яке вони встановили на цільовій системі.
- Аналітик з кібербезпеки повинен мати можливість виявити CnC комунікації, щоб знайти скомпрометований хост.
- Цей канал зв'язку може виглядати як неавторизований трафік Internet Relay Chat (IRC) або надмірний об'єм трафіку до підозрілих доменів.

Керування та контроль

У таблиці узагальнено деякі тактики і методи захисту, які використовуються на цьому кроці.

Тактика зловмисника	Дії операційного центру безпеки
Відкриття каналу для маніпуляції цілями: • Відкриття двостороннього каналу зв'язку з інфраструктурою CnC • Найпоширенішими каналами CnC є канали через Інтернет, DNS та протоколи електронної пошти • Інфраструктура CnC може належати зловмиснику або іншій цільовій мережі	Останній шанс заблокувати операцію: • Дослідження можливих нових інфраструктур CnC • Дослідження інфраструктури CnC за допомогою аналізу зловмисного ПЗ • Ізолювання DNS-трафіку підозрілих DNS-серверів, особливо динамічних DNS • Запобігання загрозі, заблокувавши або вимкнувши канал CnC • Консолідація кількості інтернет-точок присутності • Налаштування правил блокування протоколів CnC на веб-проксі

Дії для досягнення цілей

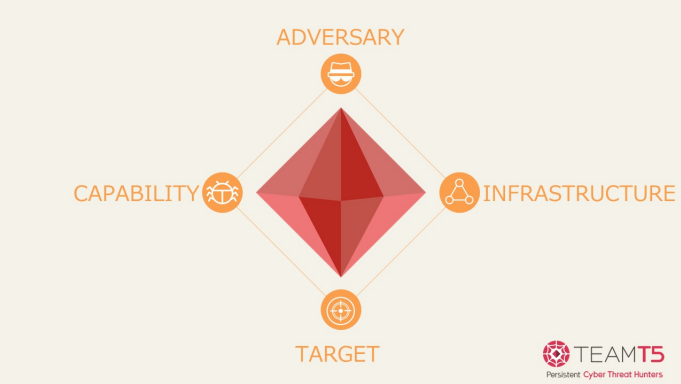
- Останній крок моделі Cyber Kill Chain описує досягнення зловмисником його початкової мети.
- Це може бути крадіжка даних, виконання DDoS-атаки, використання скомпрометованої мережі для створення та відправлення спаму, майнінг криптовалюти.
- На цьому етапі зловмисник вже глибоко вкоренився у системах організації, приховуючи свої дії та замітаючи сліди.
- Надзвичайно важко видалити нападника з мережі.

Дії для досягнення цілей

У таблиці узагальнено деякі тактики і методи захисту, які використовуються під час цього кроку.

Тактика зловмисника	Дії операційного центру безпеки
Отримання плодів успішної атаки: • Збір облікових даних користувачів • Підвищення привілеїв • Внутрішня розвідка • Горизонтальний рух через середовище • Збір і пошук даних • Руйнування системи • Перезапис, зміна або пошкодження даних	Виявлення за допомогою доказів експертизи: • Створення методики реагування на інциденти • Виявлення викрадання даних, горизонтального руху і неавторизованого використання облікових даних • Миттєва реакція аналітика на всі сповіщення • Експертиза кінцевих точок для швидкого сортування • Захоплення мережних пакетів для відтворення активності • Проведення оцінки збитку

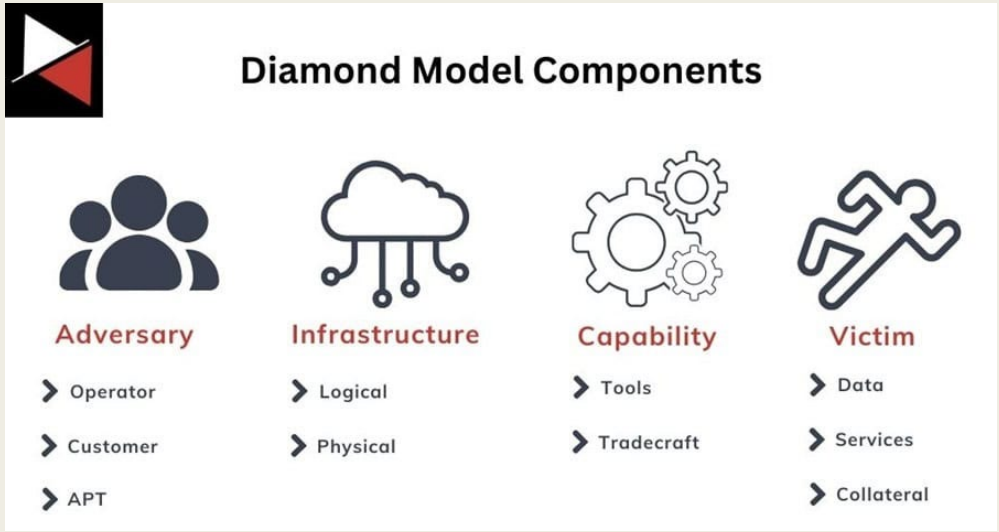
Ромбоподібна модель аналізу вторгнення



Ромбоподібна модель (Diamond Model) аналізу вторгнень складається з чотирьох частин. Модель представляє інцидент або подію безпеки. У ромбоподібній моделі подія є обмеженою за часом дією, яка виконується на певному етапі, на якому зловмисник використовує контроль над певною інфраструктурою проти жертви для досягнення потрібного результату.

Чотири основні характеристики події вторгнення – це зловмисник, можливості, інфраструктура та жертва:

- **Зловмисник:** це сторони, які відповідають за вторгнення.
- **Можливості:** інструмент або техніка, яку зловмисник використовує для атаки на жертву.
- **Інфраструктура:** це шлях у мережі або шляхи, які зловмисники використовують для встановлення та підтримки керування і контролю своїх можливостей.
- **Жертва:** ціль атаки. Проте, жертва може бути ціллю тільки спочатку, а потім використовуватися як частина інфраструктури для проведення інших атак.



Ромбоподібна модель аналізу вторгнення

- Зловмисник використовує можливості через інфраструктуру, щоб атакувати жертву. Модель можна інтерпретувати так: «Зловмисник використовує інфраструктуру для доступу до жертви. Зловмисник розвиває здатність експлуатувати жертву». Наприклад, такі можливості, як шкідливе ПЗ, можуть використовуватися зловмисником для атаки на жертву через електронну пошту.
- Такі моделі, як Attack Kill Chain і матриця MITER ATT&CK, підкреслюють TTP, які спостерігаються під час інциденту, або інфраструктуру, що використовується. Однак їм не вдається з'єднати елементи та отримати тактичну чи стратегічну розвідку. Цілісне уявлення про кіберзагрози Diamond Model дозволяє аналітику краще зрозуміти вторгнення, кампанію атаки або супротивника, переглядаючи вторгнення та показуючи лише ключові індикатори.
- Чотири компоненти, які складають ромбоподібну модель, — противник, можливості, інфраструктура та жертва.
- Кожен із цих компонентів пов'язаний. Наприклад, супротивник розробляє можливість, а потім використовує інфраструктуру для підключення жертви для надання цієї можливості. Відображення даних про вторгнення в кожен компонент розкриває зв'язки між ними. Тоді можна краще зрозуміти вторгнення, ставлячи запитання про залучені компоненти та переходячи між ними, щоб знайти відповіді.

Зловмисник

- Той, хто стоїть за нападом; держава, script kiddie або кіберзлочинець, який здійснив атаку. Можна виділити дві ролі:
  - **Оператор зловмисника** : особа, яка безпосередньо здійснює атаку.
  - **Клієнт-зловмисник** : суб’єкт, який отримує вигоду від здійсненої атаки.
- Зловмисник може виконувати обидві ці ролі або лише одну. Як правило, резонансні кібератаки включають кілька операційних груп: одна для початкового доступу, інша для розробки зловмисного програмного забезпечення, а третя для викрадання даних. Програми-вимагачі прийняли таку структуру, де буде посередник початкового доступу, який надає послугу, банда програм-вимагачів, яка ліцензує своє програмне забезпечення, і афілійована особа, яка фактично виконує атаку.
- Кількість оперативних груп і структура того, хто фактично виконує атаку, можуть швидко ускладнитися. Держави використовуватимуть проксі-групи, банди програм-вимагачів використовуватимуть філії, і межа між урядовими операціями та операціями, санкціонованими урядом, може стати розмитою. Таким чином, зазвичай ефективніше відстежувати клієнта-супротивника, який отримує найбільшу користь від атаки, а не конкретну особу чи використане шкідливе програмне забезпечення.
- Щоб почати, необхідно відстежити присутність в Інтернеті, задіяні облікові записи (електронна пошта, соціальні мережі тощо), а також намір нападу.

Можливості

- Спроможність стосується тактики, прийомів і процедур (TTP), які супротивник використовує для здійснення атаки. Їх можна класифікувати на:
  - *Інструменти :* інструменти злому, зловмисне програмне забезпечення або експлойт, які використовуються під час атаки.
  - *Tradecraft :* методи злому, які використовує супротивник, як-от використання бінарних файлів і сценаріїв живого світу (LOLBAS) або команд, що виконуються в системах. Матриця MITRE ATT&CK добре їх охоплює.
- Зіставляючи можливості ромбоподібної моделі, потрібно зосередитися на деталях. Загальні інструменти чи засоби не дуже корисні, якщо є бажання їх відстежувати. Потрібно зосередитися на даних, які виділяються, як правило, представлені вибором, який зробить зловмисник, включаючи обрані конкретні параметри конфігурації зловмисного програмного забезпечення , використане спеціальне зловмисне програмне забезпечення та нові методи атаки чи параметри командного рядка.

Інфраструктура

- Противник розгортає свої можливості за допомогою інфраструктури. Це все, що він може використати для реалізації своїх можливостей. Інфраструктура може бути фізичною, як-от командно-контрольний (C2) сервер, або логічною, як-от адреса електронної пошти чи обліковий запис служби.
- Зловмисник може використовувати цю інфраструктуру напряму, як-от сервер C2, до якого він підключається під час здійснення своїх атак, або щось, до чого підключається жертва, як-от стороння служба обміну файлами, де дані викрадаються (наприклад, file.io або Pastebin).
- Майже будь-що може бути інфраструктурою, від процесу, який запускає шкідливу DLL, до бейджа, клонованого зловмисником, щоб отримати доступ до цільової будівлі.
- Поширені типи інфраструктури:

  Сервісні облікові записи
  Адреси електронної пошти
  IP-адреси
  Домени
  C2 сервери
  Особи (імена соціальних мереж, номери телефонів, канали Telegram тощо)
  Хмарні сервіси
  Сайти обміну файлами
  Зламані сайти

Жертва

- Жертвою є окрема особа або організація, активи якої зазнали атаки (комп’ютерні системи, мережі, дані тощо). Жертви рідко мають пряме відношення до нападника; натомість вони з’єднані інфраструктурою або можливостями.
- Жертва – це лише засіб досягнення мети для супротивника. Намір суб’єкта загрози полягає в тому, щоб поставити під загрозу конфіденційність, цілісність або доступність даних або послуг, які контролює Жертва. Жертва їм байдужа; вони дбають лише про активи, якими володіє жертва, і про вигоди, які вони можуть отримати від їх експлуатації.
- Також важливо відслідковувати, хто насправді є жертвою нападу. Зловмисник може скомпрометувати постачальника програмного забезпечення, щоб здійснити атаку на ланцюжок поставок проти його справжньої цілі.

Аналітик може використовувати ромбоподібну модель з різних точок зору:

•може прийняти точку зору Жертви та шукати Інфраструктуру чи Можливість, яка пов’язує зловмисника.
•може бути постачальниками інфраструктури та шукати зловмисників, націлених на жертв, використовуючи їхні послуги.
•Може прийняти точку зору зловмисника та використати можливості та інфраструктуру, щоб знайти жертву.

Огляд ромбоподібної моделі

Мета-функції трохи розширюють модель, з включенням в неї таких важливих елементів, як:

- **Часова мітка:** Вказує час початку та закінчення події та є невід'ємною частиною групування зловмисних дій.
- **Фаза:** Є аналогом до кроків у моделі Cyber Kill Chain; зловмисна діяльність містить два або більше кроків (фаз), що виконуються послідовно для досягнення бажаного результату.
- **Результат:** Визначає те, що отримав зловмисник від події. Результати можуть документуватись як одна або декілька з наступних дій: порушено конфіденційність, порушено цілісність, порушено доступність.
- **Напрямок:** Вказує на напрямок події в ромбоподібній моделі. Можливі напрямки: від зловмисника до інфраструктури, від інфраструктури до жертви, від жертви до інфраструктури та від інфраструктури до зловмисника.
- **Методологія:** Використовується для класифікації загального типу подій, таких як сканування портів, фішингу, атаки для доставки контенту, SYN-флуд, тощо.
- **Ресурси:** Це один або декілька зовнішніх ресурсів, що використовуються зловмисником для вторгнення, наприклад, програмне забезпечення, знання зловмисника, інформація (наприклад, ім'я користувача/паролі) та ресурси, що необхідні для здійснення нападу (обладнання, кошти, засоби, доступ до мережі).

Огляд ромбоподібної моделі

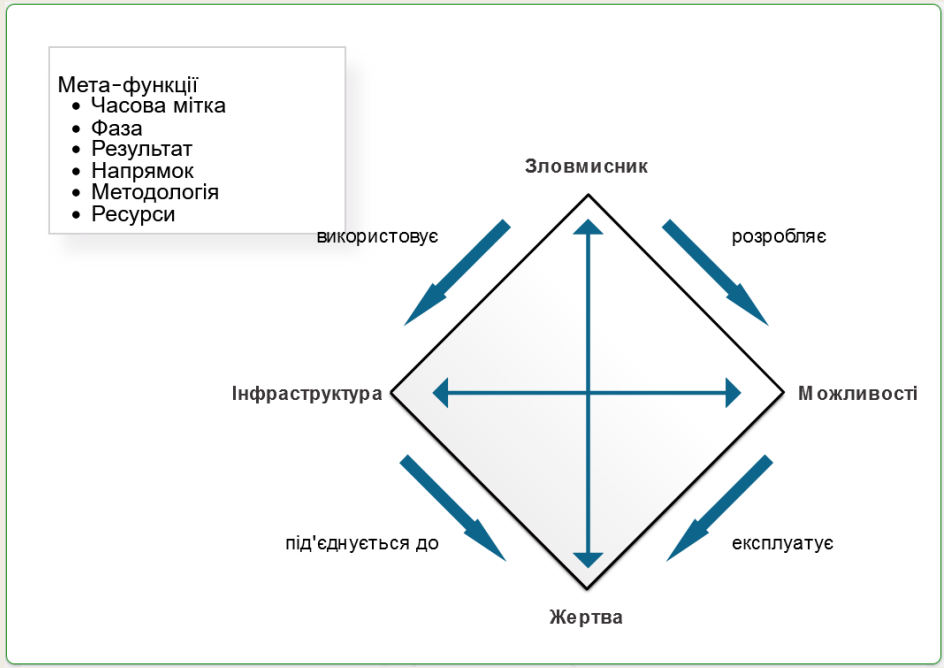
Між цими компонентами також існують різні взаємозв'язки, зокрема:

•**Зловмисник-жертва:** взаємодія між нападником і ціллю. Цей зв'язок стосується таких питань, як, чому зловмисник вибрав цю ціль, а також мотивації та цілі зловмисника.

•**Інфраструктура зловмисника:** зловмисник використовує різні технічні ресурси та активи. Цей зв'язок стосується того, як зловмисник встановлює та підтримує свої кібероперації.

•**Інфраструктура жертви:** підключення цілі до технічних ресурсів зловмисника. Цей зв'язок стосується використання зловмисником різних каналів, методів і векторів проти цілі.

•**Можливості жертви:** зв'язок цілі з інструментами та методами нападника. Цей зв'язок стосується специфічних тактик і сигнатур атаки, що використовуються проти цілі.



Аксіоми ромбоподібної моделі

1. Для кожної події вторгнення існує противник, який робить крок до наміченої мети, використовуючи можливості над інфраструктурою проти жертви, щоб отримати результат

- Це вся основа моделі. Кожна кібератака потребує зловмисника з метою. Ця мета досягається шляхом розробки можливостей (TTP), які надаються жертві через певну форму інфраструктури. Користуючись цією фундаментальною істиною, можна проаналізувати атаку та зробити висновки.

2. Існує набір супротивників (інсайдери, аутсайдери, окремі особи, групи та організації), які прагнуть скомпрометувати комп'ютерні системи чи мережі для реалізації своїх намірів і задоволення своїх потреб

- Десь завжди є зловмисники, які хочуть отримати доступ до ваших даних або вплинути на послуги, які організація надає, з фінансової, політичної чи особистої вигоди. Розуміння намірів супротивника може допомогти розробити стратегії захисту від його атак. Ось чому в кожній атаці є противник.

3. Кожна система і, відповідно, кожен актив жертви, має вразливі місця та ризики

- Усі комп'ютерні системи та мережі мають уразливості, якими може скористатися зловмисник. Потрібно допускати, що всі системи будуть зламані в якийсь момент, незалежно від того, наскільки вони дорогі чи оновлені. Таким чином, потрібно вжити запобіжних заходів, які припускають, що вони будуть порушені, і дозволять захистити критичні активи.

4. Кожна зловмисна діяльність містить дві або більше фаз, які мають бути успішно виконані послідовно для досягнення бажаного результату

- Це пов'язано з ідеєю **Cyber Kill Chain,**, згідно з якою зловмисник повинен виконати кілька кроків, щоб досягти успіху в своїй кібератаці, від початкової розвідки до дій на об'єкті. Якщо припустити, що атака має пройти через ці кроки, то можна виявити та запобігти атаці.

5.Кожна подія вторгнення вимагає, щоб один або більше зовнішніх ресурсів були задіяні перед досягненням успіху

- Це підкреслює, що супротивники не можуть існувати у вакуумі. Для здійснення атаки їм потрібне програмне забезпечення, апаратне забезпечення, доступ до мережі та інші технічні чи фінансові ресурси. Це призводить до ключових компонентів інфраструктури та жертви. Супротивник повинен використовувати інфраструктуру та мати доступ до жертви.

6.Між супротивником і його жертвою (жертвами) завжди існують стосунки, навіть якщо вони віддалені, швидкоплинні чи непрямі

- Суб'єкт загрози завжди націлюється на Жертву з причини. Причина може полягати в тому, що він з'ясував, що вони мають вразливість, якою легко скористатися, після масового сканування в Інтернеті або що вони є конкретною політичною чи фінансовою мішенню.

7.Існує підмножина набору супротивників, які мають мотивацію, ресурси та можливості підтримувати шкідливі наслідки протягом значного періоду часу проти однієї або кількох жертв, одночасно протистоячи зусиллям із пом'якшення. Відносини «супротивник-жертва» в цій підгрупі називаються постійними відносинами «супротивник»

- Це стосується Advanced Persistent Threats (APT). Ці суб'єкти загрози мають необмежені ресурси (час, гроші та люди) для підтримки тривалих операцій проти жертви. Хто це буде, залежатиме від відносин противник-жертва, і те, що супротивник наполегливий проти однієї жертви, не означає, що він наполегливий проти всіх жертв. Хорошим прикладом APT є такі держави, як Сполучені Штати, Китай і Росія, які десятиліттями проводять довгострокові кібероперації одна проти одної.

Переміщення у ромбоподібній моделі

- Ромбоподібна модель може знадобитись аналітику з кібербезпеки для розробки схеми послідовності подій вторгнення. Ромбоподібна модель ідеально підходить для ілюстрації того, як зловмисник переходить від однієї події до іншої.

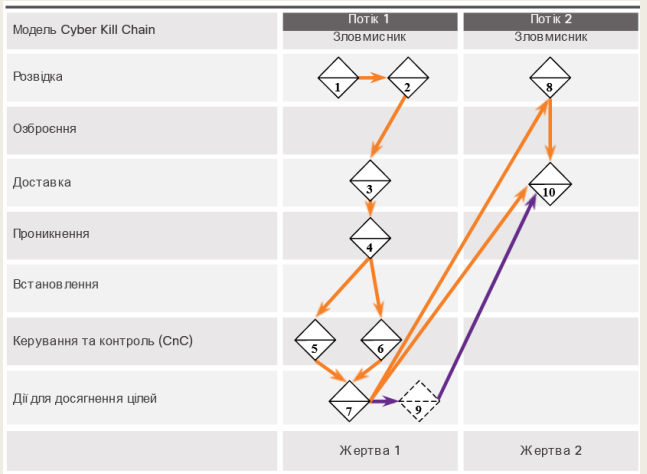
- Наприклад, на рисунку співробітник повідомляє, що його комп'ютер працює аномально.
- Сканування комп'ютера фахівцем з безпеки показує, що комп'ютер заражений шкідливим ПЗ.
- Аналіз зловмисного програмного забезпечення показує, що шкідливе ПЗ містить список доменних імен керування і контролю (CnC).
- З цих доменних імен формується список IP-адрес.
- Потім ці IP-адреси використовуються для ідентифікації зловмисника, а також досліджуються журнали, щоб визначити, чи використовується канал CnC для інших жертв в організації.

Ромбоподібна модель та модель Cyber Kill Chain

Зловмисники не діють лише в рамках однієї події. Навпаки, події з’єднуються послідовно у ланцюжок, де кожна подія повинна бути успішно завершена до настання наступної події. Цей потік подій можна співставити з моделлю Cyber Kill Chain.

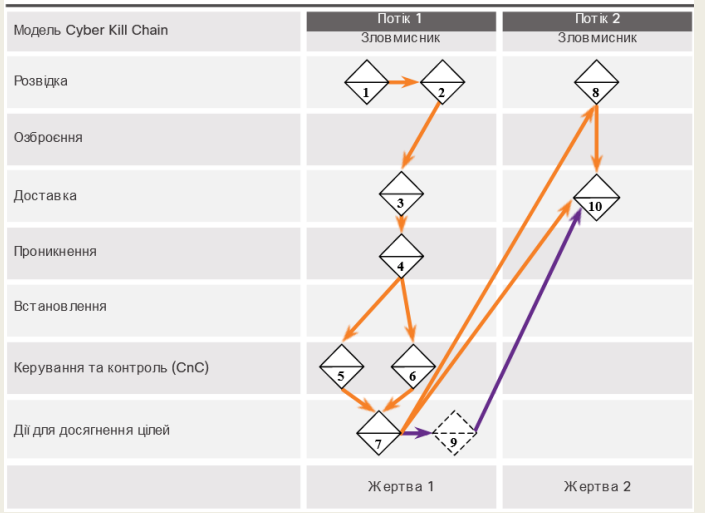
Наступний приклад ілюструє процес дій зловмисника від початку до кінця, у міру того, як він проходить у вертикальному напрямку через етапи моделі Cyber Kill Chain, використовуючи зламаний хост, щоб горизонтально переміститись до іншої жертви, а потім розпочати новий цикл нападу:

1) Зловмисник шукає в Інтернеті компанію-жертву Gadgets, Inc. отримуючи, як частину результатів, домен цієї компанії gadgets.com.
2) Зловмисник використовує виявлений домен gadets.com для нового пошуку «мережний адміністратор gadget.com» і виявляє публікації на форумі від користувачів, які стверджують, що є мережними адміністраторами gadget.com. У профілях цих користувачів вказані адреси їх електронних скриньок.
3) Зловмисник надсилає фішингові електронні листи з приєднаним троянським конем до мережних адміністраторів gadget.com.



Ромбоподібна модель та модель Cyber Kill Chain

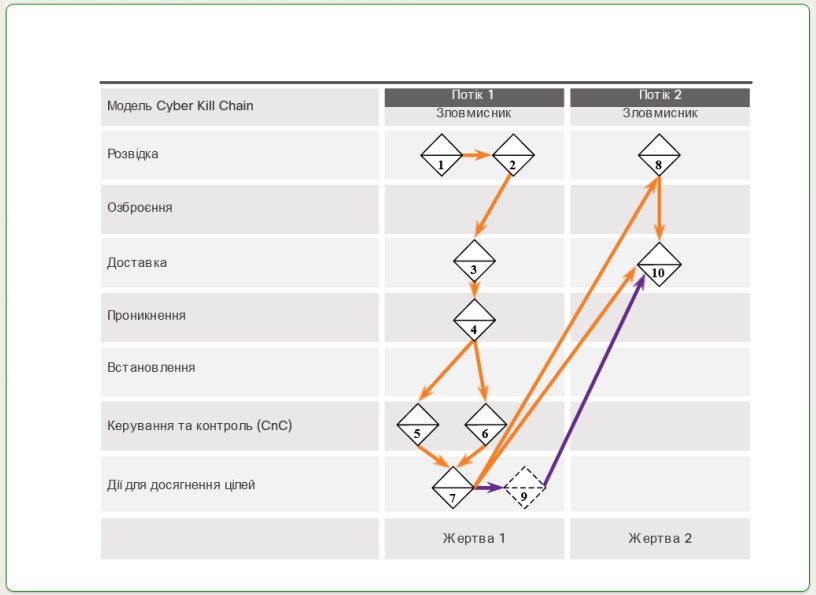
4) Один з мережних адміністраторів (NA1) gadget.com відкриває зловмисне вкладення. Воно виконує вкладений експлойт, що, в результаті, забезпечує виконання зловмисного коду.
5) Зламаний хост NA1 відправляє HTTP Post-повідомлення на IP-адресу, реєструючи його в контролері CnC. Скомпрометований хост NA1 приймає HTTP-відповідь.
6) З реверсивного інжинірінгу виявлено, що зловмисне програмне забезпечення має налаштовані додаткові IP-адреси, які працюють як резервні, якщо перший контролер не відповідає.
7) Через HTTP-відповідь CnC, відправлену на хост NA1, шкідливе ПЗ починає діяти як проксі-сервер для нових TCP-з'єднань.
8) Через інформацію на проксі-сервері, що встановлений на хості NA1, зловмисник виконує пошук за словами «найважливіше дослідження» і знаходить Жертву 2, Interesting Research Inc.
9) Зловмисник перевіряє список контактів електронної пошти NA1 у пошуку контактів від Interesting Research Inc. та знаходить контакт головного наукового співробітника Interested Research Inc.
10) Головний науковий співробітник Interesting Research Inc. отримує електронного листа з поштової адреси NA1 від Gadget Inc., що надходить від хоста NA1 з тим же вкладенням, що й у події 3.



Ромбоподібна модель та модель Cyber Kill Chain

Зловмисник тепер має дві скомпрометовані жертви, з яких можуть бути запущені додаткові атаки. Наприклад, зловмисник міг би переглянути поштові контакти головного наукового співробітника для пошуку додаткових потенційних жертв. Зловмисник також може встановити інший проксі-сервер, щоб отримати доступ до всіх файлів головного наукового співробітника.

Цей приклад є модифікованою версією прикладу, що наведений Міністерством оборони США у публікації «Ромбоподібна модель аналізу вторгнень» (The Diamond Model of Intrusion Analysis).



ВИСНОВКИ

Робота з доказами та визначення причетних до атаки:

- Цифрова експертиза – це відновлення та дослідження інформації, яка знайдена на цифрових пристроях, у тій частині, яка стосується злочинної діяльності.
- Індикатори компрометації є доказом того, що стався інцидент з кібербезпекою.
- Їх необхідно зберегти для подальшого аналізу та визначення причетних до атаки.
- Організація повинна розробити добре задокументовані процеси та процедури для проведення цифрової експертизи.
- Спеціальна публікація NIST 800-86 (NIST SP 800-86) «Керівництво з інтеграції методів експертизи у реагування на інциденти» (Guide to Integrating Forensic Techniques into Incident Response) є цінним ресурсом.
- Процес експертизи включає чотири етапи: збір, перевірка, аналіз та звітність.
- IETF RFC 3227 описує порядок збору цифрових доказів з урахуванням нестабільності даних.
- Ланцюг опіки передбачає збір, обробку та безпечне зберігання доказів.

ВИСНОВКИ

Робота з доказами та визначення причетних до атаки:

- Встановлення причетних зловмисників має відбуватися шляхом принципового та систематичного вивчення доказів.
- У розслідуванні, що базується на фактичних доказах, команда реагування на інциденти порівнює тактику, методи та процедури (Tactics, Techniques, and Procedures – TTP), які мали місце в інциденті з іншими відомими проникненнями.
- За допомогою джерел інформації про загрози можна співставити TTP, що ідентифіковані під час розслідування, з відомими джерелами подібних атак.
- Що стосується внутрішніх загроз, то виявлення пристроїв, з яких було запущено атаку, може призвести безпосередньо до зловмисника.
- Один із способів виявлення причетних до атаки – це моделювання поведінки нападника.
- База знань тактик, технік та загальновідомих знань про зловмисників MITRE (MITRE Adversarial Tactics, Techniques & Common Knowledge – ATT&CK) дозволяє фахівцям з кібербезпеки виявляти тактики, методи та процедури (tactics, techniques, and procedures – TTP) зловмисника в рамках захисту від загроз і визначення причетних до атаки.

ВИСНОВКИ

Модель Cyber Kill Chain:

- Модель Cyber Kill Chain складається з семи кроків.
- Кроки у моделі допомагають аналітикам зрозуміти методи, інструменти та процедури нападників.
- Метою реагування на інциденти є виявлення і зупинка атаки на якомога ранніх кроках моделі.
- Кроками в моделі Cyber Kill Chain є розвідка, озброєння, доставка, проникнення, встановлення, керування і контроль та дії для досягнення цілей.
- Розвідка відбувається тоді, коли нападник виконує дослідження, збирає розвідувальні дані і вибирає цілі для нападу.
- Озброєння – це використання інформації, розвіданої раніше, для розробки зброї проти конкретних цільових систем або окремих осіб в організації.
- Під час доставки зброя передається до цілі за допомогою вектора доставки.

ВИСНОВКИ

Модель Cyber Kill Chain:

- Після того, як зброя була доставлена, нападник використовує її, щоб отримати контроль над ціллю.
- Встановлення – це коли нападник встановлює «чорний хід» (back door) в систему, щоб забезпечити постійний доступ до цілі.
- Щоб зберегти цей бекдор, важливо, щоб віддалений доступ не привертав увагу аналітиків з кібербезпеки чи користувачів.
- Керування та контроль (CnC) – це встановлення контролю нападником над цільовою системою.
- CnC канали використовуються нападником для того, щоб посилати команди програмному забезпеченню, яке вони встановили на цільовій системі.
- Дії для досягнення цілей описують, як нападник досягає своєї початкової мети.
- Це може бути крадіжка даних, виконання DDoS-атаки, використання скомпрометованої мережі для створення та відправлення спаму, майнинг криптовалюти.

ВИСНОВКИ

Ромбоподібна модель аналізу вторгнення:

- Ромбоподібна модель аналізу вторгнення представляє інцидент або подію безпеки.
- Подією є обмежена за часом дія, яка виконується на певному етапі, на якому зловмисник використовує контроль над певною інфраструктурою проти жертви для досягнення потрібного результату.
- Чотири основні характеристики події вторгнення – це зловмисник, можливості, інфраструктура та жертва.
- Мета-функції, які трохи розширюють модель, включають мітку часу, етап, результат, напрямок, методологію та ресурси.
- Ромбоподібна модель може знадобитись аналітику з кібербезпеки для розробки схеми послідовності подій вторгнення.
- Зловмисники не діють лише в рамках однієї події. Навпаки, події з’єднуються послідовно у ланцюжок, де кожна подія повинна бути успішно завершена до настання наступної події.
- Цей потік подій можна співставити з моделлю Cyber Kill Chain.