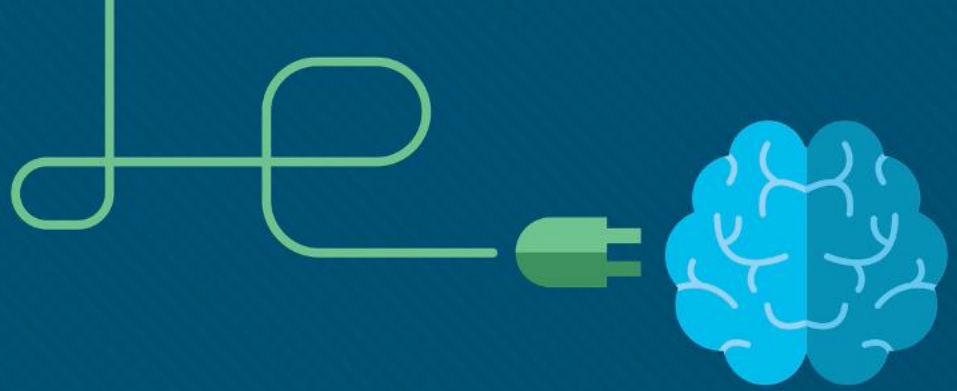

Розділ 2. Атаки, поняття та методи

Вступ до кібербезпеки (I2CS)

Мета розділу

Розділ 2. Атаки, поняття та методи

Мета розділу: Пояснити найпоширеніші кіберзагрози, атаки та вразливості.

Назва теми	Мета вивчення теми
Аналіз кібератаки	Визначити різні типи зловмисного програмного забезпечення та їх симптоми.
Методи проникнення	Описати методи проникнення.
Вразливість системи безпеки та експлойти	Пояснити, як знайти вразливості.
Ландшафт кібербезпеки	Пояснити, як класифікувати вразливості.

2.1 Аналіз кібератаки

Типи шкідливого програмного забезпечення

- Кіберзлочинці використовують багато різних типів шкідливого програмного забезпечення або шкідливих програм для здійснення своєї діяльності. Зловмисне програмне забезпечення - це будь-який код, який може використовуватися для викрадання даних, обходу системи керування доступом, пошкодження або компрометації системи. Знання різних типів і способів їх поширення є ключем до їх стримування та видалення.

Шпигунське ПЗ (Spyware)

- Шпигунське програмне забезпечення відстежує вашу активність в Інтернеті та може реєструвати кожну клавішу, яку ви натискаєте на клавіатурі, а також фіксувати майже будь-які ваші дані, включаючи конфіденційну особисту інформацію, як-от ваші онлайн-банківські реквізити. Воно призначене для відстеження та спостереження за вами. Шпигунське програмне забезпечення робить це, змінюючи налаштування безпеки на ваших пристроях.

- Воно часто поєднується з легальним програмним забезпеченням або троянськими конями.

Типи шкідливого програмного забезпечення (Прод.)

Рекламне ПЗ (Adware):

- Рекламне програмне забезпечення (Adware) часто встановлюється разом із деякими версіями програмного забезпечення і призначене для автоматичної доставки реклами користувачеві, найчастіше у веб-браузері. Ви взнаєте це, коли побачите! Важко ігнорувати, коли ви стикаєтеся з постійною виринаючою рекламою на екрані.
- Зазвичай рекламне ПЗ постачається разом із шпигунським ПЗ.

Чорний хід (Backdoor)

- Цей тип зловмисного програмного забезпечення використовується для отримання несанкціонованого доступу в обхід звичайних процедур автентифікації для доступу до системи. В результаті хакери можуть отримати віддалений доступ до ресурсів застосунку та виконувати віддалені системні команди.
- Чорний хід працює у фоновому режимі, і його важко виявити.

Типи шкідливого програмного забезпечення (Прод.)

Програма-вимагач (Ransomware):

- Програма-вимагач (Ransomware) – це програма, яка призначена для блокування комп'ютерної системи або розміщених у ній даних до моменту отримання викупу. Програмне забезпечення-вимагач зазвичай шифрує вашу інформацію, тому ви не можете отримати до неї доступ.
- Деякі версії програм-вимагачів можуть для блокування системи використати її певні вразливості. Програми-вимагачі часто поширюються через фішингові електронні листи, які спонукають вас завантажити шкідливий вкладений файл, або через уразливість програмного забезпечення.

ПЗ для залякування (Scareware)

- Це тип зловмисного програмного забезпечення (Scareware), який використовує тактику «залякування», щоб обманом змусити вас виконати певну дію. Scareware в основному складається з вікон у стилі операційної системи, які спливають, щоб попередити вас про те, що ваша система знаходиться під загрозою і потребує запуску певної програми, щоб вона повернулася до нормального режиму роботи.
- Якщо ви погоджуєтеся запустити конкретну програму, ваша система буде заражена шкідливим програмним забезпеченням.

Типи шкідливого програмного забезпечення (Прод.)

Руткіт (Rootkit):

- Це шкідливе програмне забезпечення призначене для модифікації операційної системи, щоб створити чорний хід, який зловмисники потім можуть використовувати для віддаленого доступу до вашого комп’ютера. Більшість з них використовують вразливості програмного забезпечення, щоб отримати доступ до ресурсів, які зазвичай не повинні бути доступні (підвищення привілеїв), і змінити системні файли.
- Руткіти також змінюють системні інструменти розслідування та моніторингу, що значно ускладнює виявлення цього зловмисного програмного забезпечення. Якщо руткіт заразив комп'ютер, очистіть його та перевстановіть необхідне програмне забезпечення.

Типи шкідливого програмного забезпечення (Прод.)

Віруси:

- Вірус — це тип комп'ютерної програми, яка під час виконання реплікується та приєднується до інших виконуваних файлів, наприклад документа, шляхом вставки власного коду. Більшість вірусів вимагають взаємодії з кінцевим користувачем для активації і можуть бути написані для спрацьовування в певну дату або час.
- Віруси можуть бути відносно нешкідливими, наприклад ті, які відображають смішне зображення. Або вони можуть бути руйнівними, наприклад, які змінюють або видаляють дані.
- Аби запобігти власному виявленню, віруси також можуть бути запрограмовані на мутацію. Більшість вірусів поширюється через USB-накопичувачі, оптичні диски, мережні ресурси або електронною поштою.

Троянський кінь (Trojan Horse)

- Це шкідливе програмне забезпечення виконує шкідливі операції, маскуючи свій справжній намір. Воно може здатися легальним, але насправді є надзвичайно небезпечним. Трояни експлуатують ваші привілеї користувача і найчастіше зустрічаються у файлах зображень, аудіофайлах або іграх.
- На відміну від вірусів, трояни не само-розмножуються, а діють як приманка для проникнення шкідливого програмного забезпечення минаючи нічого не підозрюючих користувачів.

Типи шкідливого програмного забезпечення (Прод.)

Хробаки (worms):

- Це тип зловмисного програмного забезпечення, яке само-розмножується, щоб поширюватися з одного комп'ютера на інший. На відміну від вірусів, які потребують запуску програм на вузлах, хробаки можуть запускатися самостійно. Крім початкового зараження вузла, вони не вимагають участі користувача і можуть дуже швидко поширюватися по мережі.
- Хробаки мають подібні моделі: вони експлуатують вразливості системи, вони мають спосіб само-розповсюдження, і всі вони містять шкідливий код (корисне навантаження), щоб завдати шкоди комп'ютерним системам або мережам.
- Хробаки спричинили деякі з найруйнівших атак в Інтернеті. У 2001 році хробак Code Red лише за 19 годин інфікував більше ніж 300 тисяч серверів.

Симптоми зараження шкідливим ПЗ

Незалежно від типу шкідливого програмного забезпечення, яким була заражена система, є деякі загальні симптоми, на які слід звернути увагу. До них належать:

- збільшення використання центрального процесора (ЦП), що уповільнює роботу пристрою
- ваш комп’ютер часто зависає або виходить з ладу
- знижується швидкість перегляду веб-сторінок
- виникають незрозумілі проблеми з мережними з'єднаннями
- змінені або видалені файли
- з'являються невідомі файли, програми або піктограми на робочому столі
- запускаються невідомі процеси або сервіси
- програми самостійно припиняють виконання або змінюють свої налаштування
- електронні листи надсилаються без відома та згоди користувача

2.2 Методи проникнення

Соціальна інженерія

- Соціальна інженерія – це маніпулювання особою задля спонукання її до виконання певних дій або розголошення конфіденційної інформації. Соціальні інженери часто використовують бажання людей допомогти іншим, а також їхні слабкості.
- Наприклад, зловмисник зателефонує уповноваженому співробітнику з невідкладною проблемою, яка вимагає негайного доступу до мережі, і звернеться до марнославства чи жадібності співробітника, або буде аргументувати свої повноваження, використовуючи вихваляння зв'язками (name-dropping), щоб отримати цей доступ.

Вигаданий привід (Pretexting)

- Це метод, коли зловмисник телефонує конкретній особі і обманом намагається отримати доступ до привілейованих даних.
- Наприклад, прикидатися, що потрібні особисті чи фінансові дані, щоб підтвердити її особу.

Соціальна інженерія (прод.)

- **Прохід на хвості (tailgating)**
  - Це коли зловмисник швидко слідує за уповноваженою особою в захищене місце розташування.

- **Послуга за послугу (Quid pro quo)**
  - Це коли зловмисник запитує персональну інформацію від особи в обмін на щось, наприклад, подарунок.

Відмова в обслуговуванні (DoS)

Атаки відмови в обслуговуванні (DoS) — це тип мережевої атаки, яку відносно легко може здійснити навіть некваліфікований зловмисник. Результатом DoS-атаки є переривання роботи мережних сервісів для користувачів, пристроїв або застосунків.

Надмірна кількість трафіку

- Це випадок, у якому мережа, вузол або застосунок надсилає величезну кількість даних зі такою швидкістю, що їх неможливо повністю обробити. Це спричиняє затримку передачі чи відповіді, або аварійне завершення роботи пристрою чи сервісу.

Зловмисно сформовані пакети

- Пакет — це набір даних, що передається між джерелом і одержувачем - пристроєм або програмою через мережу, наприклад Інтернет. Якщо зловмисно сформований пакет надсилається одержувачу, той не може його обробити.
- Наприклад, програма не може ідентифікувати пакети, що містять помилки або неналежним чином відформатовані. Це може викликати сповільнення роботи або відмову пристрою-отримувача.

Розподілений DoS

Розподілена DoS атака (DDoS) подібна до атаки DoS, але вона походить від декількох скоординованих джерел. Наприклад:

- Зловмисник будує мережу (Botnet) із інфікованих вузлів, так званих «зомбі» (Zombies), які контролюються системами управління.
- Комп'ютери-зомбі будуть постійно сканувати та заражати все більше вузлів, створюючи все більше і більше зомбі.
- Коли ботнет буде готовий, хакер дасть команду системам керування, щоб зомбі-ботнет розпочав DDoS-атаку.

Ботнет

- Бот-комп'ютер зазвичай заражається в наслідок відвідування веб-сайту, відкривання вкладення електронної пошти або через заражений медіа-файл. Ботнет – це група ботів, з'єднаних через Інтернет, які можуть контролюватися одним зловмисником або групою. У ньому можуть бути десятки тисяч або навіть сотні тисяч ботів, які зазвичай керуються через сервер команд та керування.

- Ці боти можуть активуватися для розповсюдження шкідливого програмного забезпечення, запуску DDoS-атак, розповсюдження спаму через електронну пошту або виконання атаки підбору пароля методом «грубої сили». Кіберзлочинці часто за окрему плату здають в оренду ботнети третім особам для зловмисних цілей.

- Багато організацій, такі як Cisco, примусово пропускають мережний трафік через ботнет-фільтри, щоб визначити розташування ботнету.

Ботнет (прод.)

1. Інфіковані боти намагаються зв'язатися з центром керування в Інтернеті.

2. Фільтр ботнету для Cisco Firewall — це функція, яка виявляє трафік, що надходить від пристроїв, заражених шкідливим кодом ботнету.

3. Хмарна служба Cisco Security Intelligence Operations (SIO) надає оновлені фільтри для міжмережного екрану, які відповідають трафіку з нових відомих ботнетів.

4. Попередження надходять до внутрішньої групи безпеки Cisco, щоб сповістити їх про заражені пристрої, які генерують шкідливий трафік, щоб вони могли запобігти, пом’якшити та виправити це.

Атаки на шляху

- Зловмисники, які атакують дані на шляху перехоплюють або змінюють зв'язок між двома пристроями, такими як веб-браузер і веб-сервер, щоб зібрати інформацію або видавати себе за один із пристроїв.

- Цей тип атаки також називають атакою «людина посередині» або «людина в мобільному».

Людина посередині (Man-in-the-middle)

- Атака MitM відбувається у випадку, коли кіберзлочинець отримує контроль над пристроєм без відома користувача. За допомогою такого рівня доступу зловмисник може перехоплювати та підмінювати інформацію користувача перш ніж передати її одержувачу. Атаки MitM широко використовуються для викрадення фінансової інформації.
- Існує багато типів зловмисного програмного забезпечення, які володіють можливостями атак MitM.

Атаки на шляху (прод.)

Людина в мобільному (Man-in-the-Mobile)

- Варіант атаки «Людина посередині», MitMo – це тип атаки, який використовується для отримання контролю над мобільним пристроєм користувача. Після інфікування мобільний пристрій отримує команду вилучити конфіденційну інформацію користувача та надіслати її зловмисникові. Одним з прикладів зловмисного програмного забезпечення, яке дає змогу реалізовувати атаки типу MitMo, є пакет програм ZeuS. Він дозволяє зловмисникам непомітно перехоплювати надіслані користувачам SMS-повідомлення двофакторної аутентифікації.

Отруєння SEO

- Ви, напевно, чули про пошукову оптимізацію або SEO, яка, простими словами, полягає в покращенні корпоративного веб-сайту, щоб він отримав кращу видимість у результатах пошукових систем.

- Пошукові системи, такі як Google, працюють, подаючи користувачам список веб-сторінок на основі їх пошукового запиту. Ці веб-сторінки сортуються відповідно до релевантності їх вмісту.

- Хоча багато легітимних компаній спеціалізуються на оптимізації веб-сайтів для кращого їх позиціювання, зловмисники користуються перевагами популярних пошукових запитів і використовують SEO, щоб підняти шкідливі сайти вище в результатах пошуку. Ця техніка називається "отруєння SEO".

- Найпоширенішою метою отруєння SEO є збільшення трафіку на шкідливі веб-сайти, які можуть містити зловмисні програми або застосовувати прийоми соціальної інженерії.

Атаки на паролі

Введення імені користувача та пароля є однією з найпопулярніших форм автентифікації на веб-сайті. Таким чином, виявлення вашого пароля є простим способом для кіберзлочинців отримати доступ до вашої найціннішої інформації.

Розпорошення пароля:

- Ця техніка намагається отримати доступ до системи шляхом «розпорошення» кількох часто використовуваних паролів на велику кількість облікових записів. Наприклад, кіберзлочинець використовує "Password123" з багатьма іменами користувачів, перш ніж спробувати ще раз із другим часто використовуваним паролем, таким як "qwerty".
- Ця техніка дозволяє зловмиснику залишатися непоміченим, оскільки він уникає частого блокування облікового запису.

Атаки за словником:

- Хакер систематично пробує кожне слово в словнику або списку часто вживаних слів як пароль, намагаючись зламати захищений паролем обліковий запис.

Атаки на паролі (прод.)

Атаки грубої сили

- Найпростіший і найчастіше використовуваний спосіб отримання доступу до захищеного паролем сайту — атаки грубої сили, які полягають у тому, що зловмисник використовує всі можливі комбінації літер, цифр і символів у просторі для паролів, доки він не впорається.

Атаки веселки

- Паролі в комп'ютерній системі зберігаються не як звичайний текст, а як хешовані значення (числові значення, які однозначно ідентифікують дані). Райдужна таблиця функціонує як розширений словник попередньо обчислених хешів і паролів.
- На відміну від атаки грубої сили, яка має обчислювати кожен хеш, райдужна атака порівнює хеш пароля з тим, що зберігається в таблиці веселки. Коли зловмисник знаходить відповідність, він ідентифікує пароль, використаний для створення хешу.

Атаки на паролі (прод.)

Перехоплення трафіку

- Перехоплюючи повідомлення, інші люди та машини можуть легко прочитати відкритий текст або незашифровані паролі.
- Якщо ви зберігаєте пароль у вигляді чіткого, читабельного тексту, будь-хто, хто має доступ до вашого облікового запису чи пристрою, будь то авторизований чи неавторизований, зможе прочитати його.

Вдосконалені стійкі загрози

- Вдосконалені стійкі загрози (advanced persistent threats, APT) – багатофазні, довготривалі, непомітні та складні дії, спрямовані на конкретну жертву. З цих причин окремому зловмиснику часто не вистачає навичок, ресурсів або наполегливості для виконання APT.

- Через складність і рівень кваліфікації, необхідний для здійснення такої атаки, APT зазвичай добре фінансуються і, як правило, націлені на організації або країни з ділових або політичних причин.

- Їх головна мета — розгорнути налаштовані шкідливі програми в одній або кількох цільових системах та залишатися там непоміченими.

2.3 Вразливості системи безпеки та експлойти

Апаратні вразливості/Meltdown та Spectre

Вразливості апаратного забезпечення часто обумовлені недоліками його проектування.

- Наприклад, тип пам’яті, який називається RAM, в основному складається з безлічі конденсаторів (компонент, який може утримувати електричний заряд), встановлених дуже близько один до одного.
- Однак незабаром було виявлено, що через їхнє близьке розташування, зміни, застосовані до одного з цих конденсаторів, можуть вплинути на сусідні конденсатори.
- На основі цього конструктивного недоліку було створено експлойт Rowhammer. Повторно звертаючись до рядка пам’яті (забиваючи молотком), експлойт Rowhammer викликає електричні перешкоди, які в кінцевому підсумку пошкоджують дані, що зберігаються в ОЗП.

Апаратні вразливості/ Meltdown та Spectre (прод.)

Meltdown і Spectre

- Дослідники безпеки Google виявили Meltdown і Spectre, дві апаратні вразливості, які впливають на майже всі центральні процесори (ЦП), випущені з 1995 року в настільних комп'ютерах, ноутбуках, серверах, смартфонах, розумних пристроях і хмарних сервісах.

- Зловмисники, які експлуатують ці вразливості, можуть прочитати всю пам'ять з даної системи (Meltdown), а також дані, які обробляються іншими програмами (Spectre). Використання вразливостей Meltdown і Spectre називають атаками з боку сторонніх каналів (інформація отримана в результаті впровадження комп'ютерної системи). Вони здатні скомпрометувати великі обсяги даних пам'яті, оскільки атаки можуть бути запущені на систему кілька разів з дуже малою ймовірністю збою або іншої помилки.

Вразливості програмного забезпечення

- Помилки в операційній системі або коді програми зазвичай призводять до **вразливості програмного забезпечення.**

- Уразливість SYNful Knock дозволила зловмисникам отримати контроль над маршрутизаторами корпоративного рівня, такими як застарілі маршрутизатори Cisco ISR, за допомогою яких вони могли контролювати весь мережевий зв’язок та заражати інші мережеві пристрої.

- Ця вразливість з'являлась у системі, після встановлення на маршрутизаторах модифікованої версії IOS. Щоб уникнути такої ситуації, завжди перевіряйте цілісність завантаженого образу IOS та надавайте фізичний доступ до обладнання тільки авторизованому персоналу.

Категоризація вразливостей програмного забезпечення

Більшість вразливостей програмного забезпечення поділяються на кілька основних категорій.

Переповнення буфера (Buffer Overflow):

- Буфери – це області оперативної пам'яті, які виділяються для роботи кожному застосунку. Ця вразливість виникає, коли дані записуються за межами буфера. Змінюючи дані за межами буфера, застосунок отримує доступ до оперативної пам'яті, яка була виділена для інших процесів. Це може спричинити крах системи, компрометацію даних або отримання повноважень більш високого рівня.

Категоризація вразливостей програмного забезпечення (прод.)

Відсутність перевірки введення даних:

- Програми часто вимагають введення даних, але ці вхідні дані можуть містити шкідливий вміст, призначений для того, щоб змусити програму вести себе непередбачувано.
- Наприклад, розглянемо програму, яка отримує зображення для обробки. Зловмисник може створити файл зображення із некоректними розмірами. Некорректні розміри можуть примусити програму виділити буфери неправильних та неочікуваних розмірів.

Перегони:

- Ця вразливість описує ситуацію, коли результат події залежить від того, в якій послідовності, або ж з якою тривалістю виконуються інструкції. Стан перегонів стає джерелом вразливості, коли події, які вимагають впорядкування або часової синхронізації, не відбуваються у правильному порядку або не вкладаються у належні часові межі.

Категоризація вразливостей програмного забезпечення (прод.)

Недоліки реалізації системи безпеки:

- Захист важливих даних за допомогою аутентифікації, авторизації та шифрування Розробники повинні використовувати методи безпеки та бібліотеки, які вже були створені, протестовані та перевірені, і не повинні намагатися створювати власні алгоритми безпеки. Імовірно, це може внести нові вразливості.

Проблеми контролю доступу:

- Контроль доступу — це процес контролю того, хто що робить, і варіюється від керування фізичним доступом до обладнання до визначення того, хто має доступ до ресурсу, наприклад файлу, і що вони можуть з ним робити, наприклад, читати чи змінювати файл. Багато вразливостей безпеки з'являється через неправильне використання засобів контролю доступу.
- Майже всі засоби контролю доступу та заходи безпеки можна обійти, якщо зловмисник має фізичний доступ до цільового обладнання. Наприклад, незалежно від налаштувань дозволу на файл, хакер може обійти операційну систему і прочитати дані безпосередньо з диска.

Оновлення ОС

- Програмне забезпечення оновлюється з метою підтримки його актуального стану та запобігання використанню вразливостей. Microsoft, Apple та інші виробники операційних систем випускають виправлення та оновлення майже щодня. Такі програми, як веб-браузери, мобільні застосунки та веб-сервери часто оновлюються компаніями та організаціями, які за них відповідають.

- Незважаючи на те, що організації докладають багато зусиль для пошуку та виправлення вразливостей програмного забезпечення, нові вразливості виявляються регулярно. Ось чому деякі організації використовують сторонніх дослідників безпеки, які спеціалізуються на пошуку вразливостей у програмному забезпеченні, або дійсно інвестують у власні команди з тестування на проникнення, які займаються пошуком та виправленням вразливостей програмного забезпечення, перш ніж вони можуть бути використані.

- Проект Project Zero від Google є чудовим прикладом такої практики. Після виявлення кількох вразливостей у різному ПЗ, що використовується кінцевими користувачами, Google створив постійну команду для пошуку вразливостей програмного забезпечення. Ви можете дізнатися більше про дослідження безпеки Google тут.

2.4 Ландшафт кібербезпеки

Криптовалюта

- Криптовалюта — це цифрові гроші, які можна використовувати для купівлі товарів і послуг, використовуючи надійні методи шифрування для захисту онлайн-транзакцій. Банки, уряди і навіть такі компанії, як Microsoft і AT&T, глибоко усвідомлюють її важливість і стрибають на підніжку останнього вагону криптовалюти!

- Власники криптовалют зберігають свої гроші в зашифрованих віртуальних «гаманцях». Коли транзакція відбувається між власниками двох цифрових гаманців, деталі записуються в децентралізовану електронну книгу або систему блокчейн. Це означає, що вона виконується з певною мірою анонімності та керується самостійно, без втручання третіх сторін, таких як центральні банки чи державні установи.

Криптовалюта (прод.)

- Приблизно кожні десять хвилин спеціальні комп’ютери збирають дані про останні транзакції з криптовалютою, перетворюючи їх на математичні пазли для збереження конфіденційності.
- Ці транзакції потім перевіряються за допомогою технічного та надзвичайно складного процесу, відомого як «майнінг». Цей крок зазвичай включає в себе армію «майнерів», які працюють на високоякісних ПК, щоб розв’язувати математичні пазли та перевіряти транзакції.
- Після перевірки реєстр оновлюється, копіюється в електронному вигляді та розповсюджується по всьому світу всім, хто належить до мережі блокчейн, фактично завершуючи транзакцію.

Видобуток криптовалюти без відома (Cryptojacking)

- **Cryptojacking** (криптоджекінг) – це нова загроза, яка ховається на комп'ютері, мобільному телефоні, планшеті, ноутбуці або сервері користувача, використовуючи ресурси цієї машини для «майнінгу» криптовалют без згоди або відома користувача.

- Багато жертв криптоджекінгу навіть не знали, що їх зламали, поки не стало занадто пізно!

2.5 Контрольна робота

Що нового я дізнався у цьому розділі?

- Кіберзлочинці використовують багато різних типів шкідливого програмного забезпечення або шкідливих програм для здійснення своєї діяльності. Зловмисне програмне забезпечення - це будь-який код, який може використовуватися для викрадання даних, обходу системи керування доступом, пошкодження або компрометації системи.

- Незалежно від типу шкідливого програмного забезпечення, яким була заражена система, є деякі загальні симптоми, на які слід звернути увагу. До них належать:

  - Збільшення використання центрального процесора (ЦП), що уповільнює роботу пристрою
  - ваш комп’ютер часто зависає або виходить з ладу
  - знижується швидкість перегляду веб-сторінок
  - виникають незрозумілі проблеми з мережними з'єднаннями
  - змінені або видалені файли
  - з'являються невідомі файли, програми або піктограми на робочому столі
  - запускаються невідомі процеси або сервіси
  - програми самостійно припиняють виконання або змінюють свої налаштування
  - електронні листи надсилаються без відома та згоди користувача

Що нового я дізнався у цьому розділі? (прод.)

- Соціальна інженерія – це маніпулювання особою задля спонукання її до виконання певних дій або розголошення конфіденційної інформації. Соціальні інженери часто використовують бажання людей допомогти іншим, а також їхні слабкості.

- **Атаки відмови в обслуговуванні (DoS)** — це тип мережевої атаки, яку відносно легко може здійснити навіть некваліфікований зловмисник. Результатом DoS-атаки є переривання роботи мережних сервісів для користувачів, пристроїв або застосунків.

- Розподілена DoS атака (DDoS) подібна до атаки DoS, але вона походить від декількох скоординованих джерел.

- Бот-комп'ютер зазвичай заражається в наслідок відвідування веб-сайту, відкривання вкладення електронної пошти або через заражений медіа-файл. Ботнет - це група ботів, з'єднаних через Інтернет, які можуть контролюватися одним зловмисником або групою.

Що нового я дізнався у цьому розділі? (прод.)

- Зловмисники, які атакують дані на шляху перехоплюють або змінюють зв’язок між двома пристроями, такими як веб-браузер і веб-сервер, щоб зібрати інформацію або видавати себе за один із пристроїв.
- Введення імені користувача та пароля є однією з найпопулярніших форм автентифікації на веб-сайті. Таким чином, виявлення вашого пароля є простим способом для кіберзлочинців отримати доступ до вашої найціннішої інформації.
- **Вразливості апаратного** забезпечення часто обумовлені недоліками його проектування.
- Помилки в операційній системі або коді програми зазвичай призводять до **вразливості програмного забезпечення.**

Що нового я дізнався у цьому розділі? (продовж.)

- Програмне забезпечення оновлюється з метою підтримки його актуального стану та запобігання використанню вразливостей.

- **Криптовалюта** — це цифрові гроші, які можна використовувати для купівлі товарів і послуг, використовуючи надійні методи шифрування для захисту онлайн-транзакцій. Банки, уряди і навіть такі компанії, як Microsoft і AT&T, глибоко усвідомлюють її важливість і стрибають на підніжку останнього вагону криптовалюти!

- **Cryptojacking (криптоджекінг)** – це нова загроза, яка ховається на комп'ютері, мобільному телефоні, планшеті, ноутбуці або сервері користувача, використовуючи ресурси цієї машини для «майнінгу» криптовалют без згоди або відома користувача.