Рекомендації CERT-UA щодо протидії APT (Advanced Persistent Threats)

1. Вступ

Загрози інформаційній безпеці, як відомо, змінюються. Традиційні загрози захищеності інформаційних систем з часом набули більш небезпечних, підступних та ефективних в дії типів – **Advanced Persistent Threat (APT)**.

Хоча, APT - тип загроз, що швидко розвивається, він вже голосно проявив себе та впливає на світову індустрію інформаційної безпеки. Прикладами APT, відносно нещодавно, стали:

1. Злам у 18 березня 2011 року систем RSA SecurID, які використовували двохфакторну автентифікацію та за допомогою токенів, включаючи дані, які використовувались компанією для генерації одноразових паролів.

2. Операція «Аврора» 2011 року, в рамках якої було вкрадено сенситивну інформацію, таку як інтелектуальна власність (програмні коди власності Google, Adobe та інших широковідомих компаній). Під час цього використовувались техніки високої складності та доброї скоординованості.

3. У 2014 році APT CERT-UA зафіксовано 2 атаки на органи державної влади України, які мають усі ознаки APT.

За даними фахівців, середній прямий збиток від кожної атаки APT для організацій становить 5,5 млн. у.о., які витрачаються на реагування та усунення наслідків.

Найчастіше джерелами APT є установи, що фінансуються з державних бюджетів та мають цілі, що виходять далеко за межі простої крадіжки:

- військова розвідка;
- економічний саботаж;
- технічний шпіонаж;
- фінансові махінації;
- політичні маніпуляції.

2. Як працює APT

Майже кожна атака APT має наступні етапи:

Особливості APT:

1. Етапи 3 та 4 можуть проводитись роками, що значно ускладнює їх детектування;
2. Типові заходи та засоби із захисту телекомунікаційних мереж та інформаційно-телекомунікаційних систем не діють проти APT з достатньою ефективністю, оскільки:

А) об’єкти атак APT – це чітко визначені організації, телекомунікаційна інфраструктура, технічні рішення тощо. Таким чином, атаки APT мають невеликий розголос та рідко викликають суспільний резонанс. Часто об’єкти атак бояться розголосу того, що вони стали жертвами APT в незалежності від того, державний, приватний чи комерційний сектор вони представляють;

Б) суб’єктами атак APT використовуються найновітніші хакерські техніки та технології, ціна яких зазвичай – велика для більшості звичайних комп’ютерних зловмисників. Атакуюча сторона не зупиняється при здійсненні APT, зіткнувшись з ситуацією, коли об’єкт атаки має досить надійний захист (це зазвичай робиться у разі «рядових» комп’ютерних злочинів);

В) типові пристрої та технології захисту, що використовуються у телекомунікаціях, можуть лише затримати час проведення етапу 2, проте не ефективні на етапах 3 та 4.

Г) для захисту від APT ефективні проактивні та комплексні методики захисту, які дозволяють виявляти та попереджувати етап 2 та подальші етапи. APT може змінювати характеристики, дозволяючи обходити навіть дуже надійні мережеві пристрої захисту.

3. Рекомендації CERT-UA щодо протидії APT

Успішна стратегія захисту від APT повинна включати традиційні організацію периметру захисту і заходи з забезпечення безпеки інфраструктури. Таким чином, організація повинна бути спроможною до наступних **організаційних заходів**:

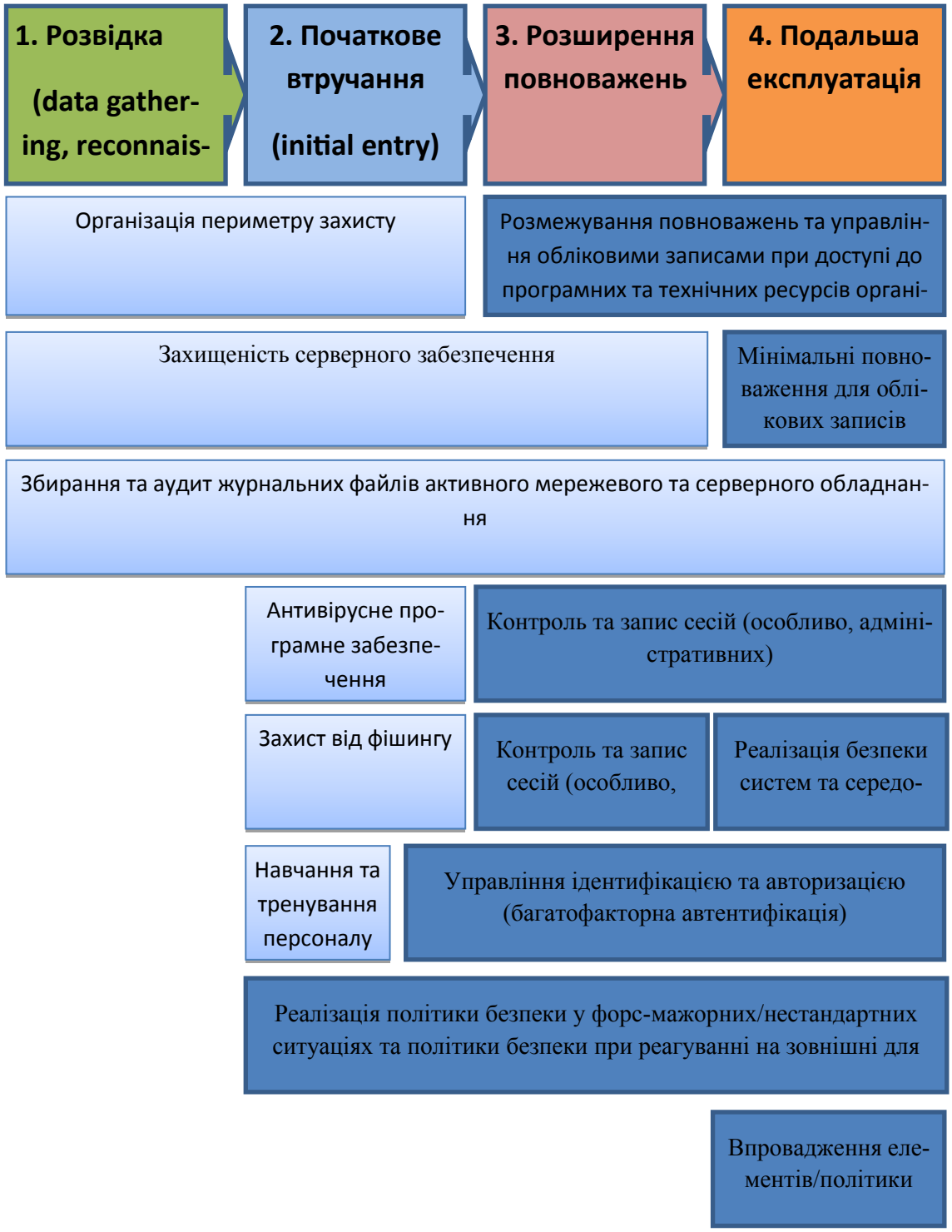
- максимально ускладнити початкове втручання (добрий приклад – забороняюча політика безпеки за принципом «заборонено все, що не дозволено»);
- знизити потенційні ризики при розширенні повноважень (наприклад, при компрометації автентифікаційних даних);
- обмежити шкоду, яка може бути нанесена при компрометації акантів організації;
- детектувати підозрілу активність та розвідку вразливих місць;
- збирати інформацію від/для розслідувань, яка необхідна для визначення наслідків APT та їх усунення.

Конкретні **технічні заходи**, які рекомендуються CERT-UA щодо протидії APT**:**

- розмежування повноважень та управління обліковими записами при доступі до програмних та технічних ресурсів організації;
- мінімальні повноваження для облікових записів;
- контроль та запис сесій (особливо, адміністративних);
- захищеність серверного забезпечення;
- реалізація політики безпеки у форс-мажорних/нестандартних ситуаціях та політики безпеки при реагуванні на зовнішні для організації загрози;
- реалізація безпеки систем та середовищ віртуалізації;
- управління ідентифікацією та авторизацією (багатофакторна автентифікація);
- впровадження елементів/політики управління даними.

4. Етапність APT

На схемі, що визначає етапність APT, перелічені вище заходи зображено у тій частині, в якій вони можуть бути корисними на різних етапах протидії атаці APT:



5. Конкретні поради CERT-UA щодо протидії APT

5.1 Для **розмежування повноважень та управління обліковими записами при доступі до програмних та технічних ресурсів організації** необхідно**:**

- безпечно зберігати зашифровані парольні дані;

- управляти складністю паролів (ввести мінімальні довжини, зробити обов'язковими спеціальні символи та різні регістри в паролях, регулярно змінювати паролі);

- обмежити доступ до адміністративних облікових записів;

- заборонити збереження автентифікаційних даних з використанням можливостей автоматичної автентифікації (веб-браузери, клієнти електронної пошти, електронні платіжні системи тощо);

- обмежити кількість осіб, які мають доступ до привілейованих облікових записів (наприклад, шляхом створення облікового запису «для нагальної потреби»);

- заборонити використання фіксованих паролів у скриптах;

5.2 Для **мінімальних повноважень для облікових записів** необхідно**:**

- не повинно надаватись доступу за принципом «все або нічого». Натомість повинно бути реалізовано схему, за якою для виконання певних завдань певні користувачі повинні шляхом авторизації та автентифікації отримати визначені для цього ролі. Наприклад:

Системні адміністратори – їм повинно дозволятись оновлення програмне забезпечення, конфігураційні зміни та встановлення нового програмного забезпечення, але не повинно бути дозволено змінювати налаштування безпеки або переглядати журнальні файли;

Адміністратори безпеки – їм повинно дозволятись оновлювати або змінювати налаштування та конфігурації, а також переглядати журнальні файли, але не повинно бути дозволено встановлювати програмне/апаратне забезпечення або здійснювати доступ до сенситивних даних;

Аудитори – повинні мати можливість перевіряти налаштування безпеки та переглядати журнальні файли, але не повинні мати можливості здійснювати будь-які зміни в системах організації.

5.3 Для **контролю та запису сесій (особливо, адміністративних)** необхідно**:**

- щоб було зрозумілим чином та легко визначити «хто що і коли робив»;

- впровадити аналітичний інструментарій з метою пошуку та виявлення загроз та уразливостей замість перегляду гігабайтів журнальних файлів;

- відмічати будь-які команди, які вводяться користувачами;

- поєднувати аномальну активність з особою, яка її породжує.

5.4 Для **захищеності серверного забезпечення** необхідно**:**

- використовувати мережевий екран (програмний і/або апаратний), який контролює з'єднання, блокує пакети даних та небезпечні (не довірені) протоколи;

- впровадити політику для дозволених програмних пакетів (тобто, визначити, що можна, а що – ні встановлювати на серверах);

- визначити специфічні для сенситивних програмних пакетів та критично важливих для організації завдань;

- заборонити внесення змін до журнальних файлів;

- здійснювати моніторинг цілісності ключових файлів;

- контролювати доступ до файлів та директорій, сервісів, фізичний доступ тощо.

5.5 Для **реалізації політики безпеки у форс-мажорних/нестандартних ситуаціях та політики безпеки при реагуванні на зовнішні для організації загрози** необхідно**:**

- використовувати утиліти та засоби моніторингу та захисту файлів для можливості адміністраторів детектувати спроби атакуючих зламати мережі;

- модифікувати імена стандартних системних команд та адрес, таким чином щоб вони були не стандартні. Стандартні системні команди та адреси повинні викликати сигнал про загрозу.

5.6 Для **реалізації безпеки систем та середовищ віртуалізації** необхідно:

- застосовувати принцип мінімальних повноважень та привілеїв для аканту гіпервізора;

- здійснювати моніторинг а журналювання усіх дій (подій), які відбуваються на рівні гіпервізора;

- зробити більш захищеними віртуальні машини шляхом активації можливостей з підтримки автоматизації процесів віртуалізації (наприклад, для версії Platinum Edition системи віртуалізації XenServer існує можливість адміністраторам створювати політики автоматичного створення знімків копій віртуальних машин, їх архівування та збереження на визначених сховищах).

5.7 Для **управління ідентифікацією та авторизацією** необхідно:

- позбавляти повноважень (та забороняти доступ до інформації, яка в них циркулює і обробляється) в програмно-апаратних рішеннях/системах персон, які полишили організацію;

- регулярно перевіряти та видаляти не використовувані та не актуальні облікові записи;

- за можливості, реалізовувати більше одного метода автентифікації при доступі до ресурсів/інформації. Як варіант, використовувати програмну двох факторну автентифікацію завтентифікаційними даними, що відрізняються для кожного пристрою/програмного продукту.

- використовувати різні методи автентифікації для різних сценаріїв (наприклад, при доступі з зовнішніх для організації мереж сценарій автентифікації може включати автентифікацію за токеном, а також потребувати введення захисного коду (captcha) для захисту від підбору автенифікаційних даних з використанням ботів);

- використовувати механізми захисту від різних технік APT (різноманітні затримки при негативних спробах автентифікації, ідентифікація пристроїв, геолокація, білі/сірі/чорні списки, індивідуальні реакції на певні загрози APT тощо);

- реалізувати вимоги щодо певного (зазвичай, більш жорсткого) порядку проходження етапів автентифікації у разі, якщо в її результаті користувачу повинно бути надано більш широкі повноваження.

5.8 Для **впровадження політики управління даними** необхідно:
- класифікувати відповідно до ступеня важливості інформацію, яка циркулює та обробляється в організації, після чого визначивши технології та методи її захисту;

- контролювати передавання даних між частинами організації (філіями) та/або іншими організаціями (наприклад, відслідковувати шляхи слідування електронної пошти та жорстких дисків тощо).