**Завдання 1.**

1. Відкрили в браузері сайт metadefender.opswat.com.

2. Обрали файл з ПК та просканували його.

3. Звіт про результат сканування:

- назва файлу: BlueStacks10Installer

- тип файлу: .exe

Після сканування файлу на metadefender.opswat.com за допомогою 32 антивірусних модулів, було виявлено наступну загрозу: Virus/Malware!qwuQNre3.

 Зазначена загроза була виявлена лише одним із 32 антивірусних модулів, що використовується на сайті metadefender.opswat.com. Інші модулі не виявили небезпеки у цьому файлі. Але, оскільки даний файл був завантажений з офіційного джерела сайту технологічної компанії , то можна вважати, що даний файл є цілком безпечним, а також через те, що лише один із багатьох антивірусних модулів виявив загрозу в файлі, а інші модулі не співпали з цим результатом, це може вказувати на деяку невизначеність чи суперечливість у виявленні потенційної загрози. У такому випадку є кілька можливих пояснень:

- False Positive (Хибний позитив): Можливо, антивірусний модуль, який виявив загрозу, зробив помилку і вважає безпечний файл за потенційно шкідливий. Такі помилки, відомі як хибні позитиви, можуть траплятися.

- Нова або маловідома загроза: Інший антивірусний модуль може виявити загрозу, яку інші модулі ще не розпізнали. Це може бути новий тип загрози або маловідома шкідлива програма.

- Варіація загрози: Можливо, інші антивірусні модулі не розпізнали дану варіацію загрози, яка виявлена одним модулем.

- Помилкове виявлення: Антивірусний модуль може виявити щось, що виглядає як загроза, але насправді є безпечним.

**Завдання 2.**

|  |  |  |
| --- | --- | --- |
| **№** | **Програма** | **Мета створення** |
| **1** | **ILOVEYOU** | Для свого поширення ILOVEYOU використовував ті ж схеми, що і Melissa. Але він не лише розсилав свої копії адресатам через Microsoft Outlook, але й поводив себе як типова троянська программа. Він намагався викрасти всі знайдені паролі, які переправляв на поштову скриньку зловмисників. Серед його можливостей було зафіксовано і видалення випадкових файлів з зображеннями або MP3, замість яких записувався вірусний код. ILOVEYOU розмножувався з кожним перезавантаженням Windows. |
| **2** | **Nimda** | Цей багатовекторний мережевий хробак заполонив мережу за короткий проміжок часу восени 2001 року. Усього лише 22 хвилини знадобилося Nimda, щоб проникнути на мільйони комп’ютерів. Для зараження ПК хробак використовував усі доступні шляхи: електронну пошту для розсилки спаму, слабкі місця у захисті ОС, загальнодоступні вебсайти, навіть знаходив старі бекдори, залишені попередніми вірусами. |
| **3** | **Slammer** | Вірус Slammer став відомий у 2003 році як один з тих, що найшвидше поширювалися. Для проникнення на 75 тисяч пристроїв йому знадобилося лише 10 хвилин. Шкідлива програма використовувала одну із уразливостей Windows, про яку було відомо ще за півроку до цього. І Microsoft навіть випустила оновлення, щоб виправити виявлену помилку. Але цей факт проігнорували більшість користувачів, в тому числі і деякі підрозділи самої корпорації. |
| **4** | **Code Red** | Мережевий хробак Code Red заявив про своє існування влітку 2001 року. Проникаючи на ПК через помилки в ОС Windows, він продовжував пошуки інших вразливих сайтів. За короткий термін (близько 20 днів) вірус інфікував близько 360 000 машин і створив з них зомбі-мережу. Основною метою діяльності хробака була DDoS-атака веб-сайту Білого Дому. Не зважаючи на завдані збитки у розмірі 3 мільярдів доларів, головної мети Code Red досягти не зміг. Причиною стала помилка розробників, особи яких досі не встановлені. Вірусна атака була запланована на IP-адресу, яку вдалося вчасно змінити і зламати плани зловмисників. |
| **5** | **Хробак Stuxnet** | Перший хробак-шпигун, який перепрограмує промислові установки, був використаний для вірусної атаки у 2010 році. В його коді знайдена ділянка, що використовує уразливості операційної системи Windows для отримання доступу до компонентів автоматичної системи управління SCADA. Такі АСУ використовуються на великих ядерних і хімічних підприємствах, на електростанціях і в аеропортах. Stuxnet таємно прописується на деяких програмованих чипах і може фізично руйнувати інфраструктуру об’єкта. |
| **6** | **Melissa** | В березні 1999 року віртуальний світ вразила епідемія вірусу Melissa, який відносять до категорії мережевих хробаків. Його творець Девід Сміт попередньо розмістив файли з вірусом на деяких форумах у вигляді списку з переліком сайтів для дорослих і паролями доступу до них. Протягом двох днів, використовуючи поштовий сервіс Microsoft Outlook, Melissa поширила свої копії на сотні тисяч ПК. Через вірусну атаку тимчасово були вимушені відключити свої e-mail сервери такі гіганти, як  Intel та Microsoft, щоб попередити подальше розповсюдження шкідливої програми. З кожного зараженого комп’ютера вірус розсилав свої копії у вигляді спаму на 50 перших адрес із списку контактів користувача. Таким чином було інфіковано близько мільйона ПК і нанесено збитків на 80 млн. доларів. |
| **7** | **Вірус WIN.CIH (Чорнобиль)** | 26 квітня 1999 року на тисячах ПК по всьому світу активізувався вірус, подібних якому ще не було. Використовуючи уразливості ОС Windows 95/98 , він через електронну пошту поширювався від комп’ютера до комп’ютера і пошкоджував вміст жорстких дисків, а подекуди і мікросхеми BIOS. Від вірусу  WIN.CIH (Чорнобиль) постраждало 300-500 тисяч ПК, розмір збитків сягає 80 мільйонів доларів |
| **8** | **Хробак Sasser** | Творіння 17-річного школяра з Німеччини розпочало своє поширення мережею навесні 2004 року. Під прицілом вірусної атаки опинилися досить серйозні цілі: Британська берегова охорона, авіакомпанія Delta Airlines, інформаційна агенція France-Presse, десятки комп’ютерних мереж великих корпорацій, університетів, лікарень. Збиток від цього вірусу нараховує сотні мільярдів доларів. Але винуватець цих подій, будучи неповнолітнім, так і залишився непокараним. |
| **9** | **Хробак Heartbleed** | Шкідлива програма, яка навесні 2014 року змусила хвилюватися весь віртуальний світ. Вірус, випадково створений програмістом Робіном Сеггельменом, використав уразливості криптографічного пакету  OpenSSL і проник за короткий термін майже на півмільйона інтернет-сайтів. Heartbleed вкрав особисті дані, інформацію про кредитні карти, паролі у багатомільйонної аудиторії користувачів мережі. |
| **10** | **Хробак Морріса** | Зразок експерименту, над яким втратили контроль, і це привело до незапланованих наслідків. У листопаді 1988 року Роберт Морріс  вирішив дослідити розміри існуючої на той час комп’ютерної мережі і використав для цього вірус, додавши в нього функцію самокопіювання. Хробак вийшов з-під контролю і спровокував епідемію, заразивши більше 6 000 ПК мережі ARPANET. Збитки від вірусної атаки склали 96,5 мільйонів доларів. |

Так, комп'ютерні віруси можуть бути загрозою не тільки для комп'ютера, але й для користувача. Вони можуть викрасти особисту інформацію, таку як паролі, номери кредитних карток, адреси електронної пошти та інші конфіденційні дані. Це може призвести до крадіжки ідентичності або фінансових втрат. Крім того, віруси можуть використовувати ваш комп'ютер для проведення незаконних дій, таких як розсилка спаму або атаки типу "відмова в обслуговуванні", що може призвести до юридичних наслідків. Тому важливо завжди мати актуальне антивірусне програмне забезпечення та регулярно оновлювати свою операційну систему та програмне забезпечення.

**Завдання 3**

Часова діаграма з основними етапами історії їх створення.



Щодо гарантії безпеки, то жодне антивірусне програмне забезпечення не може гарантувати 100% захисту, оскільки нові загрози з'являються дуже швидко. Однак використання якісного антивірусу є важливим кроком для забезпечення безпеки ваших даних та пристроїв.

**Завдання 4**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер | Випадки зараження їхнього комп'ютера вірусом | Антивірусна програма яку вони використовують | Частота оновлення | Спосіб оновлення |
| 1 | Так | Norton | Щоденно | Автоматично |
| 2 | Ні | - | - | - |
| 3 | Так | Avast | Щотижня | Вручну |
| 4 | Так | McAfee | Рідко | Автоматично |
| 5 | Ні | - | - | - |