Одеський коледж комп’ютерних технології «Сервер»

Звіт з практичної роботи №6

З предмету «Технології захисту інформації»

Тема : «комп`ютерні віруси. Їх слід в Україні»

Виконував :

Студент групи К21.1

Машков Володимир

Одеса 2024

ВСТУП

З початку 21 століття Україна зазнала численних кібератак, які мали як економічні, так і політичні наслідки. Деякі з них були спрямовані на виведення з ладу критичної інфраструктури, інші — на збагачення зловмисників за допомогою шифрувальників та троянів. Зокрема, атаки таких вірусів, як NotPetya, WannaCry та BlackEnergy, стали загрозою не лише для приватних осіб, але й для великих корпорацій і державних установ. Метою цієї роботи є аналіз основних вірусних атак, що відбулися в Україні, дослідження їх механізмів та наслідків, а також вивчення ефективних методів боротьби з ними.

АНАЛІЗ КОМП'ЮТЕРНИХ ВІРУСІВ В УКРАЇНІ

1. NotPetya (2017)

Історія створення та механізм поширення

Вірус NotPetya, що почав свою атаку 27 червня 2017 року, поширювався через українське бухгалтерське програмне забезпечення M.E.Doc, яке використовувалося багатьма українськими компаніями для подання податкової звітності. Вірус використовував уразливість протоколу SMBv1 (експлойт EternalBlue) для поширення по локальних мережах. На відміну від типових шифрувальників, NotPetya мав головною метою знищення даних, а не отримання викупу.

Механізм дії

1. Інфікування через програмне забезпечення: Вірус впроваджувався через фальшиве оновлення для програми M.E.Doc.
2. Використання EternalBlue та PsExec: Вірус швидко поширювався через корпоративні мережі, використовуючи інструменти для віддаленого керування та вразливості Windows.
3. Шифрування MBR та блокування системи: NotPetya шифрував головний завантажувальний запис (MBR), роблячи неможливим запуск операційної системи.

Наслідки та втрати

Серед найбільших постраждалих компаній були такі гіганти, як Maersk, Roshen та Нова пошта. Компанія Maersk втратила близько $300 млн через зупинку систем, а загальний глобальний збиток оцінюється в $10 мільярдів. Атака спричинила параліч багатьох українських державних установ, включно з Національним банком України та Міністерством інфраструктури України.

Реакція та боротьба

Після атаки українські організації масово почали впроваджувати політики резервного копіювання та встановлювати оновлення безпеки. Антивірусні компанії випустили спеціальні оновлення для боротьби з NotPetya, зокрема, Kaspersky Lab та Symantec.

1. WannaCry (2017)

Історія створення та механізм поширення

WannaCry був першим масштабним шифрувальником, що в травні 2017 року завдав удару по світових компаніях та державних установах, включно з українськими банками, телекомунікаційними компаніями та медичними закладами. Вірус поширювався через фішингові атаки та уразливість SMBv1 (також експлойт EternalBlue).

Механізм дії

1. Початкове зараження через фішинг або мережу: Користувачі відкривали шкідливі вкладення або заражені файли.
2. Шифрування файлів: Вірус шифрував усі важливі файли на пристрої.
3. Розповсюдження через SMB: WannaCry поширювався в межах локальної мережі компанії, використовуючи уразливість SMB.
4. Вимога викупу: На екрані з'являлося повідомлення з вимогою сплатити викуп у розмірі 300 доларів у біткоїнах за відновлення файлів.

Наслідки та втрати

В Україні WannaCry атакував кілька медичних закладів, включаючи мережу клінік "Борис" та державні банки, зокрема Ощадбанк. Хоча точні збитки від цієї атаки в Україні не оприлюднені, глобальний збиток оцінюється в $4–8 мільярдів.

Реакція та боротьба

Для боротьби з WannaCry було впроваджено масштабну кампанію з оновлення операційних систем та програмного забезпечення. Особливу увагу приділили резервному копіюванню важливих даних та встановленню патча MS17-010 від Microsoft, який закривав уразливість EternalBlue.

1. BlackEnergy (2015)

Історія створення та механізм поширення

BlackEnergy — це троян, який був розроблений для атак на критичну інфраструктуру. Він став відомим завдяки кібератаці 23 грудня 2015 року, що призвела до масових відключень електроенергії в Україні. Ця атака стала першою підтвердженою кібератакою на енергетичну систему країни, під час якої постраждало понад 230 000 споживачів електроенергії.

Механізм дії

1. Фішинг:

Зловмисники надсилали шкідливі листи співробітникам енергетичних компаній із вкладеними документами, що містили макроси з кодом трояна.

1. Впровадження трояна:

Після активації вірус BlackEnergy створював "бэкдори" у системах управління енергетичними мережами.

1. Відключення електропостачання:

В результаті атаки кіберзлочинці отримали можливість керувати енергосистемами, що призвело до відключення електроенергії в Західній Україні.

Наслідки та втрати

Атака BlackEnergy завдала значного удару по енергетичній інфраструктурі України. Відключення електроенергії призвело до хаосу в роботі служб екстреної допомоги та паралізувало транспортну інфраструктуру.

Реакція та боротьба

Після атаки енергетичні компанії почали масово впроваджувати засоби моніторингу мережевої активності та вдосконалювати свої засоби захисту від атак. Також було посилено державний контроль за захистом критичної інфраструктури.

Наслідки кібератак для україни

Кожна з описаних атак завдала значної шкоди економіці та інфраструктурі України. Найбільш серйозними наслідками стали зупинка роботи підприємств, втрата фінансових даних та підрив довіри до системи інформаційної безпеки. Ці атаки підкреслили необхідність посилення національної кібербезпеки та розробки ефективних механізмів протидії кіберзлочинності.

Методи боротьби з вірусами

1. Встановлення оновлень безпеки

Регулярні оновлення операційних систем та програмного забезпечення є ключовими для захисту від новітніх загроз.

1. Резервне копіювання

Регулярне створення резервних копій важливих даних допомагає мінімізувати збитки у випадку атаки.

1. Підвищення обізнаності

Організація тренінгів для працівників щодо безпечного використання електронної пошти та інтернету знижує ризик зараження через фішинг.

ПОРІВНЯННЯ СИГНАТУР КОМП'ЮТЕРНИХ ВІРУСІВ, ЩО АКТИВНО ЗУСТРІЧАЛИСЯ В УКРАЇНІ

Сигнатури комп'ютерних вірусів є унікальними ознаками, за якими антивірусне програмне забезпечення ідентифікує шкідливе ПЗ. Однак, незважаючи на їхню індивідуальність, багато вірусів мають спільні елементи у своїх сигнатурах, що може вказувати на схожі методи розповсюдження або цілі атак. У цьому розділі порівняємо сигнатури кількох найбільш значущих вірусів, що атакували українські компанії та інфраструктуру, таких як NotPetya, WannaCry та BlackEnergy.

NotPetya

Сигнатура NotPetya вирізняється комбінацією кількох компонентів, що характерні для вірусів-шифрувальників. Основні елементи сигнатури:

* Payload: вірус використовує модуль шифрування даних на диску з особливим акцентом на шифрування Master Boot Record (MBR), що робить систему непрацездатною.
* EternalBlue експлойт: NotPetya поширюється через мережу, використовуючи експлойт EternalBlue, відомий через уразливість в протоколі SMBv1.
* PsExec: використання цієї утиліти для віддаленого виконання команд на інфікованих пристроях.
* Шифрування MFT: вірус також модифікує Master File Table (MFT), що робить відновлення файлів неможливим навіть після оплати викупу.

Антивірусні програми ідентифікують NotPetya за певними шаблонами поведінки, що включають зміну MBR, використання протоколу SMB для поширення та характерну форму шифрування файлів.

WannaCry

Сигнатура WannaCry має схожі елементи із NotPetya, однак має свої унікальні особливості:

* Payload: шифрування файлів з використанням AES-128 у поєднанні з RSA-2048 для збереження ключів дешифрування.
* EternalBlue експлойт: як і NotPetya, WannaCry використовує цю уразливість для швидкого поширення в межах локальних мереж.
* Worm component: WannaCry має компонент для автоматичного розповсюдження, який дозволяє вірусу швидко інфікувати нові пристрої.
* Розширення файлів: після шифрування файли отримують нові розширення, що допомагає антивірусним програмам легко ідентифікувати вірус.

Ці компоненти дозволяють антивірусам виявляти WannaCry за його методами шифрування, самовідтворення та характерними файлами-запитами викупу.

BlackEnergy

Сигнатура трояну BlackEnergy суттєво відрізняється від сигнатур шифрувальників, оскільки цей вірус спрямований на компрометацію систем управління критичної інфраструктури:

* Rootkit компоненти: BlackEnergy має модулі для прихованої роботи на заражених системах, що ускладнює його виявлення.
* Plug-in архітектура: вірус використовує плагіни для розширення своїх можливостей, зокрема для збору даних, викрадення облікових записів та управління інфраструктурою.
* SCADA-націленість: BlackEnergy спеціально адаптований для атак на системи SCADA, які використовуються для управління енергетичною та транспортною інфраструктурою.
* DDoS атаки: одна з функцій BlackEnergy — організація масованих розподілених атак на відмову в обслуговуванні (DDoS), що дозволяє виводити з ладу мережеві сервіси.

Антивірусні системи ідентифікують BlackEnergy за його специфічними модулями, які спрямовані на SCADA-системи, а також за використанням rootkit-компонентів для маскування активності.

Порівняльний аналіз

* NotPetya та WannaCry мають схожі механізми поширення через використання уразливості EternalBlue, однак NotPetya спрямований на повне знищення даних, тоді як WannaCry — на отримання викупу.
* BlackEnergy значно відрізняється від цих двох вірусів, оскільки його мета — не комерційний зиск, а підрив критичної інфраструктури шляхом контролю над SCADA-системами.
* Спільною рисою для всіх трьох вірусів є використання фішингових кампаній для початкового зараження систем, однак їх методи розповсюдження та цілі значно різняться.

Таким чином, сигнатури цих вірусів демонструють різні стратегії впливу: від шифрувальників до комплексних троянів для атак на критичну інфраструктуру.

ОПИС СХЕМИ РОБОТИ ВІРУСІВ

Изображение выглядит как текст, чек, диаграмма

Автоматически созданное описание

Рисунок 1.1 – відображення схеми роботи вірусу NotPetya

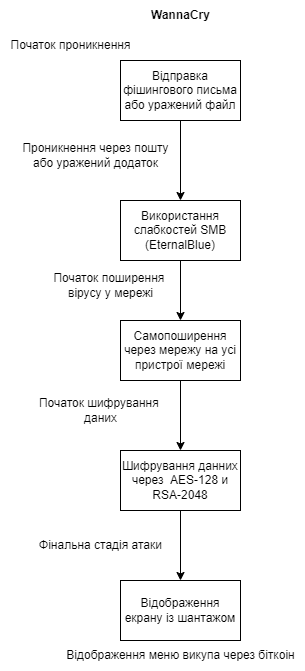


Рисунок 1.2 – відображення схеми роботи вірусу WannaCry

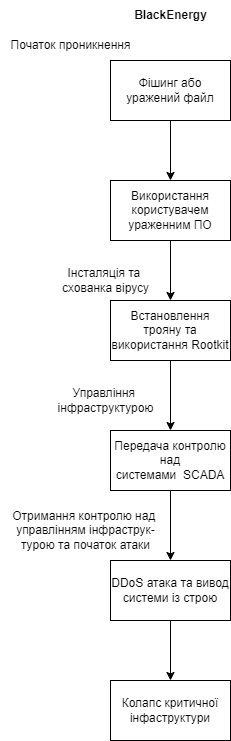


Рисунок 1.3 – відображення схеми роботи вірусу BlackEnergy

ВИСНОВКИ

Україна стала мішенню для кількох найбільших кібератак останніх років, що призвело до значних економічних та соціальних наслідків. Атаки NotPetya, WannaCry та BlackEnergy продемонстрували вразливість як приватних компаній, так і державних установ. Однак, завдяки запровадженню новітніх заходів кібербезпеки та покращенню політики захисту даних, Україна продовжує зміцнювати свій захист від майбутніх загроз.