ВІРУСИ ТА АНТИВІРУСИ

Токарський Н.М.,ст. гр. А-12-19
Терещенков Д.І.,ст. гр.А-12-19
Костікова М.В. – керівник канд. техн. наук, доцент
ХНАДУ

Введення

В наш час комп'ютерні віруси та антивірусні програми є невід'ємними складовими будь-якої операційної системи які мають доступ до мережі інтернету.

Поняттяя комп'ютерний вірус та антивірусна програма

1.1. Комп'ютерний вірус

Комп'ютерний вірус – комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням

власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу.

Антивірусна програма

Антивірусна програма (антивірус) – спеціалізована програма для знаходження комп'ютерних вірусів, а також небажаних

(шкідливих) програм загалом, та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики – запобігання зараження (модифікації) файлів чи операційної системи шкідливим кодом.

Різновиди комп’ютерних вірусів та антивірусних програм

Різновид комп’ютерних вірусів

*Хробаки – Worm.*Хробак – програма, яка робить копії самої себе. Її шкода полягає в засмічуванні комп’ютеру, через що він починає працювати повільніше. Відмінною особливістю хробака є те, що він не може стати частиною іншої нешкідливою програми.

*Віруси-маскувальники – Rootkit.*Ці віруси використовуються для приховування шкідливої активності. Вони маскують шкідливі програми, щоб уникнути їх виявлення антивірусними програмами. Rootkit також можуть модифікувати операційну систему на комп’ютері і замінювати основні її функції, щоб приховати своє власне присутність і дії, які робить зловмисник на зараженому комп’ютері.

*Віруси-шпигуни – Spyware.*Шпигуни збирають інформацію про поведінку і дії користувача. Здебільшого їх цікавить інформація – адреси, паролі, дані кредитних карт.

*Зомбі – Zombie.*Віруси зомбі дозволяють зловмисникові керувати комп’ютером користувача. Комп’ютери – зомбі можуть бути об’єднані в мережу (бот-нет) і використовуватися для масової атаки на сайти або розсилання спаму. Користувач може навіть не здогадуватися, що його комп’ютер зомбований і використовується зловмисником.

Рекламні віруси – Adware. Програми-реклами, без відома користувачів вбудовуються в різне програмне забезпечення з метою демонстрації рекламних оголошень.

Як правило, програми-реклами вбудовані в програмне забезпечення, що поширюється безкоштовно. Реклама розташовується в робочому інтерфейсі. Найчастіше такі програми також збирають і переправляють своєму розробникові персональну інформацію про користувача.

Різновид антивірусних програм

Програми-детектори призначені для знаходження заражених файлів одним із відомих вірусів. Деякі програми-детектори можуть також лікувати файли від вірусів або знищувати заражені файли. Існують спеціалізовані (тобто призначені для боротьби з одним вірусом) детектори та поліфаги (можуть боротися з багатьма вірусами).

Програми-лікарі призначені для лікування заражених дисків і програм. Лікування програми полягає у вилученні із зараженої програми тіла вірусу. Також можуть бути як поліфагами, так і спеціалізованими;

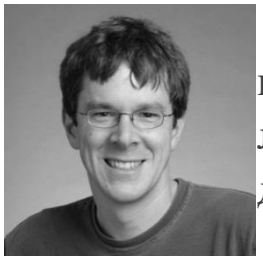
Програми-ревізори призначені для виявлення зараження вірусом файлів, а також знаходження ушкоджених файлів. Ці програми запам'ятовують дані про стан програми та системних областей дисків у нормальному стані (до зараження) і порівнюють ці дані у процесі роботи комп'ютера. В разі невідповідності даних виводиться повідомлення про можливість зараження;

Лікарі-ревізори призначені для виявлення змін у файлах і системних областях дисків й у разі змін повертають їх у початковий стан.

Програми-фільтри призначені для перехоплення звернень до операційної системи, що використовуються вірусами для розмноження і повідомляють про це користувача. Останній має можливість дозволити або заборонити виконання відповідної операції. Такі програми є резидентними, тобто вони знаходяться в оперативній пам'яті комп'ютера.

Програми-вакцини використовуються для обробки файлів і boot-секторів із метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше).

Найпопулярніші комп'ютерні віруси та антивірусні програми



*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.

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.

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.

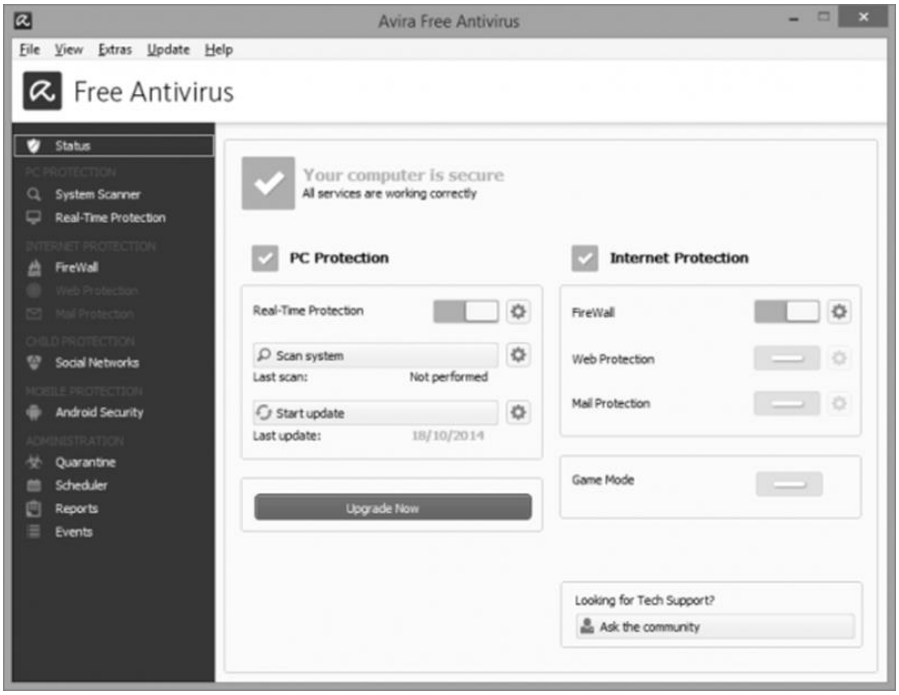
ILOVEYOU. Єдиний вірус, який було внесено до Книги рекордів Гіннеса як самий руйнівний в світі. Написаний хакерами з Філіпін хробак у 2000 році інфікував більше 3 мільйонів комп'ютерів по всьому світу і завдав шкоди на 10-15 мільярдів доларів.

Він не лише розсилав свої копії адресатам через Microsoft Outlook, але й поводив себе як типоватроянська програма. 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.

ТОП-5 антивірусних програм

*№5. Avira.*Avira – це абсолютно безкоштовне антивірусне програмне забезпечення, яке в новому році встигло здобути нових користувачів.

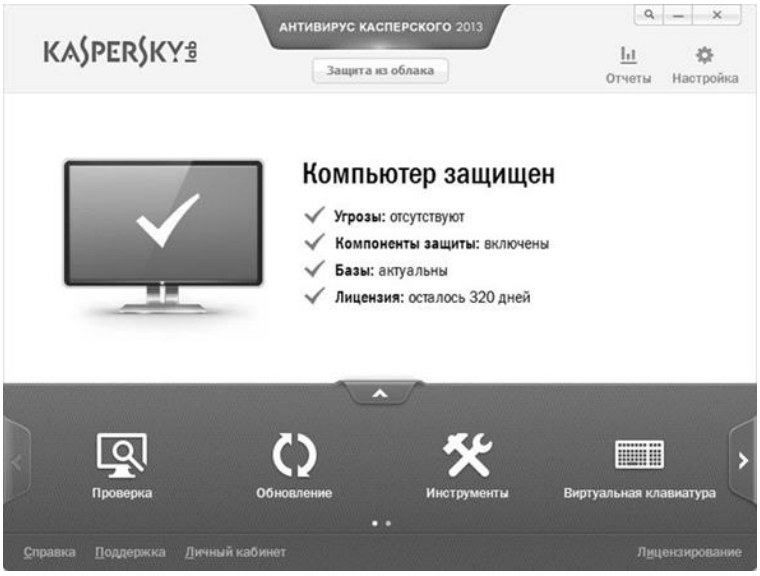


Особливості програми:

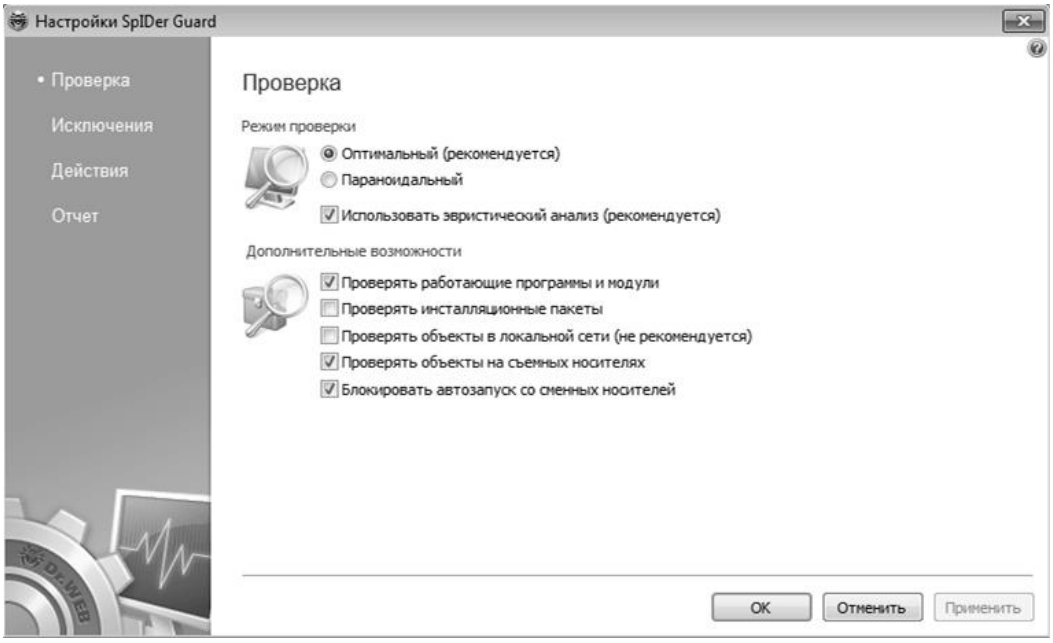
- Кросплатформеність. Ця характеристика дозволяє антивірусу залучати все більше і більше користувачів, а також синхронізувати дані на декількох пристрої в режимі онлайн.
- У новій версії поліпшені алгоритми пошуку шкідливого ПЗ.
- Висока продуктивність.

№4. Антивірус Касперського. Даний антивірус не потребує додаткового представлення. Він чудово знайомий користувачам всього світу.

Вже більше десяти років антивірус від лабораторії Касперського користується величезною популярністю і займає топові позиції в більшості тематичних рейтингів зі всього світу. Даний антивірус є найпопулярнішим захисником на території всього СНД. За багато років роботи лабораторія не обмежилася створенням тільки одного антивіруса.



№3. Dr. Web. Даний антивірус використовує один з найбільш ефективних алгоритмів пошуку вірусів.



Завдяки регулярному оновленню вірусної бази, пристрій захищений від усіх нових типів вірусів.

Завдяки особливій технології пошуку шкідливих програм, антивірус здатний аналізувати поведінку підозрілих файлів, і таким чином, визначати їх як потенційно небезпечні. Така процедура виявлення використовується для тих типів вірусів, які ще не були занесені в базу даних.

№2. Comodo. Comodo – новий захисник для персональних комп'ютерів і ноутбуків.

Даний антивірус входить в топ даного рейтингу з ряду причин:

- Незважаючи на широкий функціонал і ефективну роботу, антивірус абсолютно безкоштовний, завантажити його можна тут.
- Крім браузера, користувач може безкоштовно отримати доступ до скачування спеціального захисника для браузерів.
- Швидке виявлення загроз самих різних типів.
- Програма не навантажує систему.
- Приємний користувальницький інтерфейс.

*№1. 360 I-Security.*Перший рядок рейтингу займає антивірус, що стрімко набирає свою популярність серед користувачів всього світу – 360 Internet Security.

Функціонал програми включає в себе:

- Додаткову програму для усунення вразливостей операційної системи.
- Регулярне встановлення патчів.
- Потужна взаємодія з системою на програмному рівні.
- Утиліта для очищення пристрою від «сміття».

Множинні тестування показали, що даний комплекс програм для захисту комп'ютера не поступається платним аналогам і навіть перевершує їх.

Тому можна по праву сказати, що даний софт – це кращий безкоштовний захисник нового року.

Література

1. Визначення поняттю комп'ютерний вірус. Режим доступу: https://uk.wikipedia.org/wiki/Комп%27ютерний_вірус

2. Визначення поняттю антивірусна програма Режим доступу:https://uk.wikipedia.org/wiki/Антивірусна_програма

3. Різновиди комп'ютерних вірусів Режим доступу: https://zillya.ua/osnovni-vidi-virusnikh-program

4. Різновиди антивірусних програм. Режим доступу: https://sites.google.com/site/diresideinaction/tipi-antivirusnih-program

5. Найвідоміщі комп'ютерні віруси. Режим доступу:https://zillya.ua/top-10-kompyuternikh-virusiv-v-istori-chastina-2

6. ТОП-5 Антивірусних програм. Режим доступу:http://chvv.com.ua/top-10-rejting-populyarnih-antivirusiv-2018-roku/