Міністерство освіти і науки України

Тернопільський національний педагогічний університет
імені Володимира Гнатюка

Кафедра інформатики
та методики її викладання

Рефератна тему:

«Видалення комп’ютерних вірусів»

Виконала:

студентка групи М-12

Козіброда Тетяна

Перевірила:

Галан В.І.

Тернопіль 2014

Зміст

[ВСТУП 3](#_Toc379495603)

[РОЗДІЛ 1. Видалення вірусів з USB флеш-накопи́чувачів 4](#_Toc379495604)

[РОЗДІЛ 2. Використання антивірусної програми KasperskyVirusRemovalTool 2011 5](#_Toc379495605)

[РОЗДІЛ 3. Видаляємо вірус з оперативної пам’яті 7](#_Toc379495606)

[РОЗДІЛ 4. Практичне вирішення проблеми 8](#_Toc379495607)

[ВИСНОВКИ 10](#_Toc379495608)

[Список використаних джерел 11](#_Toc379495609)

# ВСТУП

З проблемою необхідності видалення комп'ютерних вірусів рано чи пізно стикалося більшість користувачів. На помилках вчаться, і сьогодні люди вважають за краще встановлювати антивірус завчасно, замість того, щоб боротися з наслідками зараження комп'ютера. Запобігти зараженню, безумовно, простіше, ніж видаляти вірус і усувати наслідки його діяльності, але що робити, якщо вірус вже потрапив до вас в комп'ютер?

Перше і головне правило - не піддаватися паніці і не робити необдуманих дій. Багато вірусів можна видалити навіть без використання антивірусних програм (наприклад, autorun.inf на флеш-накопичувачі).[4]

Видалення комп'ютерних вірусів найчастіше зводиться до установки на заражений комп'ютер програми для видалення вірусів (або антивірусної програми), повного сканування системи і процедури лікування комп'ютерних вірусів.

Але зовні проста процедура, як видалити вірус з комп’ютера, може принести багато неприємних сюрпризів. І тому ми розглянемо найскладніші ситуації і дізнаємося, як самостійно видалити вірус.

# РОЗДІЛ 1. Видалення вірусів з USB флеш-накопи́чувачів

Дуже часто так звані «флешки» стають джерелом поширення вірусів. Але що робити, якщо наша флешка «підхопила» вірус?

Виявити вірус на флешці дуже просто, він видає себе, коли ви відкриваєте флешку і з’являється інформація про помилку. Відбувається це дуже часто, в деяких випадках вся інформація з флешки ховається або віддаляється. Причому навіть провідник не допомагає відкрити її, з’являється помилка на невідомій мові, що нагадує ієрогліфи.

Позбутися від вірусу можна наступним способом: заходите в пуск — виконати — набираєте cmd.exe і натискаєте ОК. Далі напишіть в командному рядку такі команди:

del / a-hrsXautorun.inf;

del / a-hrs Xautorun.txt;

del / a-hrsXautorun.bin;

del / a-hrsXautorun.wsh;

del / a-hrsXautorun.reg;

del / a-hrsXAutorun. ~ ex;

del / a-hrs Xautorun.inf\_?????

del / a-hrsXautorun.srm;

del / a-hrs XAUTORUN.FCB.

Іксом є назва вашої флешки, відповідно, вставляєте його замість букви. Так як заражені файли можуть знаходитися в теці WINDOWS — system32, потрібно видалити їх звідти. Можна перевірити носій і за допомогою антивірусів, але потрібно використовувати декілька антивірусів, щоб знайти всі шкідливі програми. Перед тим як вставити флешку в комп’ютер переконайтеся, що ваш антивірус активний, інакше комп’ютер буде заражений.[3]

# РОЗДІЛ 2. Використання антивірусної програми KasperskyVirusRemovalTool 2011

Розглянемо антивірусну програму, яка допоможе ідентифікувати вірус і вилікувати його навіть на зараженому комп’ютері. Програмне забезпечення лабораторії Касперського — KasperskyVirusRemovalTool 2011. Абсолютно безкоштовна програма для разового використання при підозрі інфікування Вашої машини.

Завантажуємо KasperskyVirusRemovalTool 2011 з офіційного сайту. Для актуальності RemovalTool, потрібно кожного разу завантажувати з сайту. Працює KasperskyVirusRemovalTool 2011 і при основному антивірусі, і в Безпечному режимі завантаження.

Запускаємо .exe файл і розпочинаємо роботу. Для початку програма розархівує необхідні файли на ПК. Після чого розпочне встановлення, потрібно буде декілька хвилин зачекати. Далі приймаємо ліцензійну угоду і натискаємо «Приступить к работе».

Програма проінформує нас, що все готово і можна розпочинати перевірку.

Тиснемо «Запустить проверку» і спостерігаємо за ходом сканування. Процес може затягнутися, тому запасаємось терпінням.

Малюнок . Підтвердження згоди з ліцензійними умовами

Під час перевірки в нижньому віконці екрану можуть з'являтись повідомлення про хід сканування або виявлення проблемних зон чи інфікованих вірусом файлів. Все це ми потім подивимось в журналі перевірки.

Коли Kaspersky Virus Removal Tool 2011 закінчить шукати вірус, про це Вас повідомить головне вікно програми. Тривалість перевірки залежить від виставленого режиму. При встановленому основному антивірусі Eset Smart Security 4 програма успішно просканувала систему і вірусів не виявила.

Малюнок . Процес перевірки

В Kaspersky Virus Removal Tool присутня функція відправки звітів в лабораторію Касперського. Для цього переходимо на вкладку «Лечение вручную» і збираємо інформацію про систему.

Після цього буде сформований архів, який можна відправити на аналіз.

Далі давайте перейдемо в журнал сканування. Тут ми можемо продивитись, які файли були перевірені на наявність вірусів, в яких вірус був виявлений і які повідомлення нам показували під час перевірки. Можемо побачити, що повідомлення про захищені паролем архіви виникали тоді, коли Kaspersky Virus Removal Tool 2011 намагався перевірити сам себе.

Тепер давайте перейдемо в розділ Налаштувань. Тут ми можемо виставити, які області ПК необхідно перевіряти.

Також можна виставити рівень безпеки. При найвищому рівні проскануються всі закапелки ПК, всі архіви і теки, тобто практично все. Але й перевірка тоді може затягнутись на 1-2 години, а то й більше.

В наступній опції ми можемо наказати програмі, яку дію виконувати при ідентифікації вірусу. Можна залишити по замовчуванню, в такому випадку при команді Вірус, програма буде перепитувати Вас: А що з ним робити?"

Ось, в принципі, і все про роботу та основні налаштування Kaspersky Virus Removal Tool 2011.

Основні принципи роботи:

* Kaspersky Virus Removal Tool 2011 не є основним антивірусом для Вашого ПК.
* Його варто використовувати тільки тоді, коли є підозра на вірус.
* Не конфліктує з основною антивірусною програмою.
* Коли вірус не дає комп'ютеру завантажитись і ввімкнути його можна тільки в Безпечному режимі, то Removal Tool чудово просканує систему і тут.[1]

# РОЗДІЛ 3. Видаляємо вірус з оперативної пам’яті

Процедура, як видалити вірус оперативної пам’яті, сильно ускладнена тим, що будь антивірус, запущений на комп’ютері, буде запущений вже після присутності вірусу в ram. Говорячи начистоту – у вашого антивіруса практично немає шансів самому залишитися не зараженим і виконати свою функцію, як видалити вірус з пам’яті. Тому видалити вірус з оперативної пам’яті надійно можна лише одним способом – доведеться скористатися онлайн-утилітою.

Перейдіть за адресою: www.viruslab.ru/service/check/. Знайдіть очима кнопку синього кольору з написом «перевірити ПК». Сміливо тисніть її.

У вікні антивіруса-онлайн ви побачите кілька кнопок, таких як «повне сканування», «швидке сканування» і «вибіркові перевірки».

Підберіть спосіб, необхідний вам. Вам буде запропоновано завантажити компонент ActiveX. Повторно натисніть «сканувати» і трохи почекайте. Оперативна пам’ять вашого комп’ютера очищена від вірусів![2]

# РОЗДІЛ 4. Практичне вирішення проблеми

Під час виконання практичного завдання проблему довелось вирішувати найрізноманітнішими шляхами. Спершу, використовуючи антивірусну програму Avast,запустивши сканування при завантаженні, ми знайшли та знешкодили 13 файлів, інфікованих вірусами win32:rootkit-gen[Rtk] та win32:malware-gen, а також відновили доступ до диспетчера завдань.



Малюнок . Результати сканування програмою Avast

Потім ми використали KasperskyVirusRemovalToolта MalwarebytesAnti-Malware, з допомогою яких знищили ту частину інфікованих файлів, що не можна було видалити з допомогою Avast.



Малюнок . Сканування Kaspersky Virus Removal Tool

Загалом теоретична інформація, знайдена мною, була корисною для нашої роботи. А щодо шляхів розв’язання проблеми, то вони відрізнявся від початкового плану. Це зумовлено неможливістю виконання деяких пунктів, або їх безкорисливістю в даній ситуації.

Загалом реальний план наших дій виглядав так:

На жаль, через брак часу інші методи боротьби з комп’ютерними вірусами застосувати не вдалось.

# ВИСНОВКИ

Отже, в результаті теоретичних і практичних досліджень можна зробити висновок, що знищення комп’ютерних вірусів з допомогою антивірусних програм і утиліт є досить ефективним способом, більше того: одним із найчастіше використовуваних. Проте очевидним є той факт, що абсолютно жодна програма не в змозі справитись із усіма вірусами, а інколи навіть і не ідентифікує їх. Тому, важливо захистити комп’ютер до того як туди потраплять віруси, адже інколи, здавалось би незначний вірус, може завдати незворотної шкоди, призводячи до втрати цінної інформації. Тому для безпеки власних даних необхідно приймати максимально можливі міри захисту.

# Список використаних джерел

1. http://webdigest.com.ua/bezpeka-kompyutera/antyvirusy/96-virus-kompyuter-infikovano-scho-robity.html
2. http://onlinenews.rv.ua/prohramne-zabezpechennya/yak-vydalyty-virus/
3. http://lifer.com.ua/yak-vidaliti-virus-z-kompyutera.html
4. http://www.callgenius.com.ua/resursi/119-vidalennya-virusiv

АНОТАЦІЯ

У роботі подано теоретичні відомості про методи знищення комп’ютерних вірусів, а також результати практичних досліджень. Порушуються питання видалення вірусів із оперативної пам’яті комп’ютера та USB флеш-накопичувачів. А також описано процес сканування комп’ютера з допомогою програми Kaspersky Virus Removal Tool.

КЛЮЧОВІ СЛОВА:

Видалення комп’ютерних вірусів, антивірусні програми, Kaspersky Virus Removal Tool