Муниципальное автономное общеобразовательное учреждение
средняя общеобразовательная школа №9

Разновидности компьютерных вирусов и методы защиты от них

исследовательский проект

Исполнитель:
обучающийся 11А класса
Ларионов Андрей
Руководитель:
учитель информатике
Коротеев Антон Геннадьевич

Нижний Тагил
2021

Содержание

Введение

Актуальность:

В настоящий период времени компьютеры осуществляют огромное количество целей и задач. По сути, сейчас не существует людей, работающих без электронно-вычислительных машин. Но для того чтобы она работала требуется операционная система. Одной из самых популярных является ОС Alt Linux. Она бесплатна, что очень дает большое преимущество перед другими.

Цель:

Повышение уровня информационной безопасности при использовании свободно распространяемого программного обеспечения

Задачи:

1. исследовать степень уязвимости ОС ALT Linux к вирусной активности
2. создать простейший вирус, работающий под управлением ОС ALT Linux
3. создать простейший антивирус, работающий под управлением ОС ALT Linux
4. протестировать созданное ПО на разных версиях ОС ALT Linux
5. сделать выводы исследования

цели и задачи проекта вы можете видеть на экране

Основные виды компьютерных вирусов

Вирусы

Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях или (раньше) на дискетах. По данным Национального института стандартов и технологий (NIST)

1.Червь

Червь– программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы.

2.Троянская программа (троянский конь, троян)

Троянская программа маскируется в других безвредных программах. До того момента как пользователь не запустит эту самую безвредную программу, троян не несет никакой опасности. Тронская программа может нанести различный ущерб для компьютера. В основном трояны используются для кражи, изменения или удаления данных. Отличительной особенностью трояна является то, что он не может самостоятельно размножаться.

3.Программы – шпионы

Шпионы собирают информацию о действиях и поведении пользователя. В основном их интересует информация (адреса, пароли).

4.Зомби

Зомби позволяют злоумышленнику управлять компьютером пользователя. Компьютеры – зомби могут быть объединены в сеть и использоваться для массовой атаки на сайты или рассылки спама. Пользователь может не догадываться, что его компьютер зомбирован и используется злоумышленником

5.Программы – блокировщики (баннеры)

Это программа, которая блокирует пользователю доступ к операционной системе. При загрузке компьютера появляется окно, в котором пользователя обвиняют в скачивание нелицензионного контента или нарушение авторских прав. И под угрозой полного удаления всех данных с компьютера требуют отослать смс на номер телефона или просто пополнить его счет. Естественно после того как пользователь выполнит эти требования банер никуда не исчезнет

Методы защиты от компьютерных вирусов

Вирусы, как правило, пользуются ошибками или эксплойтами в коде этих программ для того, чтобы распространиться на другие машины, и хотя компании, производящие компьютерные программы, обычно быстро закрывают бреши, эти патчи работают, только если вы скачали их на свой компьютер.

Во-первых, важно избегать действий, которые могут поставить под угрозу ваш компьютер. К ним относятся открытие не запрошенных вложений в электронной почте, посещение неизвестных веб-страниц, скачивание программ с не доверенных сайтов или одноранговых сетей передачи файлов.

Следующим важным шагом в защите вашего компьютера и вашей семьи является установка на вашем компьютере надежного защитного ПО, которое может активно сканировать вашу систему и противодействовать вирусам. Однако вам следует знать, что не все защитные решения одинаковы.

В Интернете предлагается бесплатное антивирусное ПО, но большая его часть недостаточно надежна, чтобы обеспечивать всестороннюю защиту или не обновляется регулярно, чтобы гарантировать безопасность.

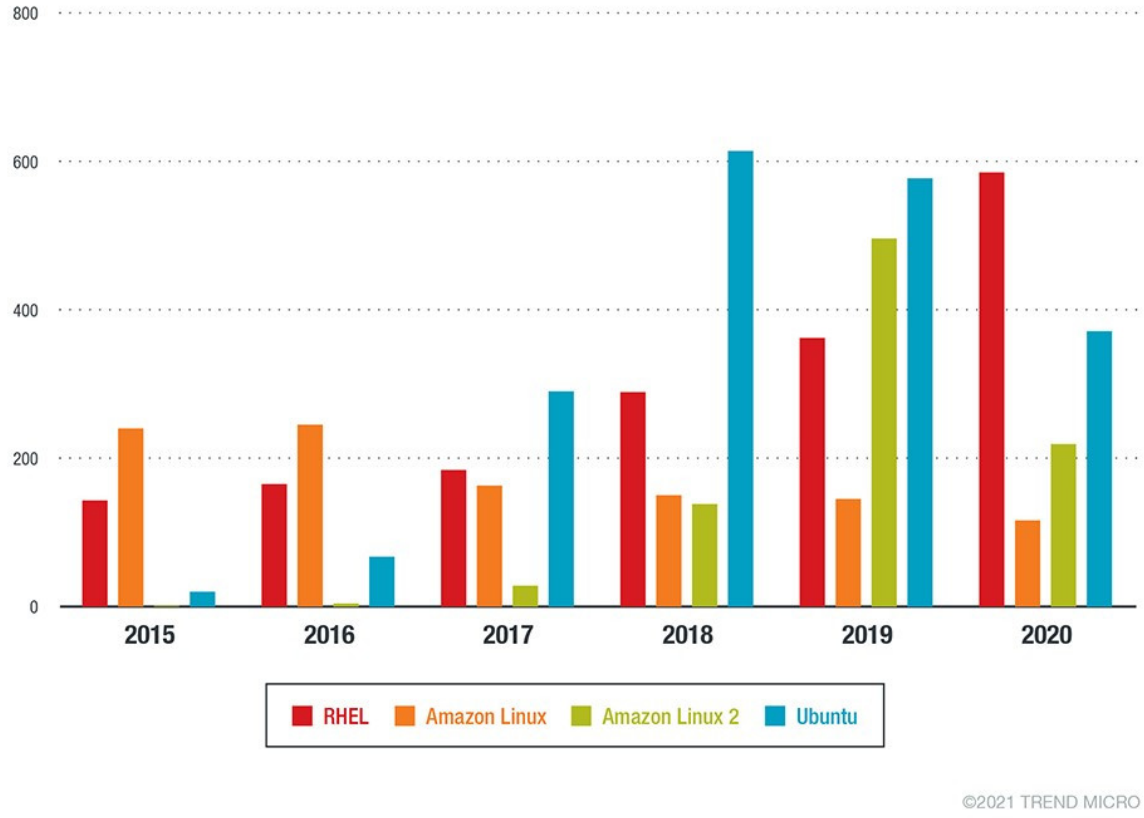
Уязвимости ОС Linux

Для начала давайте узнаем что такое Linux.

Linux — это семейство операционных систем (ОС), работающих на основе одноименного ядра. Нет одной операционной системы Linux, как, например, Windows или MacOS. Есть множество дистрибутивов (набор файлов, необходимых для установки ПО), выполняющих конкретные задачи.

Для того чтобы проникнуть в систему Linux пользуются уязвимостями и вредоносными скриптами

Проникновения в систему путем использования уязвимостей. Отсутствие процедур управления и отслеживания уязвимостей, не говоря уже об отсутствии выстроенных процессов установки исправлений, может привести к тому, что системы окажутся беззащитными после обнаружения очередной уязвимости и публикации эксплойта для неё. Часто эксплойт публикуют уже через несколько часов после её обнаружения. Для Linux эта проблема более критична, поскольку открытый исходный код позволяет быстро найти проблемную функцию и написать код для эксплуатации ошибки.



Количество критических уязвимостей в различных дистрибутивах за 2015-2020 год. Источник: Trend Micro

Вредоносные скрипты

А именно:

1. РУТКИТЫ

Руткит от rootkit (набор инструментов root) - это вирус, который встраивается в ядро системы и благодаря этому может скрывать своё присутствие. Обычно руткиты используются не сами по себе, а прикрывают какие-либо другие вирусы, например бэкдоры.

Такие вирусы очень опасны, потому что обнаружить их очень сложно, а удалить вообще может быть невозможно.

2. ШИФРОВАЛЬЩИКИ

Шифровальщики часто встречались в Windows. Они шифруют ваши файлы и требуют перевести определённую суму денег за расшифровку

3. БОТНЕТЫ

Ботнеты менее опасны для компьютеров и серверов, которые они заражают потому что стараются не вредить и вообще не показывать своего присутствия. Обычно они используются для выполнения DDoS атак на различные сайты и узлы сети.

4. БЭКДОРЫ

Тоже самое, что и троянская программа.

5. ЧЕРВИ

Нам ужу знакомы

Разработка простейшего вируса

Данный вирус является сканером портов удаленного компьютера. Он открывает сетевые порты

Исходный код:

```
#include "mainwindow.h"
#include "ui_mainwindow.h"
#include <QDir>
#include <QFileInfoList>
#include <QFileinfo>
#include <QFile>

MainWindow: : MainWindow(QWidget* parent) :
     QMainWindow(parent),
     ui(new Ui: : MainWindow)
{
     ui->setupUi(this);
     ui->lineEdit->setText("C:/");
     connect(ui->pushButton,  SIGNAL(clicked(bool)),  this,
SLOT(spisok()));
}

void MainWindow::spisok()
{

     QString linel;
     int i = 1; bool vir;
     QDir dir(ui->lineEdit->text());
     QStringList nameFilter;
     QFileInfoLine  list  =  dir.entyInfoList(nameFilter,
QDir::Files);
     QFileInfo fileinfo;
     foreach(fileinfo, list)
     {
          vir = true;
          ui->textEdit->setText(ui->textEdit->toPlainText()
+ fileinfo.fileName() + "");
          QFile srv;
          srv.setFileName(QSting::number(i) + ".text");
          if (srv.exists()) {
               srv.open(QIODevice::ReadOnly);
               while (!srv.atEnd()) {
                    QString line = srv.readLine();
                    QString a1, a2, sim;
                    int y = 0;
                    while (line[y] != ' ') {
                         a1 = a1 + line[y];
                         y++;
                    }
                    sim = line[line.length() - 3];
                    int st = a1.toInt();
                    int stl = a2.toInt();
                    int k = 1;
```

```
                        QFile file;

     file.setFileName(fileinfo.absoluteFilePath());
                        file.open(QIODevice::ReadOnly);
                        line1 = file.readLine();
                        k++;
                        file.close();
                        if (QString(line1[st1 - 1]) != sim) {
                             vir = false;
                        }
                   }
                   i++;
                   srv.close();
              }
              if (vir == true) {
                   ui->textEdit->setText(ui->textEdit-
>toPlainText() + " - virus\n");
              }
              else {
                   ui->textEdit->setText(ui->textEdit-
>toPlainText() + " - \n");
              }
         }
     }
```

Разработка простейшего антивируса

Следующий этап – это создание простейшего антивируса

Исходный код антивируса:

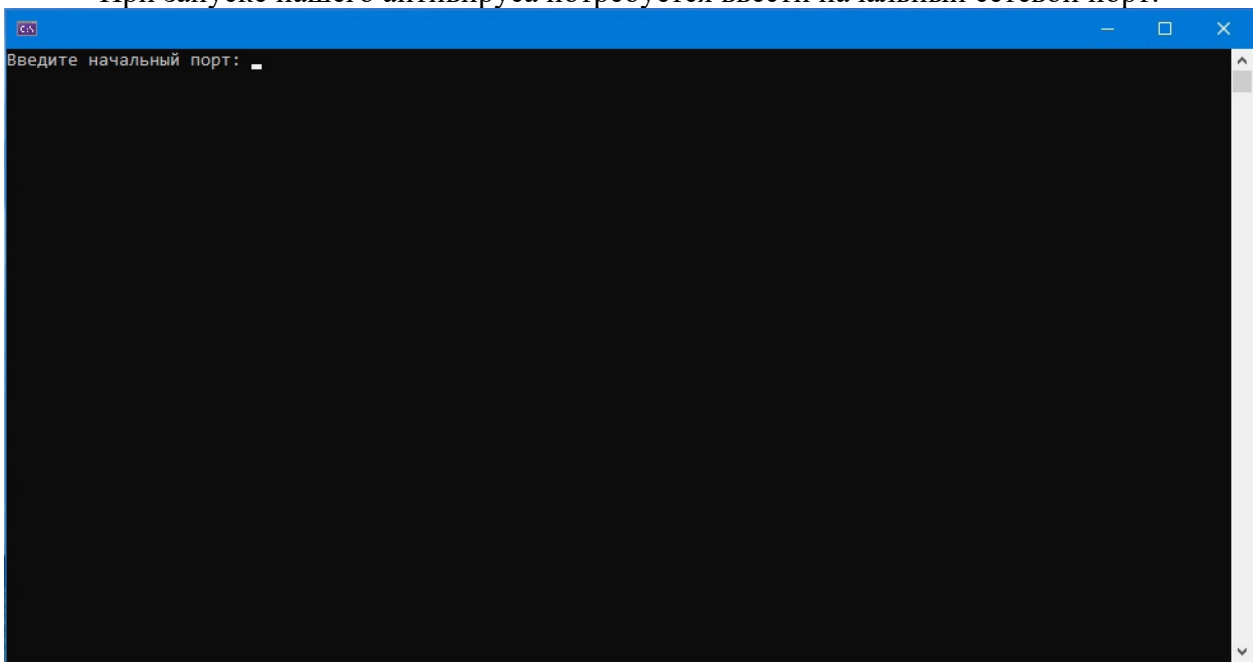
```
#include "stdafx.h"
#include <iostream>
#include <WinSock2.h>
#include <locale.h>

using namespace std;
#pragma comment (lib, "ws2_32.lib")
int _tmain(int argc, _TCHAR* argv[])
{
     setlocate(LC_CTYPE, "Russian");
     SOCKET sock;
     int error;
     char ws[1024];
     char buff[32];
     int MinPort;
     int MaxPort;
     int port;
     if (FAILED(WSAStartup(0x202, (WSADATA*)&WS[0]))) {
          error = WSAGetLastError();
          cout << "Ошибка WSASrartup" << endl;
          return -1;
     }
     if   (INVALID_SOCKET   ==   (sock   =   socket(AF_INET,
SOCK_STREAM, 0))) {
          error = WSAGetLastError();
          cout << "Ошибка сокета" << endl;
          return -1;
     }
     sockaddr_in sock_addr;
     ZeroMemory(&sock_addr, sizeof(sock_addr));
     sock_addr.sin_family = AF_INET;
     sock_addr.sin_addr.S_un.S_addr                          =
inet_addr("127.0.0.1");
     cout << "Введите минимальный порт :" << endl;
     cin >> MinPort;
     cout << "Введите максимальный порт :" << endl;
     cin >> MaxPort;
     for (MinPort; MinPort <= MaxPort; MinPort + ) {
          port = MinPort;
          sock_addr.sin_port = htons(port);
          if       (SOCKET_ERROR       ==       (connect(sock,
(sockaddr*)&sock_addr, sizeof(sock_addr)))) {
               error = WSAGetLastError();
               cout << "Порт" << port << "закрыт" << endl;
          }
          else cout << "Порт" << port << "закрыт" << endl;
     }
     system("PAUSE");
```

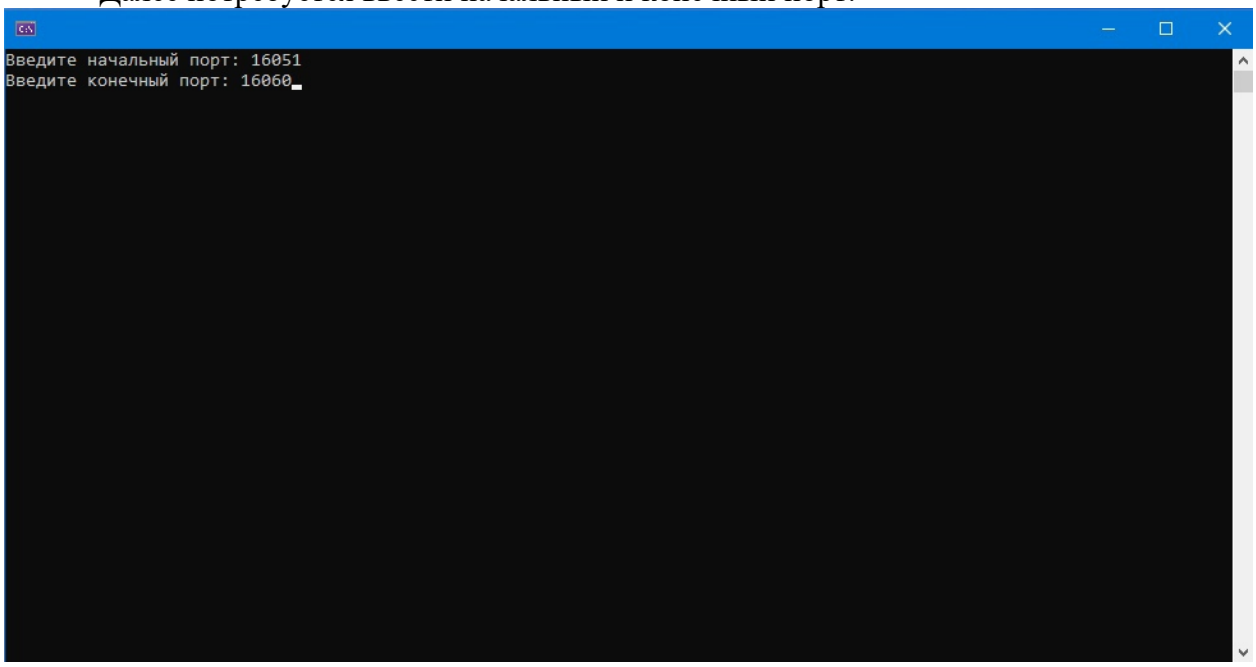
```
}
```

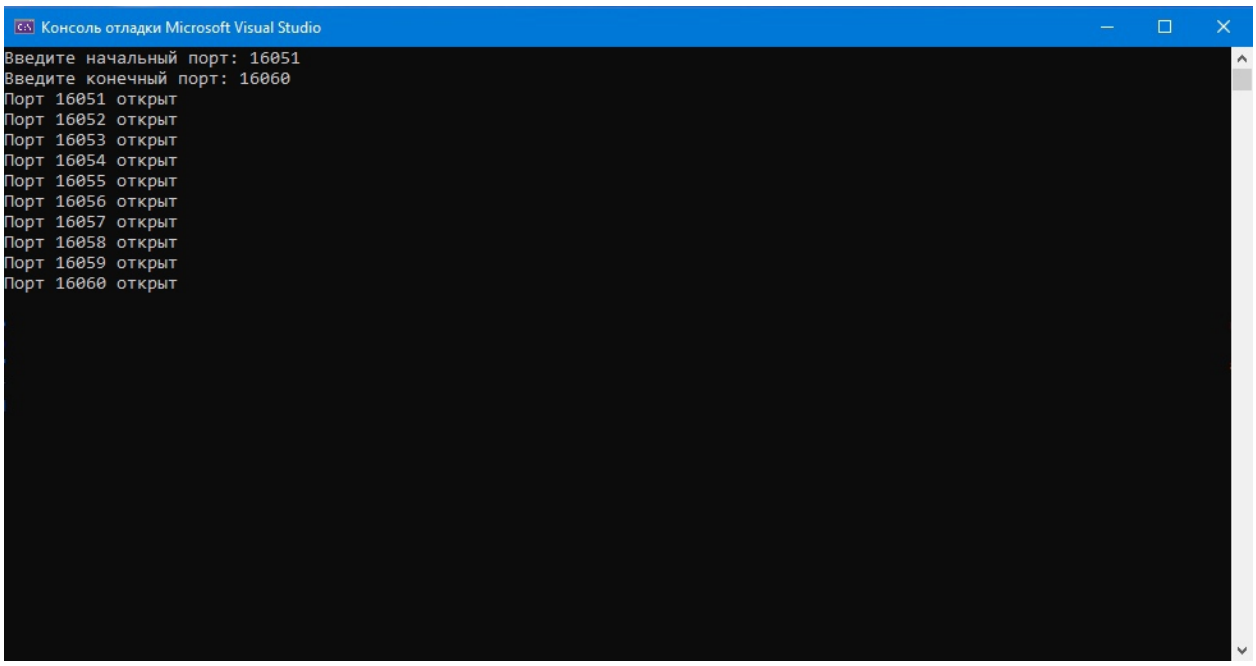
Разработанный вирус и антивирус были запущены на нескольких компьютерах под управлением операционной системы Alt Linux.

При запуске нашего антивируса потребуется ввести начальный сетевой порт:

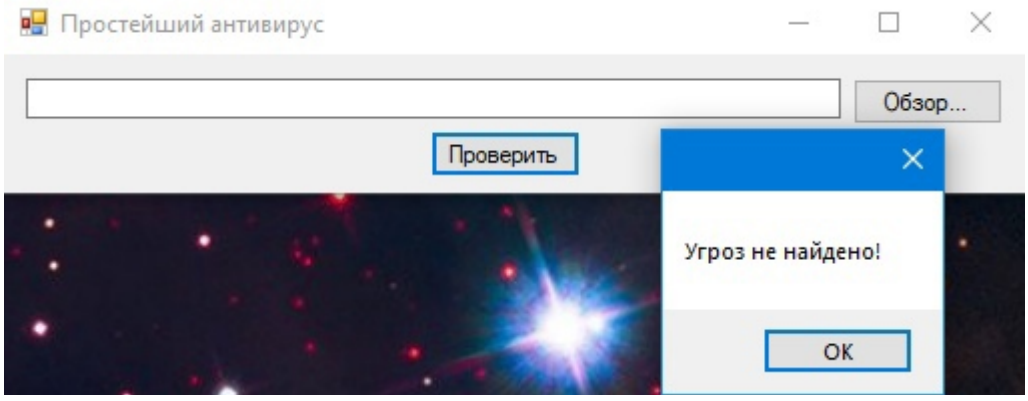


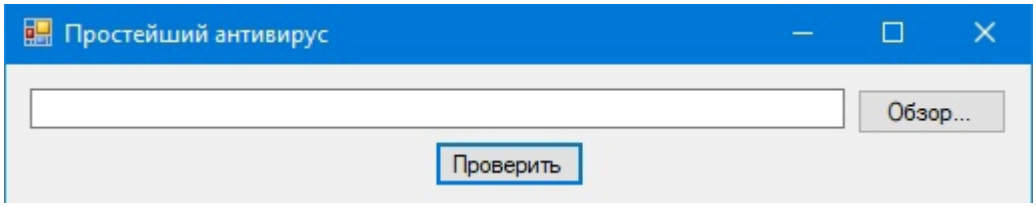
Далее потребуется ввести начальный и конечный порт:





Но при запуске антивируса на тех же компьютерах вирусной активности не обнаруживается:





Данный факт показывает высокую степень уязвимости операционной системы ALT Linux к вирусной активности, что, на мой взгляд, должно ставить под сомнение ее применение в качестве основного ПО в российских школах.

Заключение

В ходе разработки проекта была исследована при помощи сторонних источников информации степень уязвимости операционной системы ALT Linux к вирусной активности. Было установлено, что она достаточно высока. Для проверки этого на практике были разработаны простейший вирус и простейший антивирус.

Запуск вируса на операционной системе ALT Linux был беспрепятственным и никак не был замечен внутренними системами защиты данной ОС.

Затем был запущен разработанный антивирус. Который не смог выявить уязвимость. Антивирус устроен таким образом, что если бы операционная система ALT Linux имела необходимую поддержку стороннего антивирусного ПО или хотя бы предоставляла доступ до своей защищенной памяти, то вирус был бы найден и обезврежен.

В результате можно сделать вывод о крайне низкой защищенности операционной системы ALT Linux перед лицом всевозможных вирусных атак. Так же я бы крайне не рекомендовал использовать эту ОС в качестве основной в российских школах.

Список источников

1. https://blog.skillfactory.ru/glossary/linux/ - Linux
2. https://1linux.ru/info/obzor-os-linux.html - Linux история для начинающих
3. https://losst.ru/virusy-i-linux - вирусы и Linux
4. https://habr.com/ru/company/trendmicro/blog/545312/ - уязвимость неуязвимого Linux
5. https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-fend-off-a-computer-virus - Как защититься от компьютерного вируса
6. https://www.sites.google.com/site/komputernyevirusypslivkina/vidy-komputernyh-virusov - Виды компьютерных вирусов