Научное общество учащихся «Эврика»

МУНИЦИПАЛЬНОе АВТОНОМНОЕ ОБЩЕобразовательное учреждение «ЛИЦЕЙ № 38»

Советского района г. Нижнего Новгорода

Анализ современных антивирусных программ

Выполнил:

Касаткин Денис

ученик 10"Г" класса

Руководитель:

Быстрова Ася Викторовна

учитель информатики

Нижний Новгород

2023

Оглавление

[Введение 3](#_Toc99070609)

[1. Теоретическая часть 4](#_Toc99070610)

[1.1. Понятие антивирус и его основные критерии 4](#_Toc99070611)

[1.2 Типы антивирусных программ и принцип работы 5](#_Toc99070612)

[1.3 Популярные антивирусные программы и их характеристика 6](#_Toc99070613)

[2. Практическая часть 8](#_Toc99070614)

[2.1 Написание экспериментального Trojan-PSW 8](#_Toc99070615)

[2.2 Тестирование программы в разных видах 9](#_Toc99070616)

[3. Рейтинг антивирусных программ 12](#_Toc99070617)

[4. Выводы: 13](#_Toc99070618)

[5. Список использованной литературы 14](#_Toc99070619)

[Приложение 15](#_Toc99070620)

# **Введение**

На данный момент компьютер и различные гаджеты плотно вошли и закрепились в нашем быту. Они облегчают нашу жизнь. Количество информации, которую люди доверяют своему «электронному другу», с каждым днем растет. С ними растет количество мошенников, которые распространяют вредоносное ПО.

Чтобы справиться с ними, необходимо создавать более универсальные и новые антивирусные программы

**Актуальность**

С активным развитием глобальных сетей актуальным является вопрос информационной безопасности, так как проникающие из сети вирусы могут нарушить целостность и сохранность нашей информации. Для защиты от них стоит устанавливать антивирусные программы, а самое главное, чтобы они были актуальными. Есть различные типы антивирусных программ и каждый из них защищает ПК по-разному.

**Цель работы:** Провести исследование и проанализировать современные антивирусные программы.

**Задачи проекта:**

* раскрыть основные понятия антивирусных программ;
* изучить разновидности и типы антивирусных программ;
* на основе полученных данных написать свою вредоносною программу;
* провести ее тестирование;
* провести исследование, какой антивирус лучше справится с задачей;
* составить рейтинг антивирусов, которые прошли этапы;
* подвести итоги.

**Гипотеза**: Не каждый антивирус сможет пройти все этапы и обнаружить агента в файле, не все сервисы смогут подтвердить статус «полностью надежного».

# Теоретическая часть

# Понятие антивирус и его основные критерии

**Антивирусная программа** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ. Предотвращения заражения файлов или операционной системы вредоносным кодом.

Из-за огромного количества новых антивирусов пользователям становится трудно выбирать наиболее подходящий. Стоит руководствоваться определенными критериями, которые каждый пользователь определяет для себя сам. Но мы собрали базовые критерии для каждого антивируса, которые мы будем использовать при оценке.

1. **Надежность и удобство работы** – отсутствие зависаний антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
2. **Качество обнаружения вирусов**. Проверка внутри файлов, документов.
3. **Кроссплатформенность**. Существование версий антивируса под все популярные платформы.
4. **Мощность**. Скорость работы и полезные функции.

Следует отметить, что нужно отличать пассивный режим работы антивируса и активный. Пассивный режим – это когда антивирус свёрнут в трей и мониторит работу компьютера, а активный – когда вы самостоятельно запустили проверку компьютера на вирусы или производите другое активное действие.

# Типы антивирусных программ и принцип работы

Суть работы антивируса заключается в его алгоритмах, благодаря которым распознаётся наличие вирусов в компьютере. Обнаружение вирусов происходит по их активности или по определённым действиям. Большинство вирусов постоянно вносятся в базу, с помощью которых антивирус легко находит вредную программу. Также есть и новые вирусы, которые пока не известны разработчикам антивирусов и не внесены в антивирусные базы. Алгоритмы антивируса контролируют активность файлов и приложений и при их подозрительных действиях информируют пользователя. Есть много способов обнаружения.

На данный момент выделяют 4 типа работы антивирусов:

**1. Сканеры**— антивирус ищет наличие вируса в базе. Качество сканирования зависит от даты обновления баз данных. Пример: Утилита Dr.Web

**2. Ревизорный модуль**— запоминает состояние файловой системы, что в последствии дает возможность сравнить отличия и сопоставить результаты. В случае отличия, вирус ловиться.

**3. Мониторы**— это специальный программы, которые выявляют потенциально опасное вредоносное ПО. Далее, пользователю дается выбор, на основе которого программа выполняет действие.

**4. Иммунизаторы**— принцип действия этого модуля напоминает вакцину. Когда вирус хочет проникнуть и заразить программу, то вакцина показывает вирусу, что программа уже заражена. Данный способ уже устарел.

# Популярные антивирусные программы и их характеристика

Мы собрали список антивирусов, которые стоят по скачиванию на первых позициях. Им больше всего отдают свое предпочтение пользователи и доверяют.

**ESET NOD32 Smart Security** – обеспечивает защиту персональных компьютеров и корпоративных систем. Преимуществами является быстрая работа, способность ловить большую часть вирусных программ. Из минусов, это влияние на производительность ПК.

**360 Total Security** – основной тип работы: облачный сканер. Отлично блокирует кейлоггеры и мелкие программы перехвата данных (стиллеры). Минимальная нагрузка на ПК, многофункциональность, которая заключается в использовании нескольких типов защиты. Основной минус – это Неспособность заблокировать зараженный файл до того, как он был загружен

**Kaspersky Internet Security** – это превосходный антивирус, который «проверен веками». Встроены уникальные технологические компоненты, позволяющие пользователю отслеживать все происходящие на компьютере изменения и контролировать поведение документов в формате MS Office, обеспечивая эти документы дополнительным уровнем безопасности. Из плюсов: защита устройств ввода, использование нескольких типов антивирусов, режим безопасных платежей. Из минусов: потребление ресурсов ПК в большом количестве и реклама, даже на платных тарифах.

**Avast Free Antivirus**- Система предусматривает защиту от вирусов-шифровальщиков, проведение безопасных интернет-платежей, улучшенная производительность. Модуль поведения позволяет отследить подозрительную активность некоторых приложений, таким образом блокируя работы шифровальщиков. С помощью веб-экрана все страницы сканируются, защищая пользователей от вирусных атак. Еще к плюсам нужно отнести проверку Wi-Fi потока. К большому сожалению слабая защита от фишинга

**Dr.Web Antivirus** - Антивирусная программа гарантирует комплексную защиту от всех интернет-угроз. Одно из сильных преимуществ сервиса — может очистить уже поврежденный ПК. С помощью специальной облачной технологии антивирус может проверять почту и ссылки в реальном времени. Наличие хорошего изолирующего карантина. Из минусов: потребление большого количества оперативной памяти, требование перезагрузки ПК.

**AVG AntiVirus Free Edition** - показывает хорошие результаты в тестах независимых лабораторий. Предназначен для защиты от вирусов, шпионских программ и оптимизации устройств. Софт отличается хорошей блокировкой угроз: запрещается доступ к сайтам с потенциальными угрозами, прерывается скачивание небезопасных программ. Даже если приложение попало на компьютер, все равно перед запуском выполняется дополнительная проверка и запрашивается доступ на удаление. К минусам – неудобное приложение, по сравнению с конкурентами и защита от фишинговых ПО оставляет желать лучшего.

**Microsoft Security Essentials –** является встроенным ПО для начальной защиты от троянов, программ-шпионов и вредоносного ПО. Антивирус работает со стандартным брандмауэром. Если была замечена передача вредоносного кода, система автоматически блокирует сетевое соединение.

Главный минус: слабый уровень обнаружения.

Все перечисленные антивирусы обладают хорошим интерфейсом и имеют дополнительные функции, которые облегчают работу пользователя. Имеют кроссплатформенность.

# Практическая часть

# Написание экспериментального Trojan-PSW

Теперь основной задачей стоит проверить статус всех перечисленных антивирусов. Смогут они пройти тесты и доказать свою защиту?

Для начала нужно выбрать тип нашего вредоносного ПО. Мы решили рассмотреть 2 типа распространенных мошеннических типа вируса. Это RAT и PSW.

RAT – программа, с помощью которой злоумышленник может получить удалённый доступ к компьютеру. Дословно аббревиатура означает Remote Access Trojan – программа троян для удалённого доступа. Злоумышленник выгружает все данные с компьютера, с помощью которых он может получить доступ к нужным ему ресурсам. За счет получения удаленного доступа к компьютеру жертвы, злоумышленник может помешать препятствию своим действиям. Избавление от такого типа вирусов возможно только полным сбросом системы.

Однако, тип такого вируса хорошо блокируется антивирусами и для написания работоспособного RAT понадобится знание языков программирования на высоком уровне.

PSW- Trojan – вредоносная программа, предназначенная для кражи

пользовательских аккаунтов с пораженных компьютеров. Название **PSW** произошло от Password-Stealing-Ware При запуске PSW-троянцы ищут необходимую им информацию системных файлов, хранящих различную конфиденциальную информацию. В случае успешного поиска программа отсылает найденные данные «хозяину». Может использоваться, как кейлоггер.

Программа, которая не сложна в написании и реже попадается в поле зрения антивирусных программ. Но при этом, наносит пользователю не меньший вред. Именно ее мы реализуем и протестируем на антивирусах.

Мы создаем учебную версию вируса, поэтому нам будет достаточно языка программирования Python. Работа начинается с подключения нужных библиотек (Приложение 1).

Далее мы начинаем сбор паролей и cookie файлов. Под удар мы берем самые популярные браузеры: Google, Yandex, Opera, FireFox. Прописываем так же, создание скриншота рабочего окна, общих данных о компьютере, архивирование полученных данных и отправку через Telegram и E-mail. Использовать так же можно отправку на выделенный сервер или GitHub. Но мы все делаем в ознакомительных целях без распространения, поэтому нам двух работоспособных сервисов будет достаточно.

Однако, сервисы E-mail начали блокировать вход и отправку файла. Пришлось подбирать и перебирать сервисы, чтобы найти без защиты.

# Тестирование программы в разных видах

Теперь, код мы начинаем проверять через сайт VirusTotal.com, что помогает проверить мой вирус среди порядка 61 антивируса. И по исходу проверки мы получили удивительные результаты. Только 4/61 антивирусов увидели в моем коде Агента. Среди них: Avast,Kaspersky,AVG. Это сервисы из моего списка, которые определили Стиллер (Приложение 2).

Далее, собираем файл в exe. Отправляем на повторную проверку и получаем отличные результаты. AVG не смог обнаружить в exe файле программу-мошенника, но ESET NOD32нашел в файле вора (Приложение 3).

Теперь файл нужно скрыть и уменьшить количество обнаружений.

Мы воспользовались программами по шифрованию, но многие антивирусы легко распознали попытку обойти их систему и количество обнаружений увеличивается. Даже те антивирусы, которые изначально не видели в файле ничего странного, начинают жаловаться исключительно на попытку шифрования.

Одним из самых простых методов скрыть вредоносную, мошенническую программу - заархивировать ее. Заархивировав файл с помощью WinRAR мы снизили количество детектов с 5 до 3. А из популярных антивирусов остался только NOD32. Зачастую мошенники используют именно такой метод доставления своего ПО на компьютер жертвы. (См.Приложение 4)

Однако, мне такой результат показался удивительным. Ведь код программы крайне прост и должен быть сдержан антивирусами, но этого не происходит. Тогда, мы на виртуальной машине запускаем файл. Спустя 1,5 минуты мне приходит уведомление. Программа успешно завершила свою работу и все данные успешно получил. Мы повторили действия несколько раз с небольшим временным интервалом (Приложение 5).

Подождав время, мы повторно отправляем файл на проверку антивирусами. Получаю старый результат. Но, буквально через 30 минут, мы получаем скриншот и 1 файл от неизвестного мне источника. Не поняв, откуда они появились, мы проигнорировали данное действие. Через 2,5 часа мы получаем очередное оповещение о получении данных. Решив углубиться в полученные мной данные, мы не находим абсолютно ничего. Почти полностью пустой скриншот рабочего стола, а данные имеют не полный набор, а в имеющихся нет должной информации. Тогда, мы выдвигаем теорию, что это может быть виртуальная машина антивирусных программ. Отправляю сайт на повторную проверку и буквально через минуту мы получаем новые данные от моей программы. Ничего не изменилось, тот же пустой рабочий стол, с запущенной командной строкой. Через 2 часа повтор и через час мы снова получаем данные (Приложение 6).

Изучив подробнее эту систему, моя теория подтверждается. На рабочем столе одного из скриншотов мы видим зацепку. Файлы с названиями: notes, report. А в командной строке мы видим директорию D:\TOOLS (Приложение 7). Продолжаем рассмотрение и видим, что единственный полученный файл из списка (history.txt), содержит одинаковые строки, что означает работу одной и той же машины, а значит одного и того же антивируса. Можно было бы получить 100 процентное доказательство, однако, файл alldata.txt получен не был. Видим, что разрешение у всех скриншотов 800х600, а такое разрешение имеют очень старые мониторы. Взяв другой скриншот, мы видим группу файлов, разного расширения, но имеющие одинаковое имя (Приложение 8).

Таким образом мы видим работу антивирусов, которые работают по принципу «Мониторы». В дальнейшем, при обнаружении вируса, такие антивирусы блокируют его и заносят в базу.

Исходя из полученных знаний и итогов работы, мы получаем информацию. Основная часть антивирусов работают по принципу «Сканеры». Пользуются готовой базой данных. Это видно из реакции антивирусов, на попытку шифрования. И основной ориентир для них является загрузка на компьютер сторонних файлов. Меня крайне удивило, что антивирусы для проверки используют виртуальные машины, ведь информации мы в интернете не нашли по этой теме.

# Рейтинг антивирусных программ

Исходя из экспериментов, поставленных мной, можно составить рейтинг антивирусов, которые отлично подойдут для предотвращения работы мошеннических программ.

1. **ESET NOD32 Smart Security – отлично выполнил свою работу. Прошел 2 из 3 испытаний успешно.**
2. **Kaspersky Internet Security – прошел 2/3 испытаний, но уходит на второй план, так как не смог отработать с заархивированным файлом.**
3. **AVG AntiVirus Free Edition – прошел 1/3 испытаний, смог обнаружить PSW только в чистом коде.**
4. **Avast Free Antivirus – прошел 1/3 испытаний, обнаружил PSW только в чистом коде.**

Остальные антивирусы не обнаружили агента вообще, но имеют свои преимущества и недостатки.

# Выводы:

1. Антивирусы не всегда смогут защитить ваш компьютер от вирусов, особенно от тех, которые не загружают на компьютер дополнительных файлов.
2. Проведя ряд экспериментов, я подтвердил свою гипотезу

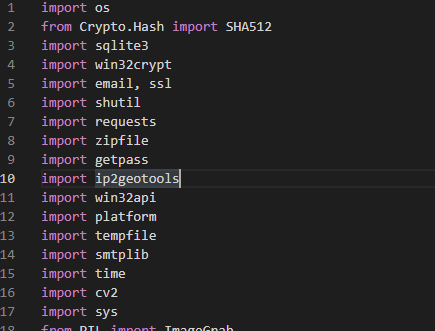
Ежедневно десятки тысяч пользователь попадаются на уловки мошенников. Люди, уповая на антивирусы, забывают про безопасность. Своей работой я показал, как легко внедрить PSW троян на компьютер, получить данные, которые после могут быть использованы против пользователя. Антивирусы далеко не всегда могут защитить ваш компьютер от всех источников опасности. Поэтому, стоит скачивать что-то из сети Internet только с проверенных источников. Я все выполнил в ознакомительных целях и не занимался распространением вредоносной программой.

# Список использованной литературы

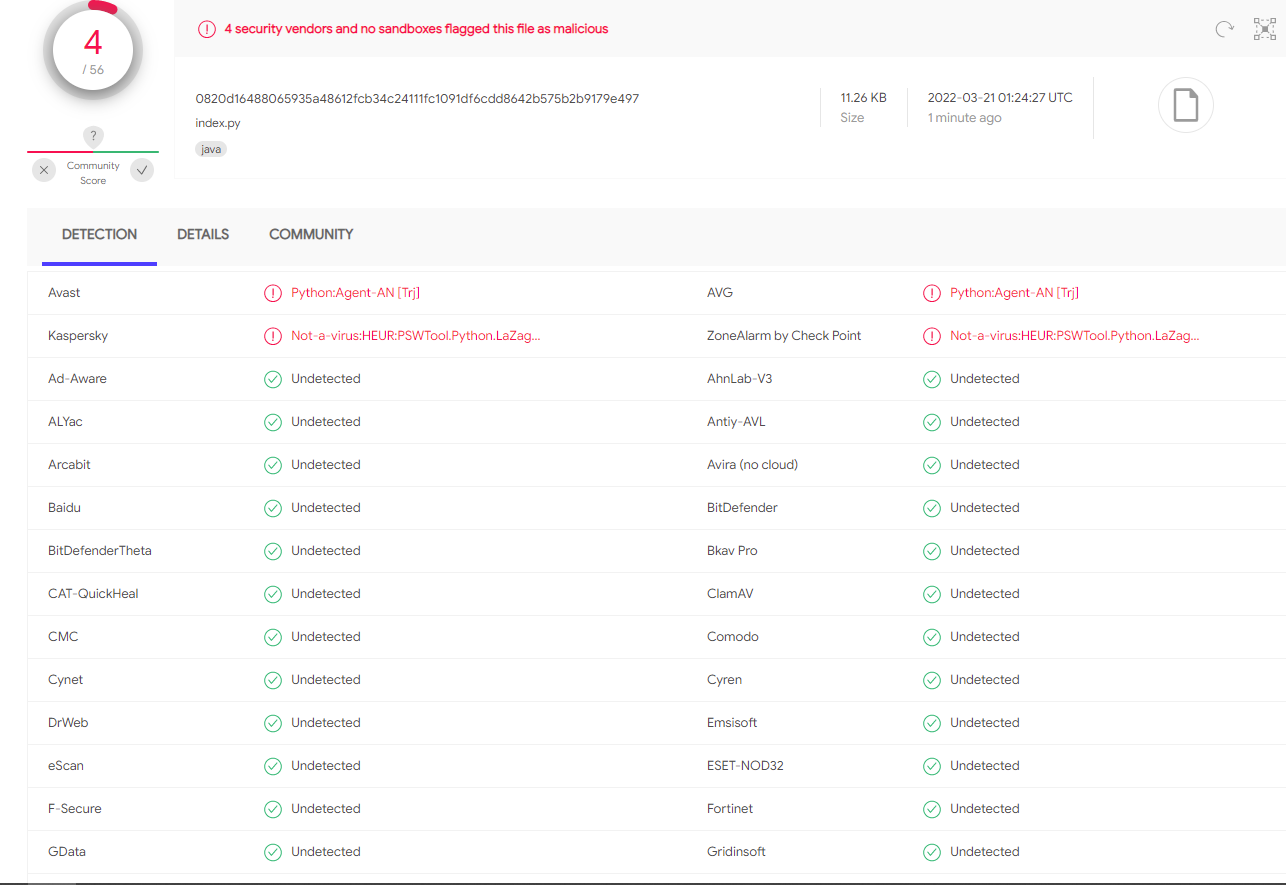
* <https://ru.wikipedia.org/wiki/Trojan-PSW>
* <https://ru.wikipedia.org/wiki/RAT>
* <https://habr.com/ru/company/drweb/blog/532444/>
* <https://virustotal.com>
* <https://edu.tltsu.ru/er/book_view.php?book_id=2792&page_id=31408>
* <https://ru.wikipedia.org/wiki/Антивирусная_программа>

# Приложения

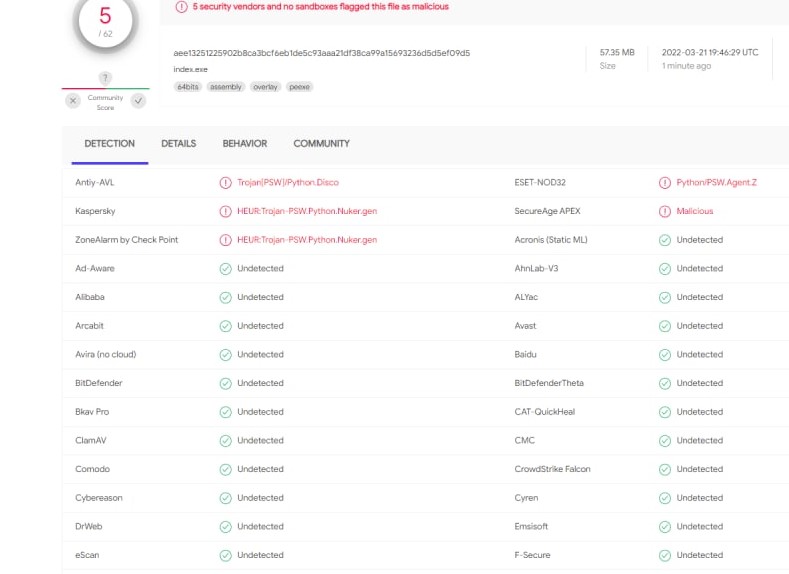
1)



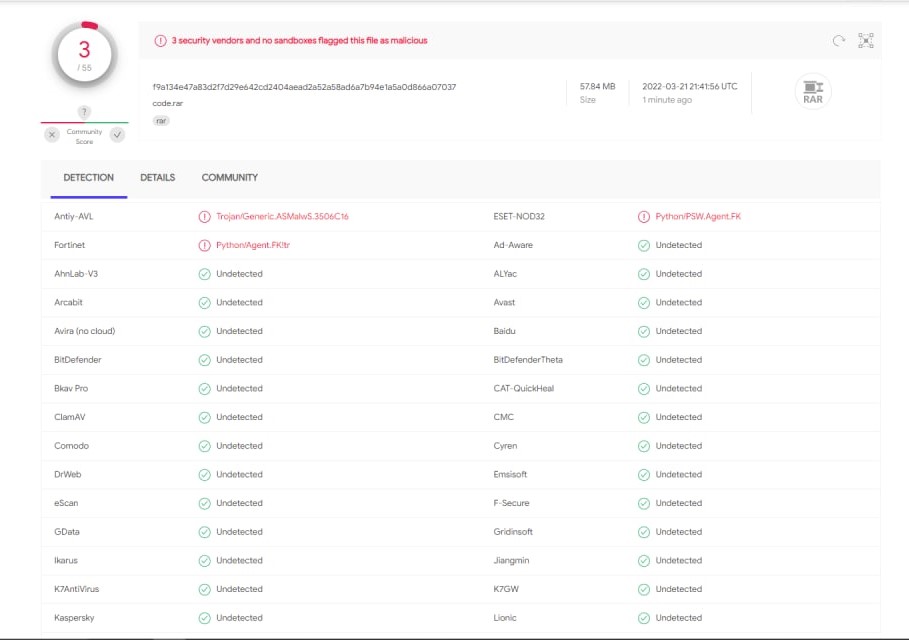
2)



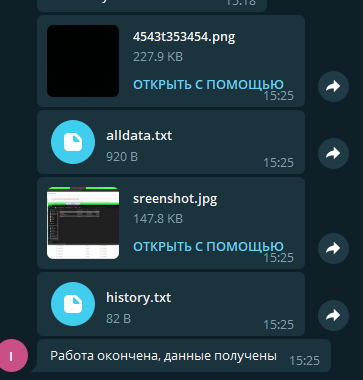
3)



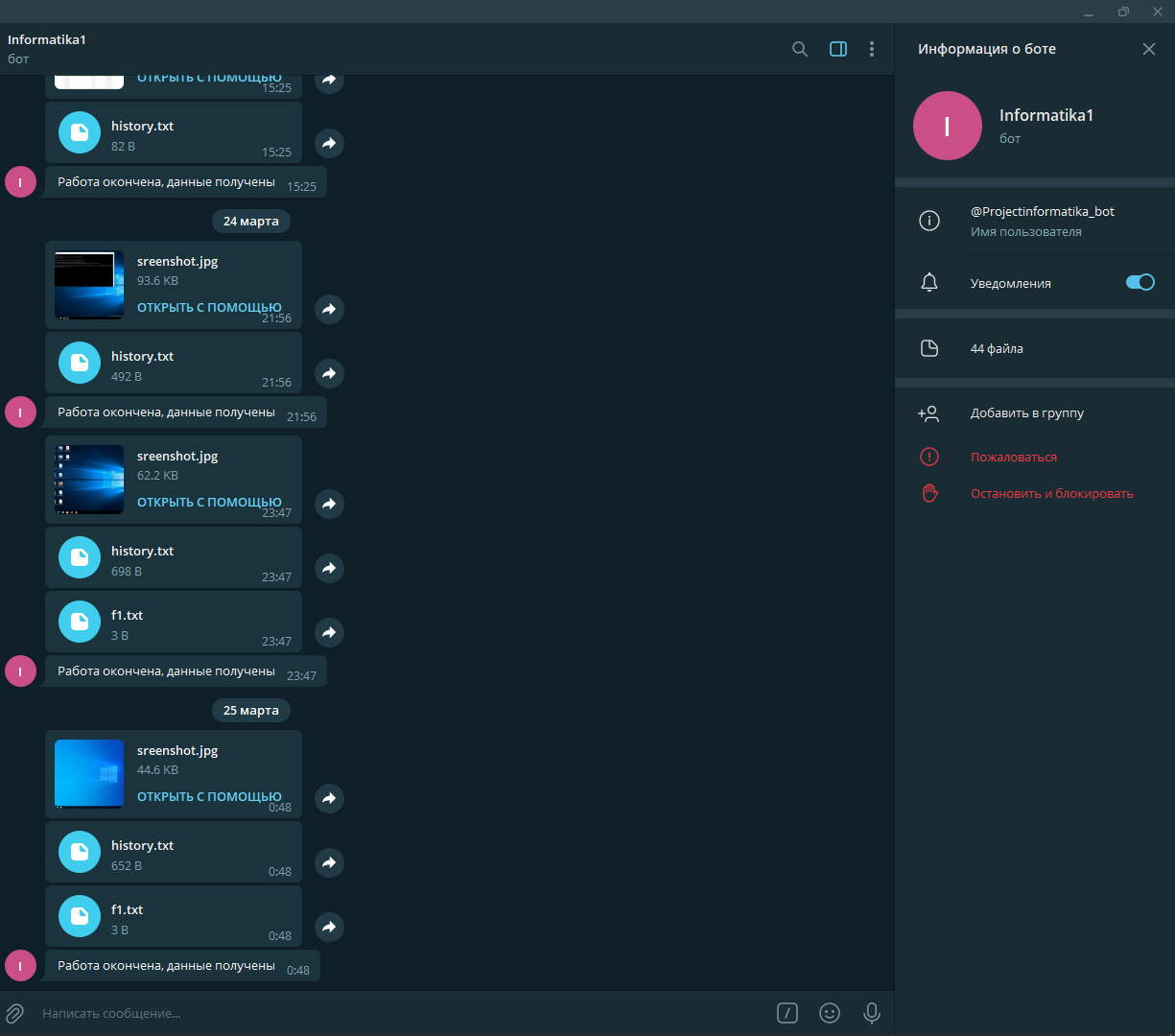
4)

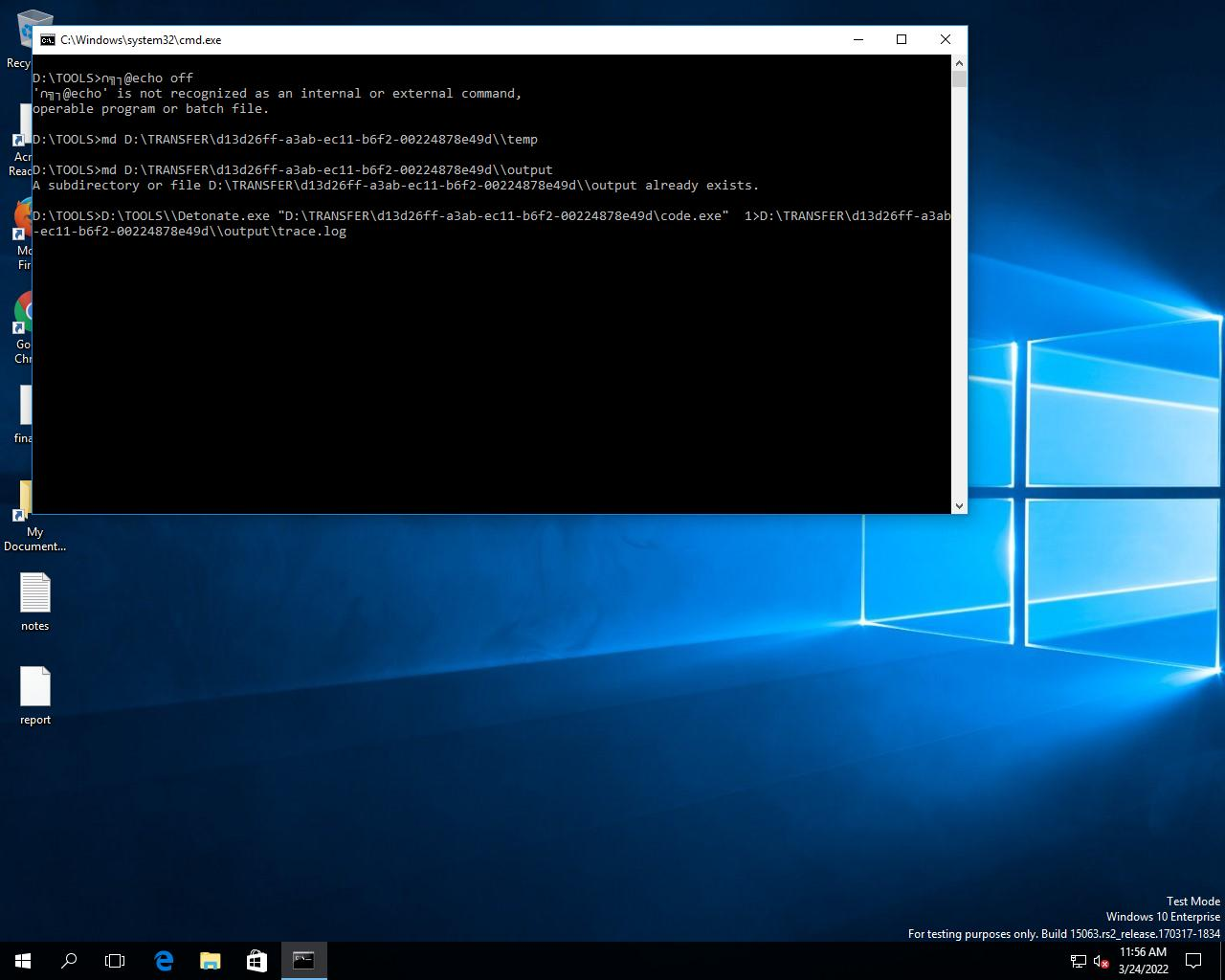


5)



6)



7)  


8)  
