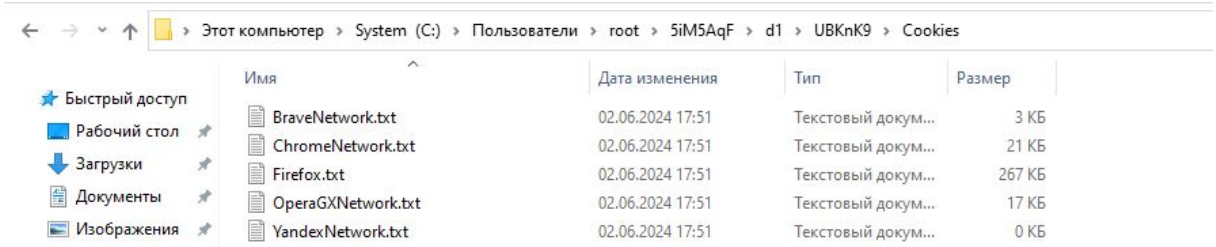
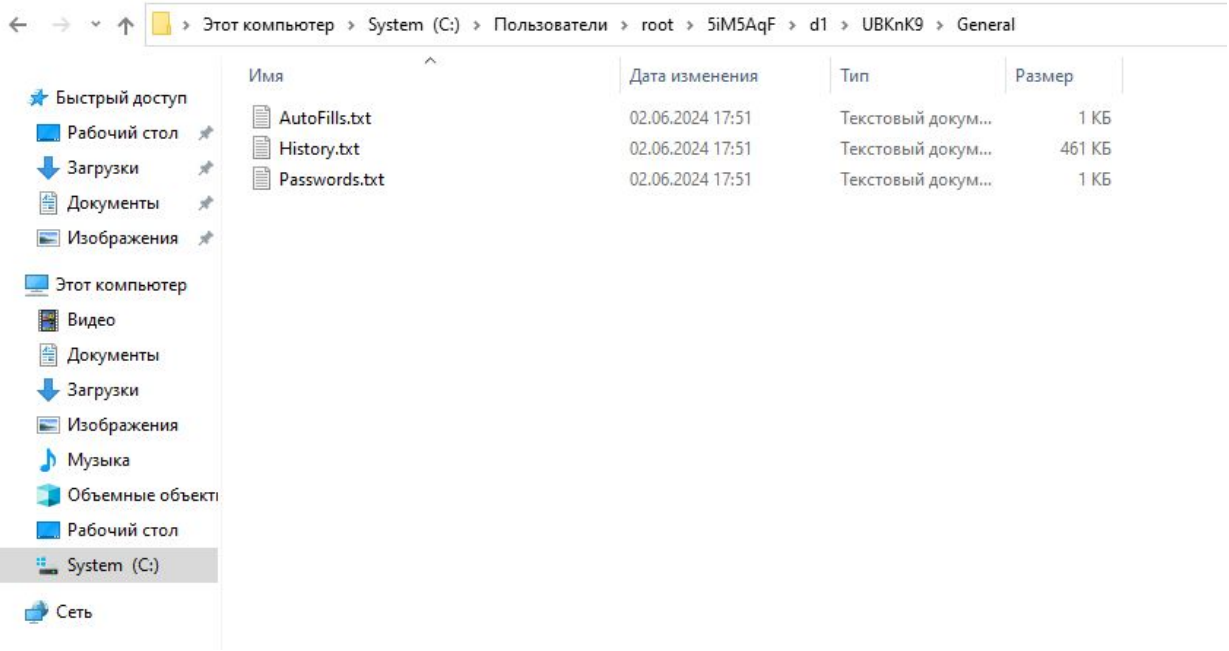
Stealer Xabarovsk

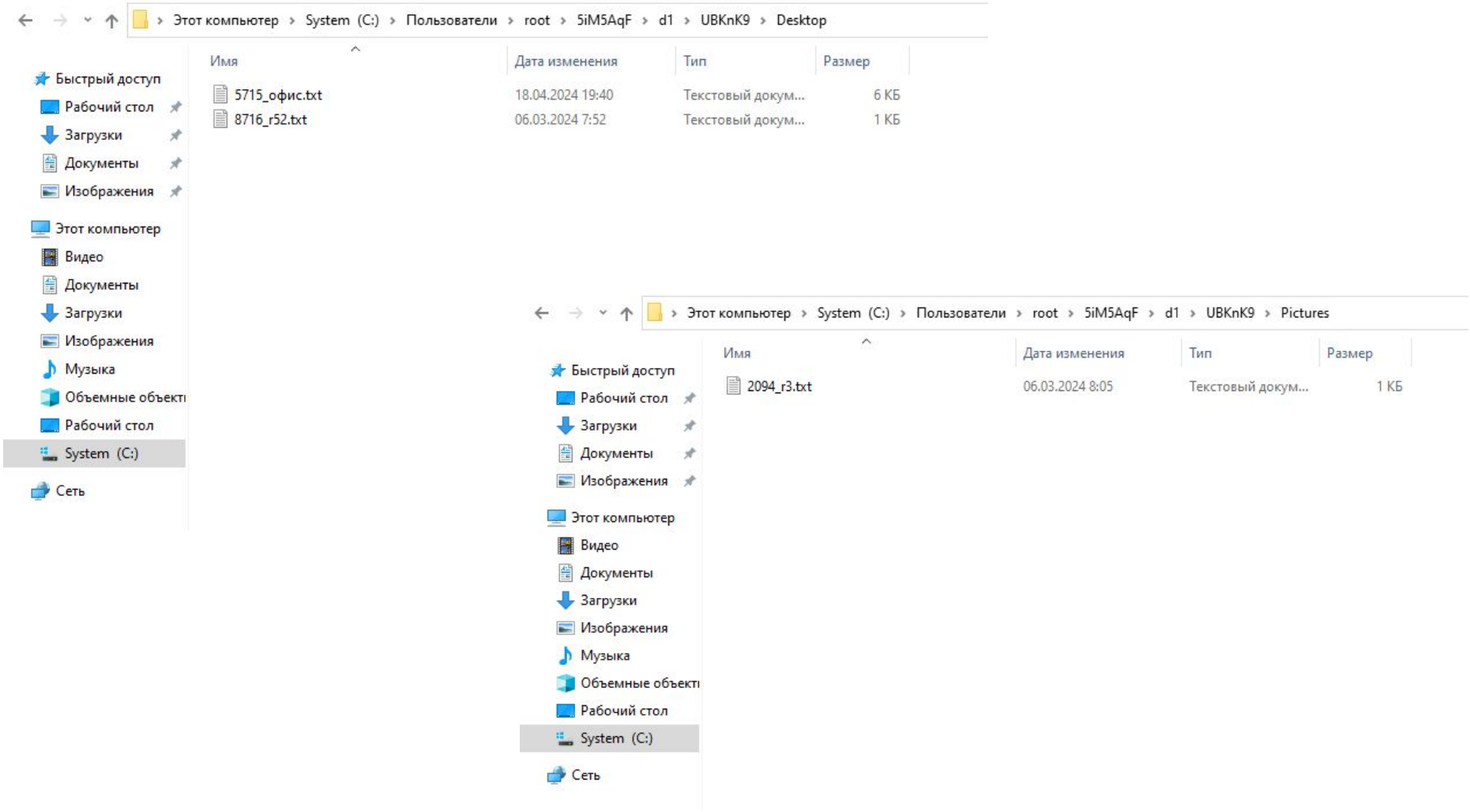
Stealer Xabarovsk (Win | чистая Java) — это программа, которая предназначена для сбора и переноса на удаленный сервер конфиденциальных данных с устройства пользователя . Xabarovsk предназначен для следующего:

1. Сбор логинов и паролей со всех популярных браузеров(
   Brave
   Chrome
   Edge
   Firefox
   Opera
   OperaGX
   Vivaldi
   Yandex
), такие как учетные записи веб-сайтов, куки, данные банковских карт, история посещений, логины и пароли(расшифровка на стороне пк, а не сервера), расширение.


Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 › Cookies
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
Имя
Дата изменения
Тип
Размер
BraveNetwork.txt 02.06.2024 17:51 Текстовый докум... 3 КБ
ChromeNetwork.txt 02.06.2024 17:51 Текстовый докум... 21 КБ
Firefox.txt 02.06.2024 17:51 Текстовый докум... 267 КБ
OperaGXNetwork.txt 02.06.2024 17:51 Текстовый докум... 17 КБ
YandexNetwork.txt 02.06.2024 17:51 Текстовый докум... 0 КБ


Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 › General
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
Имя
Дата изменения
Тип
Размер
AutoFills.txt 02.06.2024 17:51 Текстовый докум... 1 КБ
History.txt 02.06.2024 17:51 Текстовый докум... 461 КБ
Passwords.txt 02.06.2024 17:51 Текстовый докум... 1 КБ

2. Сбор файлов с Рабочего стола и папки Документов(
   Расширение
      txt
      pdf
      png
      jpg
      jpeg
   пути: pictures, desktop
): сбор происходит рекурсивно, проходит по всем папкам и подпапкам и собирает все файлы с нужным расширением. Файлы копируются и передаются на удаленный сервер.


Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 › Desktop
Имя
Дата изменения
Тип
Размер
5715_офис.txt
18.04.2024 19:40
Текстовый докум...
6 КБ
8716_r52.txt
06.03.2024 7:52
Текстовый докум...
1 КБ
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 › Pictures
Имя
Дата изменения
Тип
Размер
2094_r3.txt
06.03.2024 8:05
Текстовый докум...
1 КБ
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть

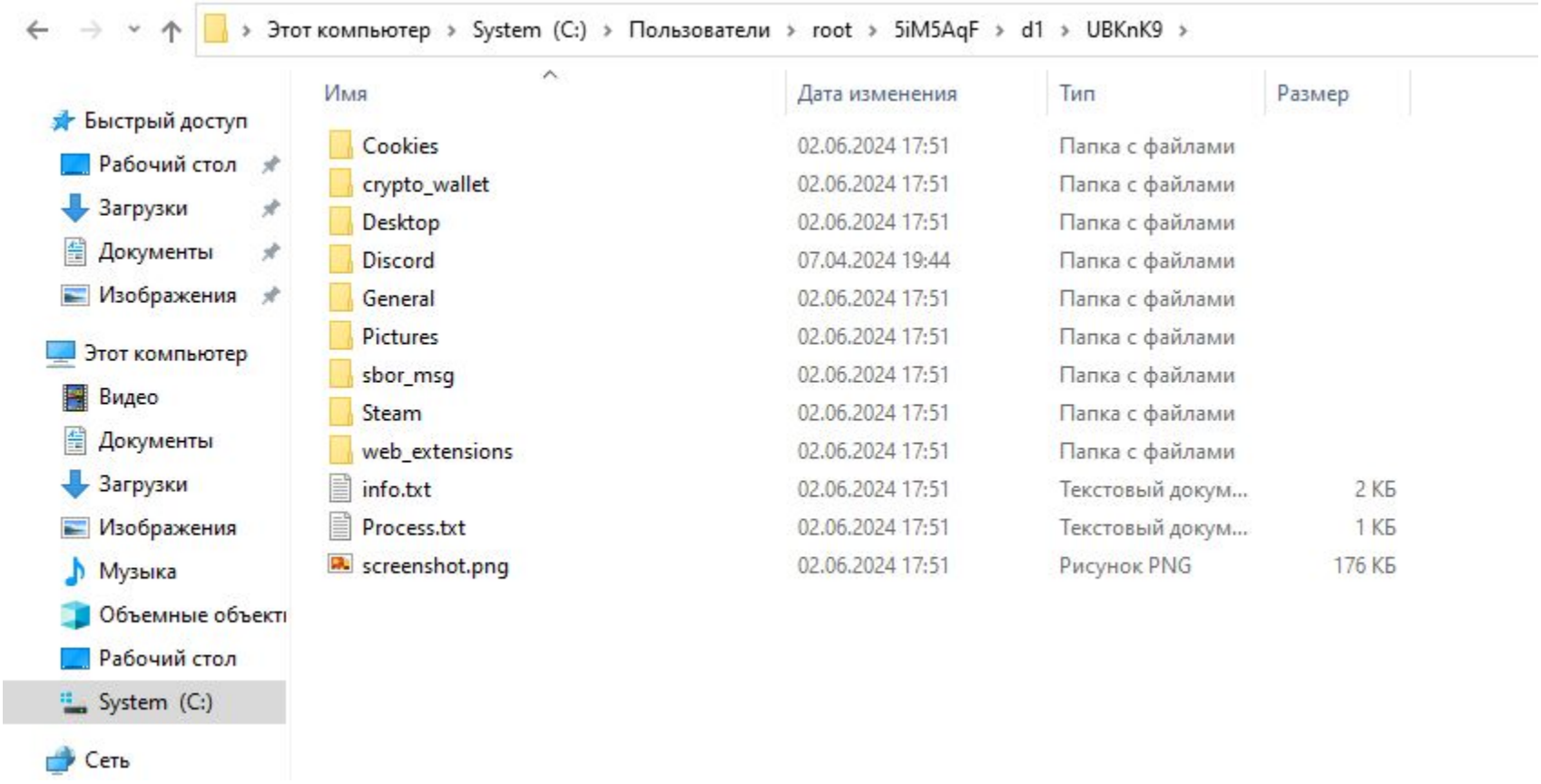
3. Сбор учетных записей и сессий популярных десктопных приложений:

Telegram

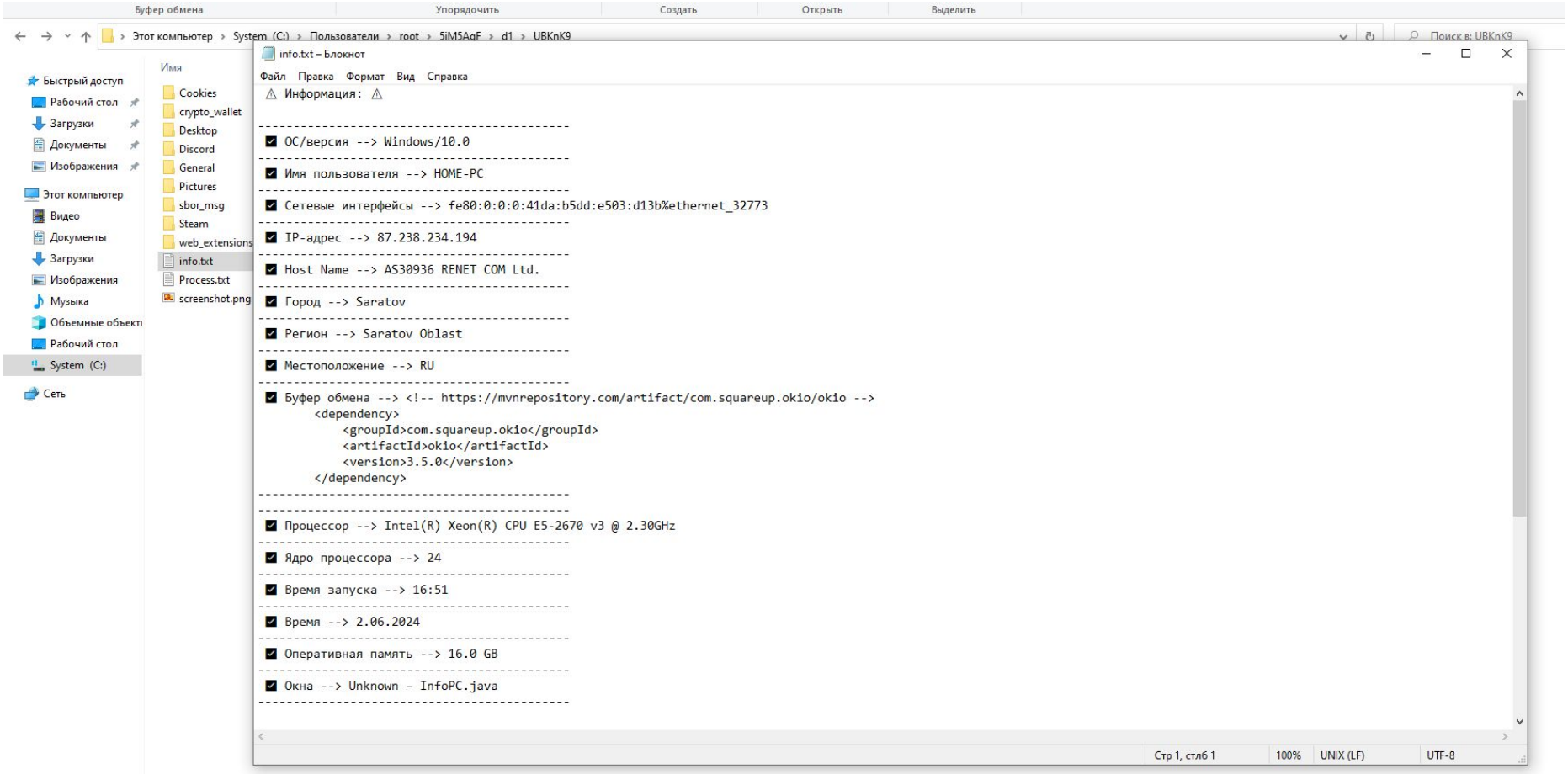
Steam

Discord

Телеграм - tdata, дискорд и стим - как браузер(token), так и с десктопная версия.

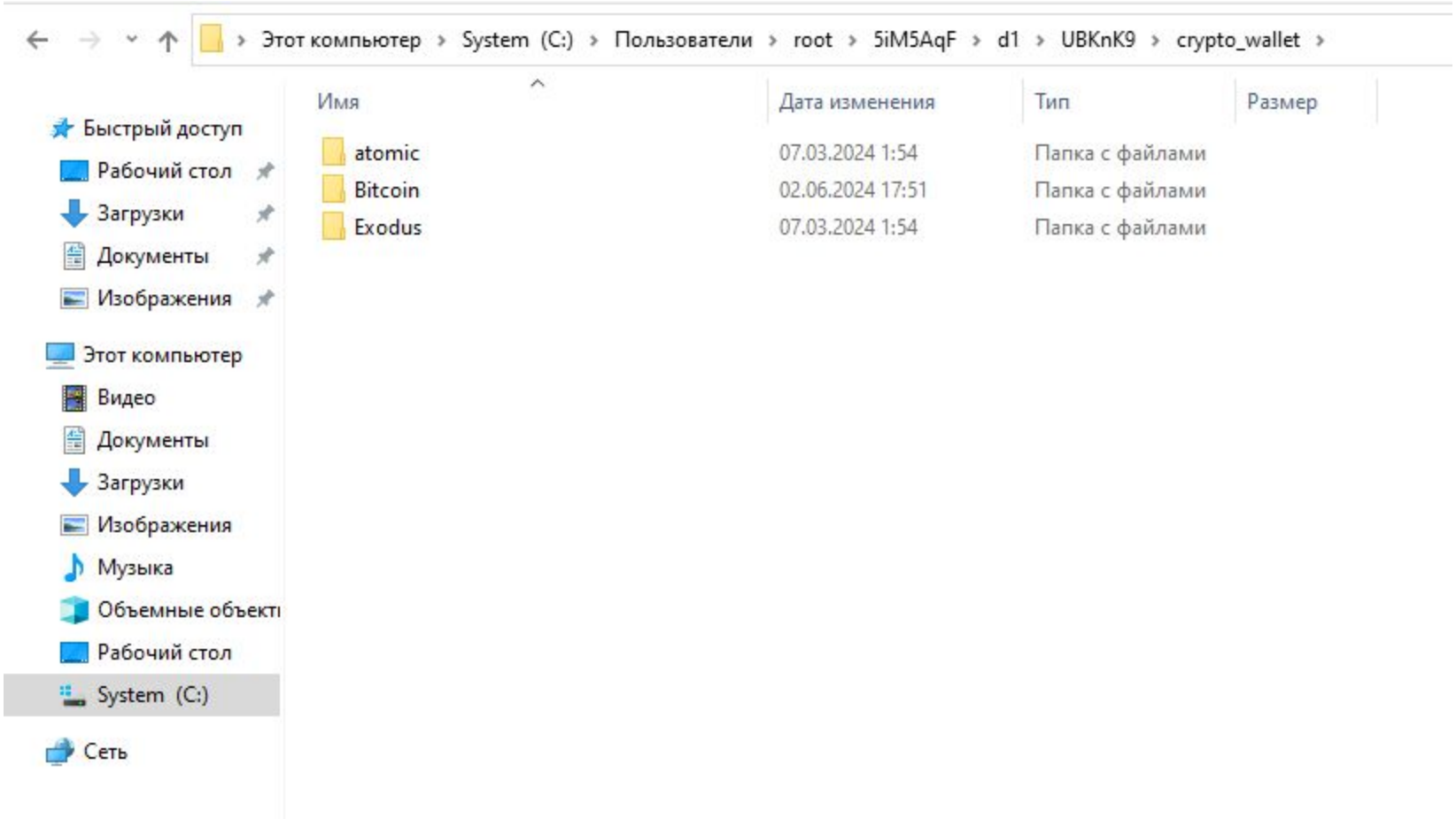

Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 ›
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
Имя
Дата изменения
Тип
Размер
Cookies 02.06.2024 17:51 Папка с файлами
crypto_wallet 02.06.2024 17:51 Папка с файлами
Desktop 02.06.2024 17:51 Папка с файлами
Discord 07.04.2024 19:44 Папка с файлами
General 02.06.2024 17:51 Папка с файлами
Pictures 02.06.2024 17:51 Папка с файлами
sbor_msg 02.06.2024 17:51 Папка с файлами
Steam 02.06.2024 17:51 Папка с файлами
web_extensions 02.06.2024 17:51 Папка с файлами
info.txt 02.06.2024 17:51 Текстовый докум... 2 КБ
Process.txt 02.06.2024 17:51 Текстовый докум... 1 КБ
screenshot.png 02.06.2024 17:51 Рисунок PNG 176 КБ

4. Сбор информации о системе: собор информации о системе, такую как
IP-адреса,
Характеристики оборудования
Имя пользователя
Запущенное программное обеспечение
Сетевые интерфейсы
Имя хоста
Город и регион
Буфер обмена
Время запуска
Путь запуска


Буфер обмена
Упорядочить
Создать
Открыть
Выделить
Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9
Поиск в: UBKnK9
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
Имя
Cookies
crypto_wallet
Desktop
Discord
General
Pictures
sbor_msg
Steam
web_extensions
info.txt
Process.txt
screenshot.png
info.txt – Блокнот
Файл Правка Формат Вид Справка
⚠ Информация: ⚠
OC/версия --> Windows/10.0
Имя пользователя --> HOME-PC
Сетевые интерфейсы --> fe80:0:0:0:41da:b5dd:e503:d13b%ethernet_32773
IP-адрес --> 87.238.234.194
Host Name --> AS30936 RENET COM Ltd.
Город --> Saratov
Регион --> Saratov Oblast
Местоположение --> RU
Буфер обмена --> <!-- https://mvnrepository.com/artifact/com.squareup.okio/okio -->
<dependency>
<groupId>com.squareup.okio</groupId>
<artifactId>okio</artifactId>
<version>3.5.0</version>
</dependency>
Процессор --> Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.30GHz
Ядро процессора --> 24
Время запуска --> 16:51
Время --> 2.06.2024
Оперативная память --> 16.0 GB
Окна --> Unknown – InfoPC.java
Стр 1, стлб 1
100%
UNIX (LF)
UTF-8

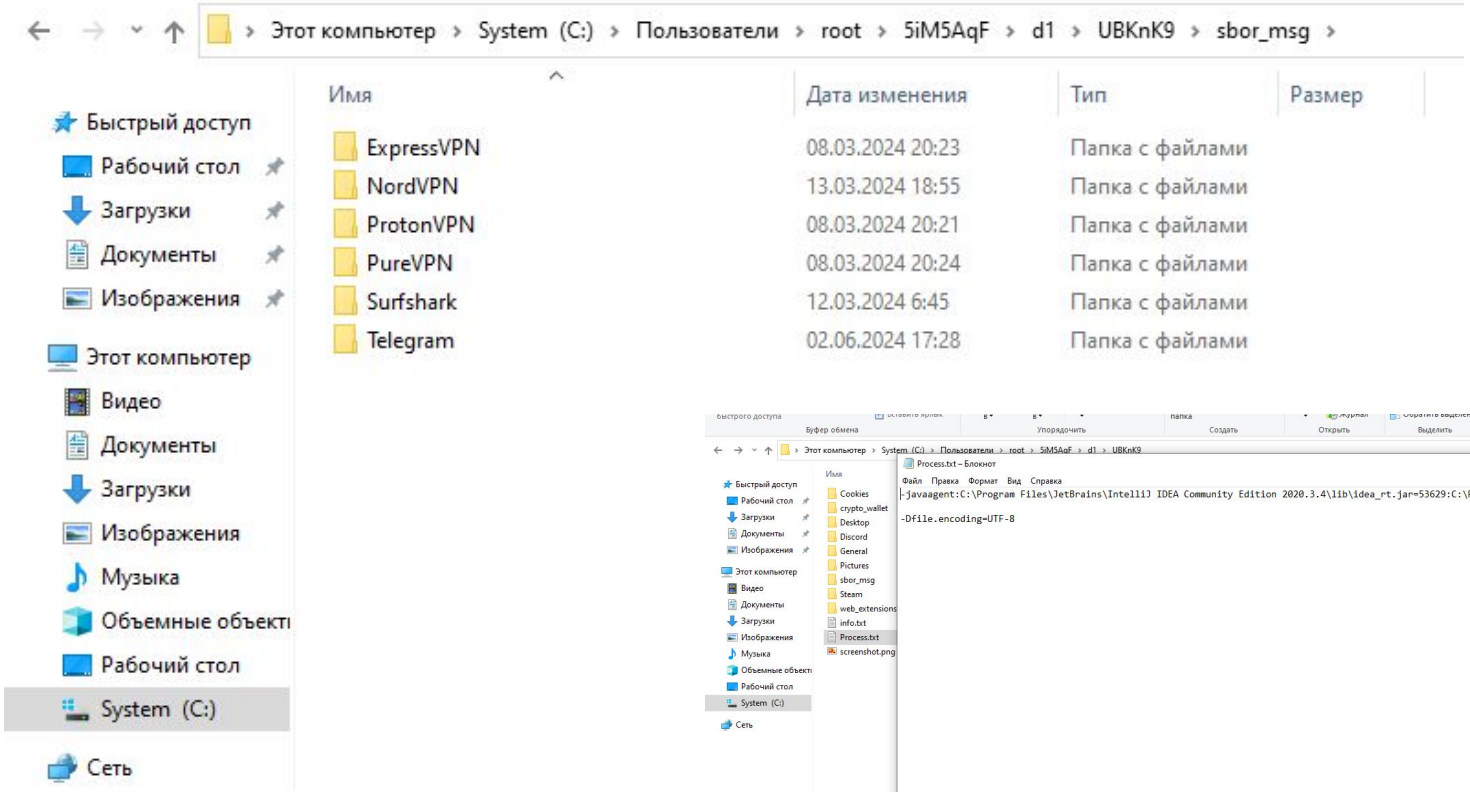
5. Сбор в реальном времени. С
веб камеры
скриншот экрана

6. Сбор десктопных криптокошельков:
bitcoin
exodus
jaxx
atomic


Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 › crypto_wallet ›
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
Имя
Дата изменения
Тип
Размер
atomic
07.03.2024 1:54
Папка с файлами
Bitcoin
02.06.2024 17:51
Папка с файлами
Exodus
07.03.2024 1:54
Папка с файлами

7. Сбор запущенных процессов
штатных для работы ОС
запущенных пользователем

8. Сбор VPN десктопных приложений:
Таких vpn как
NordVPN
Surfshark
ProtonVPN
ExpressVPN
PureVPN

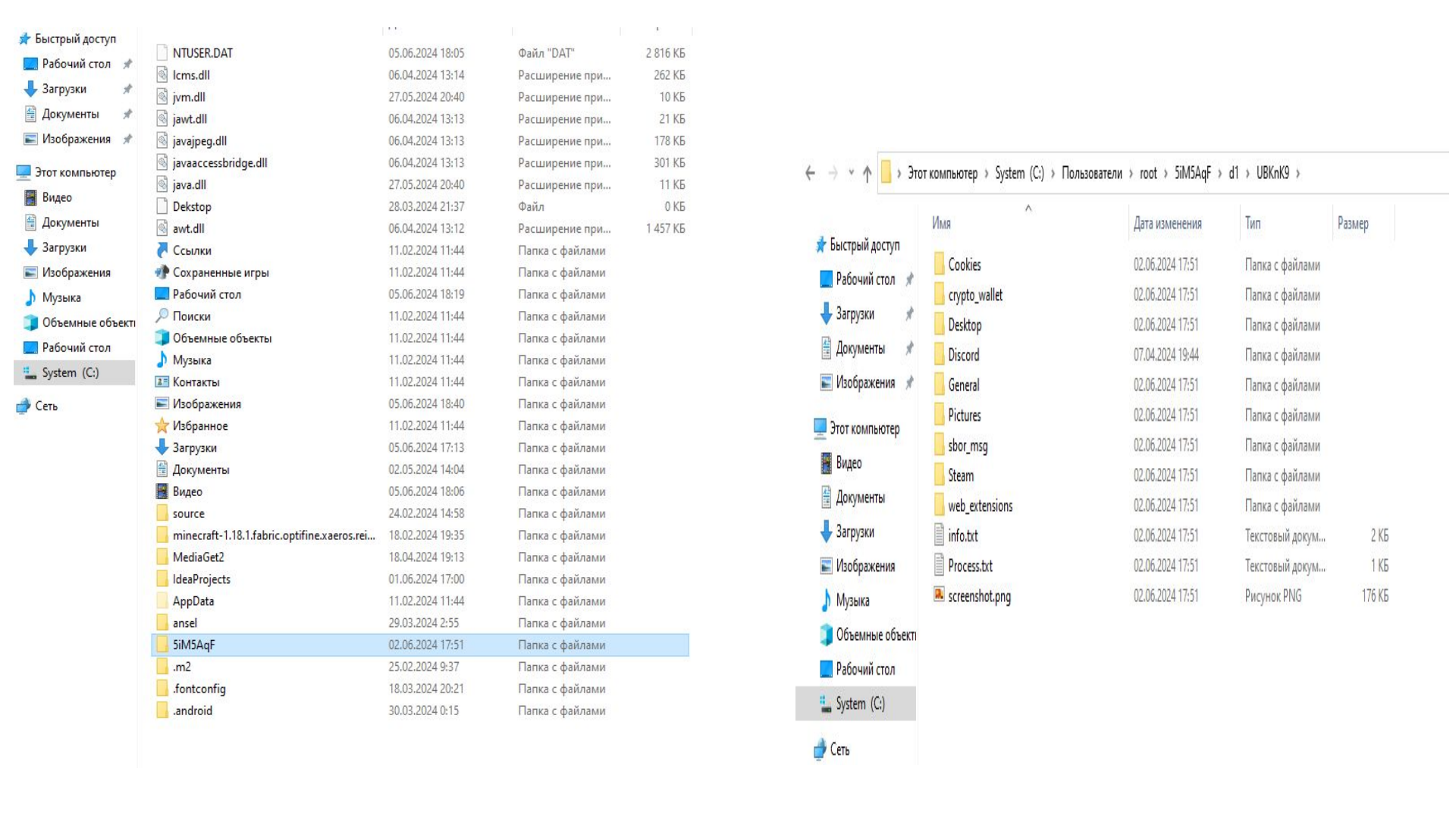

Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 › sbor_msg ›
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
Имя
Дата изменения
Тип
Размер
ExpressVPN 08.03.2024 20:23 Папка с файлами
NordVPN 13.03.2024 18:55 Папка с файлами
ProtonVPN 08.03.2024 20:21 Папка с файлами
PureVPN 08.03.2024 20:24 Папка с файлами
Surfshark 12.03.2024 6:45 Папка с файлами
Telegram 02.06.2024 17:28 Папка с файлами
Process.txt – Блокнот
Файл Правка Формат Вид Справка
-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2020.3.4\lib\idea_rt.jar=53629:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2020.3.4\bin
-Dfile.encoding=UTF-8
Стр 1, стлб 1
100%
UNIX (LF)
UTF-8

9. Сбор записей с инструментов для администрирования: FileZilla(FTP-клиент)

10. Проверка виртуалки/песочницы
Запуск только на десктопных версиях ОС

11. Запуск VNC для удаленного администрирования и работы с ПК пользователя в реальном времени

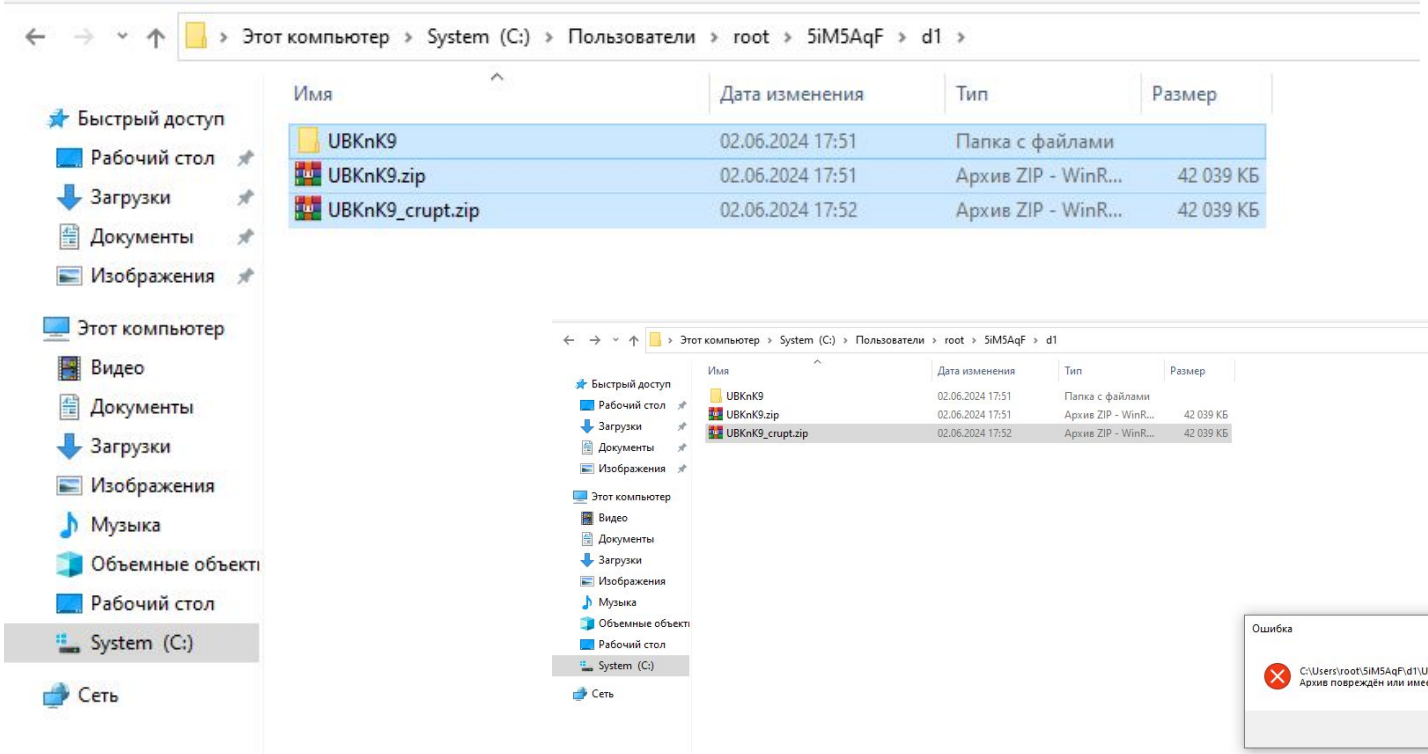
Лог сохраняется на жестком диске системы. Далее строит динамически количество папок и их имя куда будет сохранен лог. Так же можно добавить пути куда может быть сохранен лог, и после отправки удален. Например, это удобно при работы с сетями из пользователей, что бы в дальнейшем анализировать старые логи с новыми. Все это сделано динамически и можно легко настроить.


Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекти
Рабочий стол
System (C:)
Сеть
NTUSER.DAT 05.06.2024 18:05 Файл "DAT" 2 816 КБ
lcms.dll 06.04.2024 13:14 Расширение при... 262 КБ
jvm.dll 27.05.2024 20:40 Расширение при... 10 КБ
jawt.dll 06.04.2024 13:13 Расширение при... 21 КБ
javajpeg.dll 06.04.2024 13:13 Расширение при... 178 КБ
javaaccessbridge.dll 06.04.2024 13:13 Расширение при... 301 КБ
java.dll 27.05.2024 20:40 Расширение при... 11 КБ
Dekstop 28.03.2024 21:37 Файл 0 КБ
awt.dll 06.04.2024 13:12 Расширение при... 1 457 КБ
Ссылки 11.02.2024 11:44 Папка с файлами
Сохраненные игры 11.02.2024 11:44 Папка с файлами
Рабочий стол 05.06.2024 18:19 Папка с файлами
Поиски 11.02.2024 11:44 Папка с файлами
Объемные объекты 11.02.2024 11:44 Папка с файлами
Музыка 11.02.2024 11:44 Папка с файлами
Контакты 11.02.2024 11:44 Папка с файлами
Изображения 05.06.2024 18:40 Папка с файлами
Избранное 11.02.2024 11:44 Папка с файлами
Загрузки 05.06.2024 17:13 Папка с файлами
Документы 02.05.2024 14:04 Папка с файлами
Видео 05.06.2024 18:06 Папка с файлами
source 24.02.2024 14:58 Папка с файлами
minecraft-1.18.1.fabric.optifine.xaeros.rei... 18.02.2024 19:35 Папка с файлами
MediaGet2 18.04.2024 19:13 Папка с файлами
IdeaProjects 01.06.2024 17:00 Папка с файлами
AppData 11.02.2024 11:44 Папка с файлами
ansel 29.03.2024 2:55 Папка с файлами
5iM5AqF 02.06.2024 17:51 Папка с файлами
.m2 25.02.2024 9:37 Папка с файлами
.fontconfig 18.03.2024 20:21 Папка с файлами
.android 30.03.2024 0:15 Папка с файлами
Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 › UBKnK9 ›
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекти
Рабочий стол
System (C:)
Сеть
Имя
Дата изменения
Тип
Размер
Cookies 02.06.2024 17:51 Папка с файлами
crypto_wallet 02.06.2024 17:51 Папка с файлами
Desktop 02.06.2024 17:51 Папка с файлами
Discord 07.04.2024 19:44 Папка с файлами
General 02.06.2024 17:51 Папка с файлами
Pictures 02.06.2024 17:51 Папка с файлами
sbor_msg 02.06.2024 17:51 Папка с файлами
Steam 02.06.2024 17:51 Папка с файлами
web_extensions 02.06.2024 17:51 Папка с файлами
info.txt 02.06.2024 17:51 Текстовый докум... 2 КБ
Process.txt 02.06.2024 17:51 Текстовый докум... 1 КБ
screenshot.png 02.06.2024 17:51 Рисунок PNG 176 КБ

Реализована многопоточность, все функции программы начинают свою работу одновременно и асинхронно. Что уменьшает время работы программы.

Весь код на 95% уникален(только работа с браузерами была подсмотрена из другого проекта).

Нет админ панели, лог приходит просто в виде архива, расшифровываются по уникальному ключу и разархивируются. Алгоритм шифрования AES-256 нужен для того что бы нельзя было провести МИТМ атаку, и по не защищенному протоколу перехватить лог и получить все данные в открытом виде. Лог шифруется на ПК пользователя криптографическим ключом, и расшифровывается тем же ключом на сервере.


Этот компьютер › System (C:) › Пользователи › root › 5iM5AqF › d1 ›
Имя
Дата изменения
Тип
Размер
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
System (C:)
Сеть
UBKnK9
02.06.2024 17:51
Папка с файлами
UBKnK9.zip
02.06.2024 17:51
Архив ZIP - WinR...
42 039 КБ
UBKnK9_crupt.zip
02.06.2024 17:52
Архив ZIP - WinR...
42 039 КБ
Ошибка
C:\Users\root\5iM5AqF\d1\UBKnK9_crupt.zip
Архив повреждён или имеет неизвестный формат
OK

Динамический стаб(вызов модулей с каждым запуском происходит в рандомном порядке).

Сам лог перед отправкой архивируется и шифруется по алгоритму aes256, и передается на сервер(ftp оправка нужно указать лишь ip/port сервера). Как лог пришел на сервер, он разархивируется и расшифровывается.

Все пути до собираемых ресурсов, а также до информации о ip/port сервера, зашифроаванны по алгоритму aes256. Хранятся в настройках программы в зашифрованном виде, только когда программа запущена, она динамически при использовании какого то конкретного модуля расшифровывает нужную строку. Например, при сборе крипто кошельков, по очередно берутся зашифрованные пути, расшифровываютя и передаются в модуль, расшифрованные пути хранятся только в памяти. По такому же смыслу отправляется и лог(в зашифрованном виде).

Программа написана полностью на java. Зависимости есть, но они не подгружаются с сервера, а уже идут с коробки, из за этого вес билда довольно большой(8 мб) в jar. Исходный код программы обфусцируется с помощью штатного обфускатора и после этого java код пересоберается в нативный код с помощью graalvm.

Дело в том, что java запускается только если на пк есть jvm(java виртуальная машина), без нее программа к сожалению не запуститься. Так же минусом будет скорость программы(побыстрее конечно чем питон, но и помедленнее плюсов), из за того что код передается с начало в jvm, там он компилируется в машинный код и только потом исполняется.

Но с помощью graalvm мы сразу из java соберем нативный(машинный) код, в .exe а не .jar. что гораздо ускорит скорость отработки стиллера(менее 3с), и добавит возможность запуска без jvm, даже на чистых машинах. Так же вес нативно собранного билда - около 3 мб.

Так же реализована простенькая функция подписки - после определенной даты, программа перестает запускаться. Ее можно легко убрать или оставить по вашему желанию.

При работе используются следующие зависимости:
org.json | - для сбора информации о пк
jna для работы с winapi _
sarxos для захвата веб камеры(удаляется при желании)
org.apache.commons для копирования директорий
windpapi4j для вызова некоторых системных функций виндовс