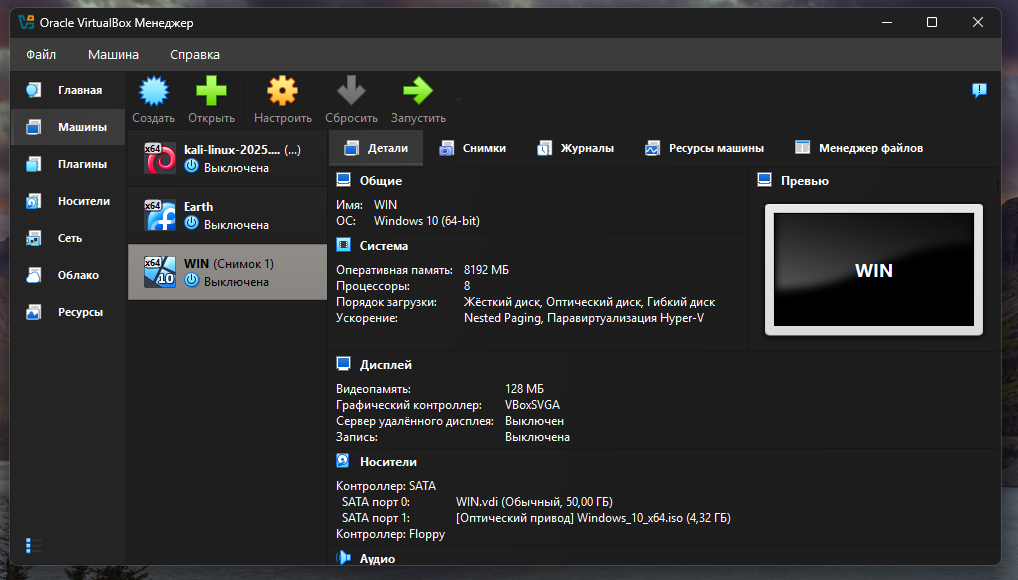
**АЛГОРИТМ ДЕЙСТВИЙ**

СОЗДАНИЕ ТЕСТОВОЙ СРЕДЫ ЭТАП 1: ПОДГОТОВКА

Создание виртуальной среды:

Устанавливаю VirtualBox с полностью отключенными общими папками и общим буфером обмена

Разворачиваю ВМ с Windows 10 x64 (снапшот "Clean State")



Устанавливаю инструменты анализа:

Process Monitor - для мониторинга файловой системы и реестра

Process Explorer - для анализа процессов и потоков

Wireshark - для перехвата сетевого трафика

Autoruns - для контроля автозагрузки

PEStudio - для статического анализа

Настройка изоляции:

Перед запуском образца отключаю сетевой адаптер ВМ

Создаю тестовые файлы в различных каталогах для отслеживания изменений:

C:\Test\document.txt

C:\Users\Public\image.jpg

C:\Temp\data.xlsx

ЭТАП 2: СТАТИЧЕСКИЙ АНАЛИЗ (БЕЗ ЗАПУСКА)

Анализ в PEStudio:

Изучаю импорты PE-файла:

Ищу CryptEncrypt, CreateFile, WriteFile (признаки шифровальщика)

Проверяю наличие RegSetValue, CreateService (установка в систему)

Анализирую сетевые функции (socket, connect, send)

Анализирую строки:

Поиск URL, IP-адресов, доменов

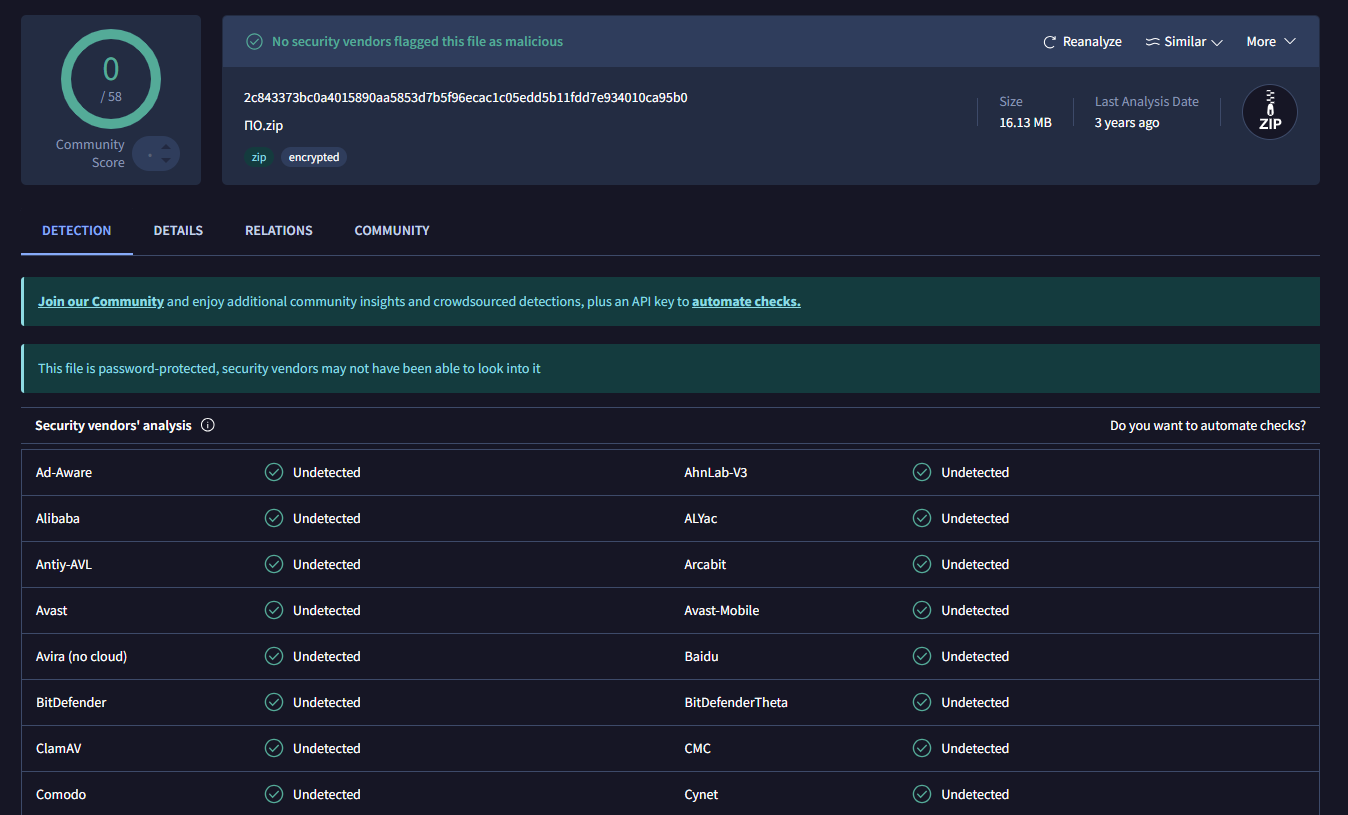
Поиск сообщений ("Your files are encrypted")

Поиск путей к системным файлам

Проверка на VirusTotal:

Загружаю файл (с осторожностью, чтобы не раскрыть образец)

Анализирую результаты антивирусных сканеров для предварительной классификации



ЭТАП 3: ДИНАМИЧЕСКИЙ АНАЛИЗ (С ЗАПУСКОМ)

Подготовка к запуску:

Запускаю Process Monitor с фильтрами:

Process Name = имя анализируемого файла

Operation = CreateFile, WriteFile, RegSetValue

Запускаю Process Explorer для мониторинга процессов

Запускаю Wireshark

Запуск образца:

Извлечение файла из "ПО.zip" с паролем "infected"

Открываю файл

Наблюдаю за поведением в реальном времени

События открытия файла:

После разархивации и открытия файла он пропадает (скрытие после запуска)

Мониторинг активности:

Файловая система: Отслеживаю создание/изменение файлов

Реестр: Контролирую изменения в автозагрузке и службах

Память: Анализирую активность других процессов

Сеть: Фиксирую попытки сетевых соединений

Последующий анализ:

Проверяю целостность тестовых файлов

Анализирую дампы памяти с помощью Volatility

Проверяю автозагрузку через Autoruns

Вывод:

Файл **crack.exe** является вредоносным Dropper'ом. Его основная функция — это скрытая доставка и запуск другой вредоносной нагрузки в системе. После запуска он самоудаляется, оставляя в системе создаваемый компонент, который обеспечивает постоянство и устанавливает сетевое соединение для дальнейших malicious-действий. Зашифрованные сообщения\Затронутый путь: Ransom:Win32/Filecoder.A, file: C:\Users\Vlad\Desktop\New Folder\crack.exe.