**#tinkoff fintech**

homework #6

**Forensics**& **Malware** Analysis

**22.04.2019**

# Tasks#:

#### **#01 LAB-01**

#### basic static malware analysis

.

#### **#02 LAB-02**

#### basic dynamic malware analysis

# ПОДГОТОВКА БЕЗОПАСНОЙ СРЕДЫ

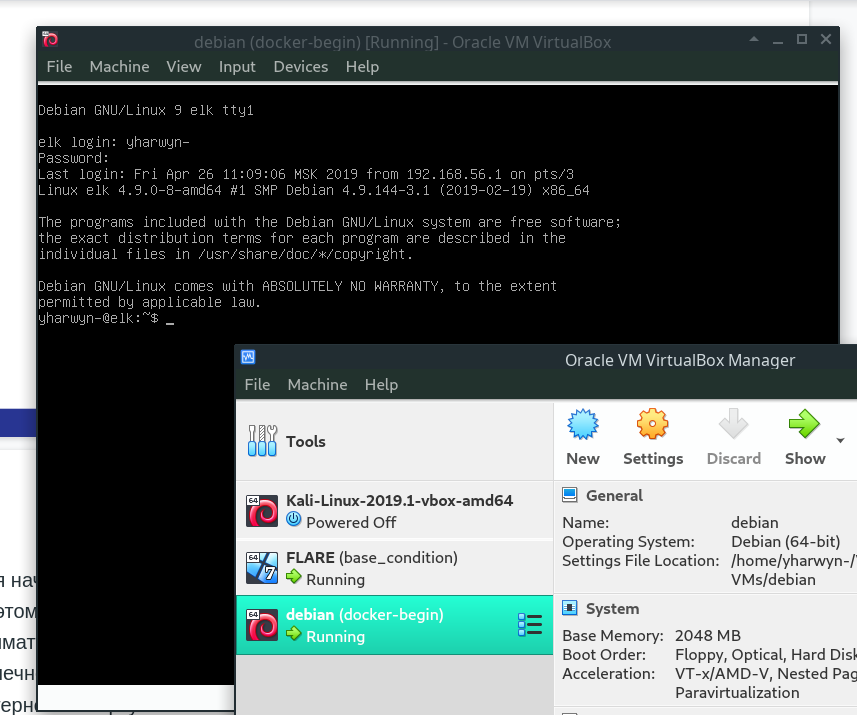
Для начала, надо понимать, что анализ малварей, да и вообще, всё что с этим связано дело **опасное**. Особенно - динамический анализ.

Поэтому, помимо того, что надо быть особенно аккуратным и внимательным, надо сделать пару шагов.

Конечно, можно обойтись просто snapshot’ами и отключить вообще весь интернет на виртуальной машине. Но это не тру. Хотя бы потому, что малварю может не понравится такая атмосфера (ну и мы не сможем узнать о конкретных целях, днс серверах \ ip с2с сервера).

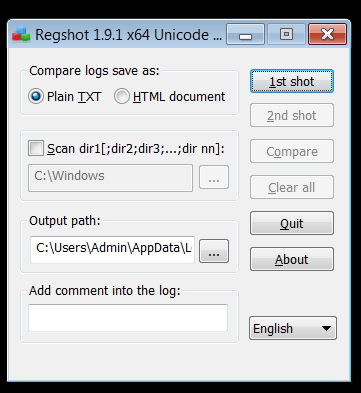
### Поэтому что я сделал:

1. **Установил минимальный дебиан**

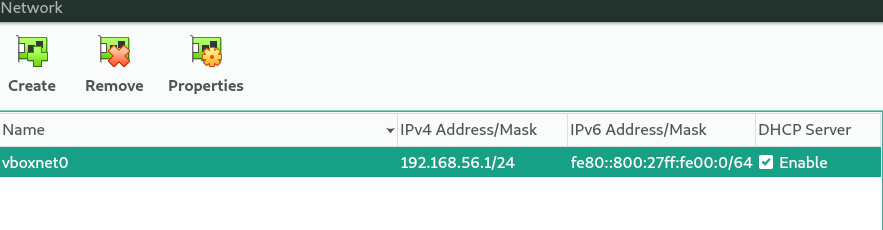
****

**2. Сделал снэпшоты для Windows 7**

**3. RegShot Backups**

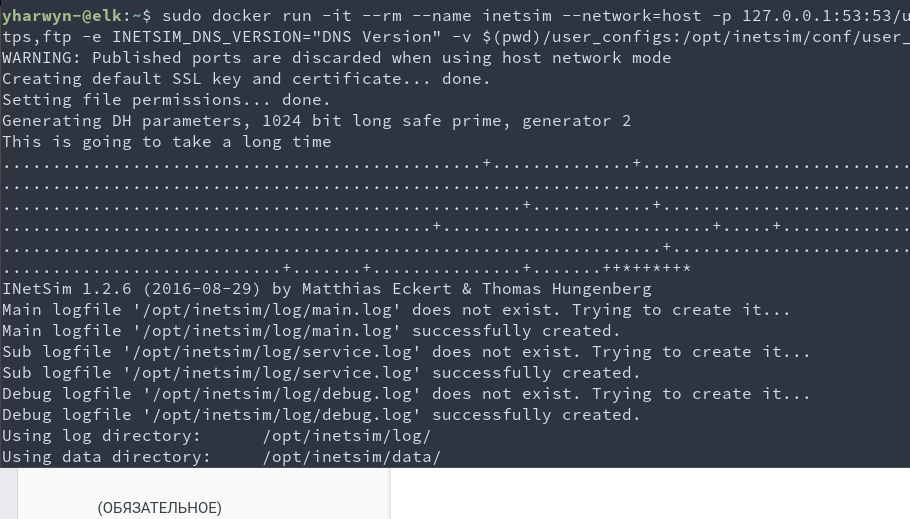
****

**4. Создаем в VirtualBox - Host only network** (и соответственно присоединяем наши машины в одну сеть).

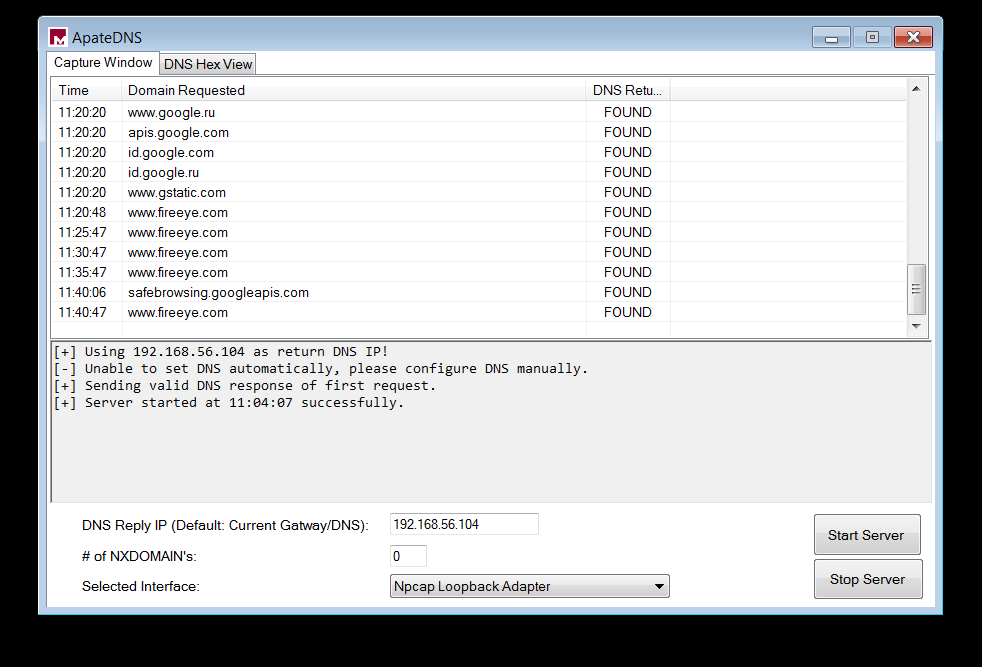
****

**5. На дебиане устанавливаем докер и скачиваем контейнер с INETSIM** (штука, позволяющая создать много фэйковых сервисов, а-ля http, ftp, dns для анализа запросов малваря)

****

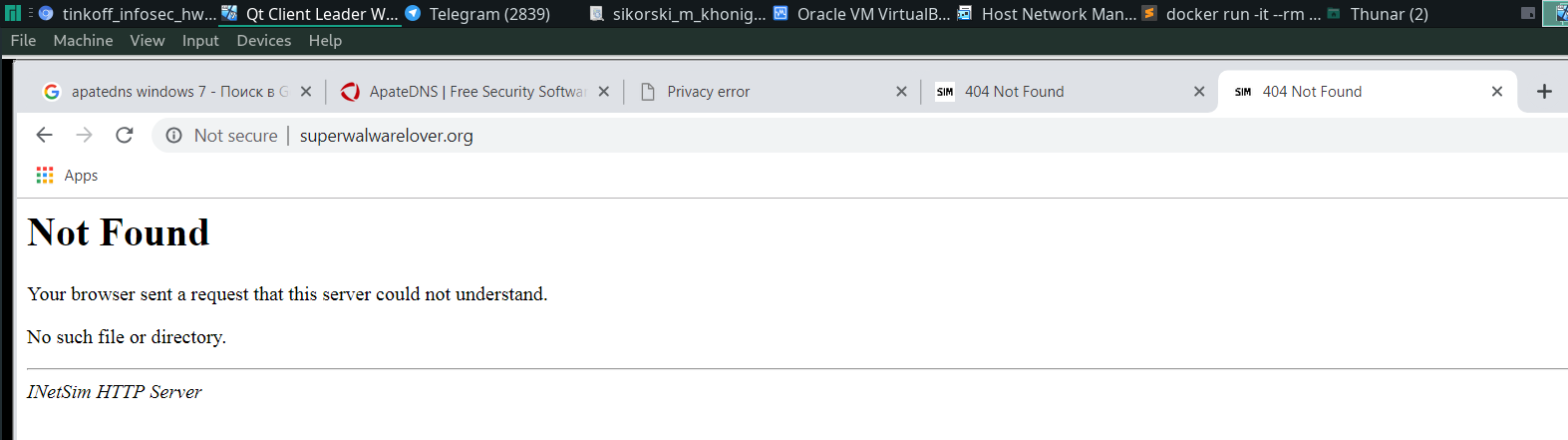
****

Запускаем контейнер в среде дебиан, убеждаемся что он работает и после этого на Windows 7 скачиваем софтик



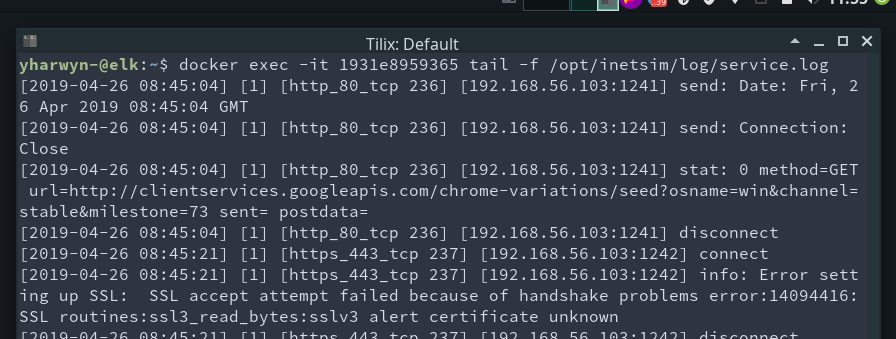
Собственно я его и настроил сразу (dns указал адрес дебиана с запущенным докер контейнером).

Осталось только сделать финальный тест, октрыть скажем через бразуер какой-нибуть сайт



**Ну и как бонус для себя, на родном manjaro открываю ssh сессию на дебиан, а оттуда кидаю тэйл на логи inetsim-контейнера, чтобы в режиме онлайн смотреть на всё это**

**Docker exec -it <id of container> tail -f /path/to/log**

****

Ну вот теперь, вроде как, среда обезопасена и можно уже позапускать малварики )))

#### ***(ну если совсем все пойдёт не так, то есть же snapshots).***

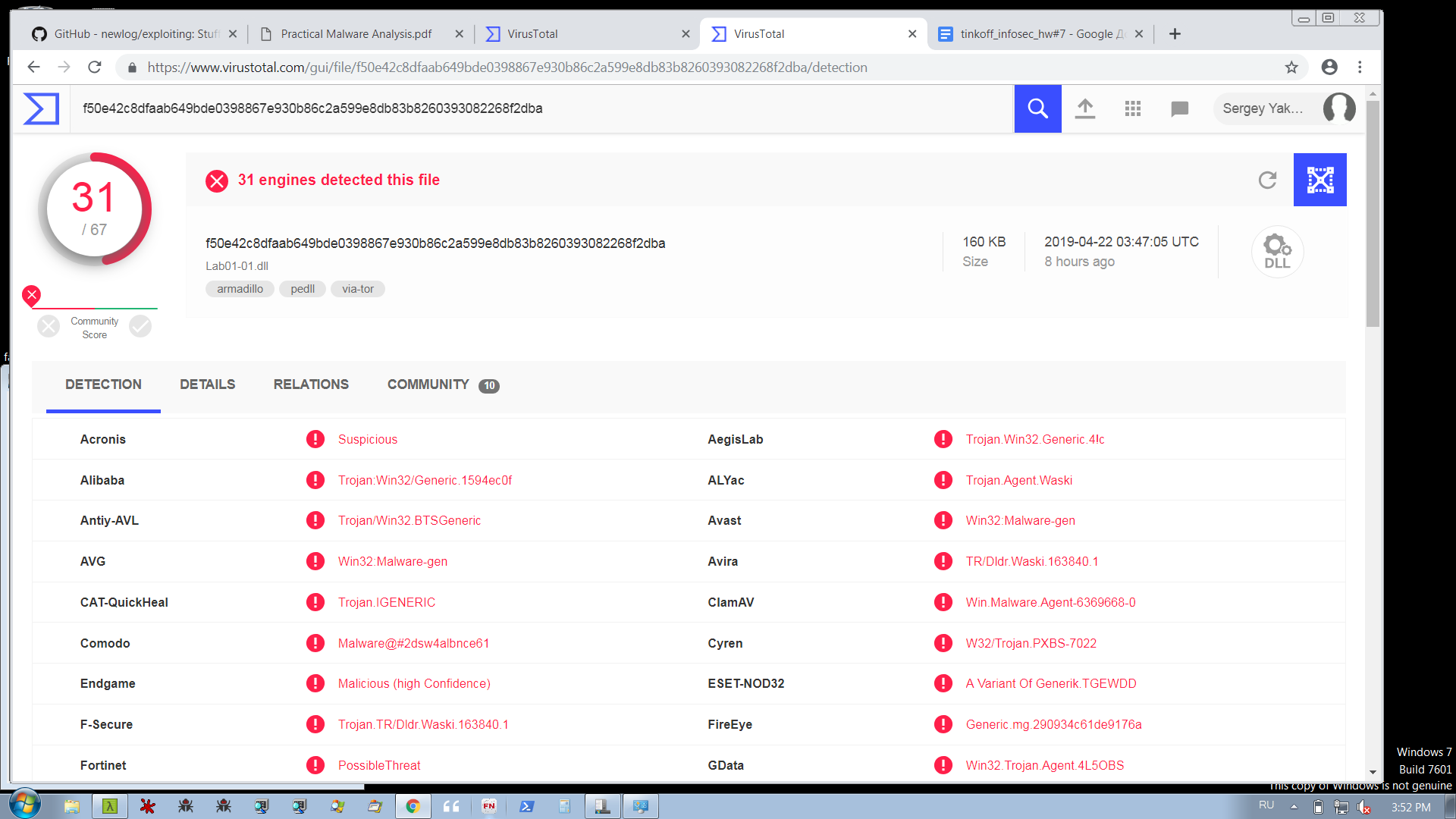
#### Task #1:LAB-1-1

This lab uses the files Lab01-01.exe and Lab01-01.dll. Use the tools and techniques described in the chapter to gain information about the files and answer the questions below.

### Questions

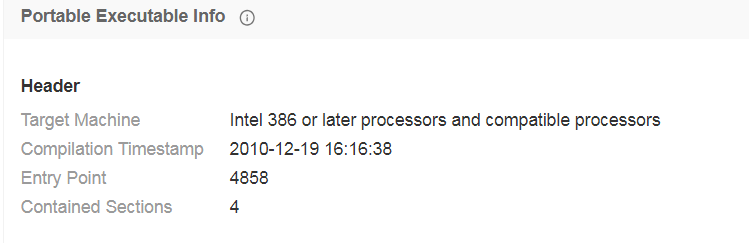
1. **Загрузить файлы на вирустотал. Посмотреть репорты. Нашелся ли он в сигнатурах?**
2. **Когда были скомпиленны эти файлы?**
3. **Есть ли какие-либо индикаторы того, что эти файлы были запакованны или обфусцированны?**
4. **Какой-либо импорт намекает на то что делает малварь? Если да то какой импорт.**
5. **Существуют ли какие-либо другие файлы или индикаторы на которые ты можешь обратить внимание на зараженных системах?**
6. **Какие network-based индикаторы могут быть использованы чтобы найти малварь на инфицированных машинах?**
7. **Какое предназначение этих файлов?**

### 1. Загрузить файлы на вирустотал. Посмотреть репорты. Нашелся ли он в сигнатурах



Загрузил оба файла. Посмотрел репорты. Страшно :)

### 2. Когда были скомпиленны эти файлы?



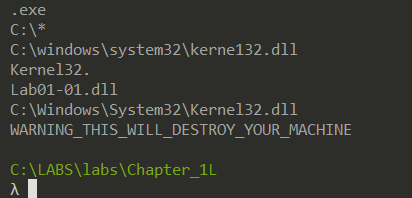
**2010-12-19 16:16:38**

(разница минимальна между двумя файлами, 30 секунд)

Можно предположить что эти файлы работают в тандеме :) А может и нет.

### 3. Есть ли какие-либо индикаторы того, что эти файлы были запакованны или обфусцированны?

По классике, сначала смотрим через strings. Если выводятся строки со смыслом, и вообще, количество их достаточно большое, то скорее всего файл не обфусцирован (либо в слабой форме). Вот к примеру вывод strings lab01-01.exe



Видим строчку с предупреждением. Пока не понимаю что этот malware замыслил, но звучит страшно :) (scareware :D)

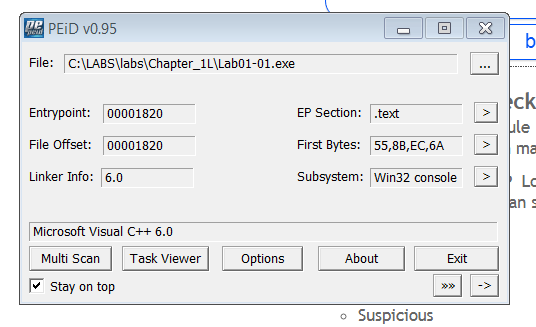
А вот strings на файле lab01-01.dll - выводит крайне мало информации. В основном это чтото вроде: D$@ / x0@

Эти срочки не несут смысла и могу быть проигнорированны (strings выводит все символы по ascii, без какой-либо фильтрации). А из полезных строчек для lab01-01.dll есть вот:



Из интересного, отмечаю вызов ws2\_32.dll (библиотека отвечает за работу с интернетом, открытие сокетов и т.д.). И как подтверждение - ниже выводится ай-пи адрес. Мог бы предположить что это малварь пытается соединится с интернетом но меня смущает диапазон - 127.\*.\*.\* - это диапазон зарезервированный под локальные адреса. Странный малварь)

Из важного, стоит упомянуть программу PEiD - в первую очередь с помощью которой можно попробовать узнать запакован ли файл.



(для \*.dll вывод аналогичен)

Как видим - определяется Microsoft Visual C++ 6.0, доверенный вендер )))) не какой-нибуть UPX ))

### 4. Какой-либо импорт намекает на то что делает малварь? Если да то какой импорт.

Что интересного из импорта нашел для себя из LAB01-01.exe:

**CreateFileA FindNextFileA FindFirstFileA CopyFileA** - вот эта цепочка с созданием, поиском и копированием файлов - очень подозрительно)) похоже на какого-то червя)))

**Lab01-01.dll WARNING\_THIS\_WILL\_DESTROY\_YOUR\_MACHINE-** вот эти строчки из стринга говорят нам, что во-первых лаб01-01.длл и лаб01-01.ехе - работают в паре) поэтому надо проанализировать их оба одновременно. Ну а предупрждение от малваря пока для меня не понятно. Либо user’a пугает, либо что-то иное.

Анализ LAB01-01.dll:

**CreateProcessA CreateMutexA OpenMutexA KERNEL32.dll WS2\_32.dll** - вот эта цепочка значит, что создается какой-то процесс, + задействуется сетевая либа WS2\_32.dll.

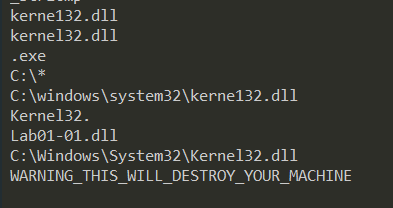
**exec sleep hello 127.26.152.13** - тут цепочка следующая (предположительно) exec - что-то запускает, затем идет sleep (ожидание чего-либо) строка hello - возможно посылается какой-то запрос с приветствием? И наконец ай-пи адрес (я выше уже писал свои мысли) для соединения по сети. С какими целями не знаю.

### 5. Существуют ли какие-либо другие файлы или индикаторы на которые ты можешь обратить внимание на зараженных системах?

### 6. Какие network-based индикаторы могут быть использованы чтобы найти малварь на инфицированных машинах?

### 7. Какое предназначение этих файлов?

Собственно про это я уже расписал выше. Я пришел к выводу что lab01-01.exe & lab01-01.dll - это malware (по сигнатурам вирустотал), с сетевой активностью (длл содержит импорты, а также строки а-ля IP), с функционалом поиска и копирования файлов (импорты Find&CreateFile). Буду честен, сразу не заметил вот этот момент:



Я не заметил сразу отличия в написании библиотеки kernel32.dll. Коварный малварь пишет символ “l” как “1”, что не очень очевидно на маленьком экране и с этим шрифтом (надо наверно поменять его в будущем). В общем, смысл такой: малварь пытается выдать свою библиотеку за родную.

Думаю что по факту, малварь ждем каких-то команд от управляющего хоста (**127.26.152.13).**

#### Task #1:LAB-1-2

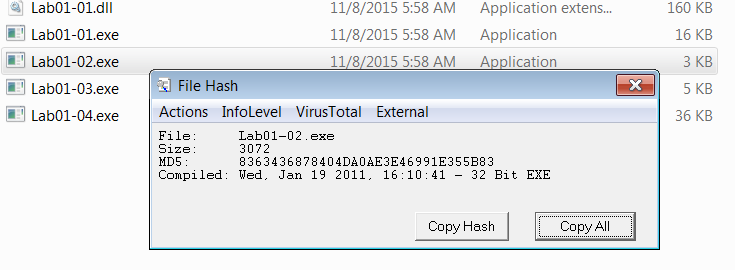
Analyze the file Lab01-02.exe

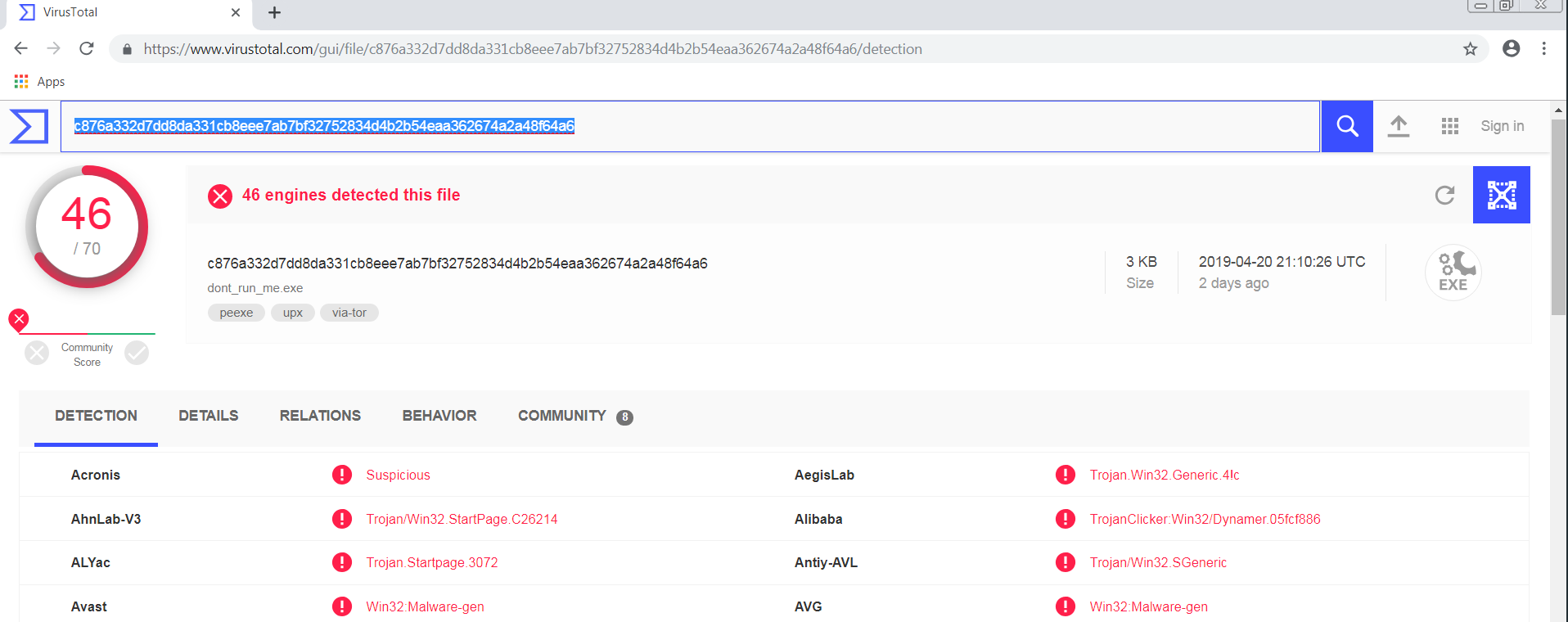
### Questions

1. **Загрузить файл на вирустотал. Чекнуть результат.**
2. **Обфусцированы \ упакованы - проверить статус. Если запакованы - распаковать.**
3. **Какой-либо импорт намекает на то что делает малварь? Если да то какой импорт.**
4. **Существуют ли какие-либо другие файлы или индикаторы на которые ты можешь обратить внимание на зараженных системах?**

### Загрузить файл на вирустотал. Чекнуть результат.

В этот раз сделаем хэш нашего малваря и отправим его на вирустотал. Загрузили, смотрим. Сигнатуры явно говорят об опасности))



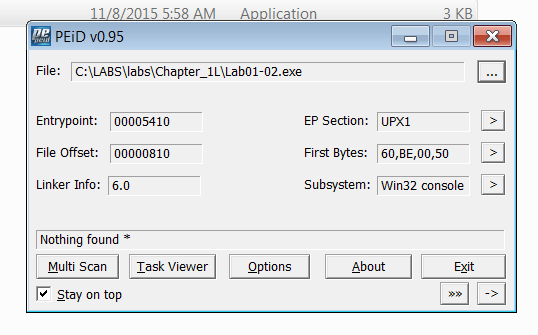


### 

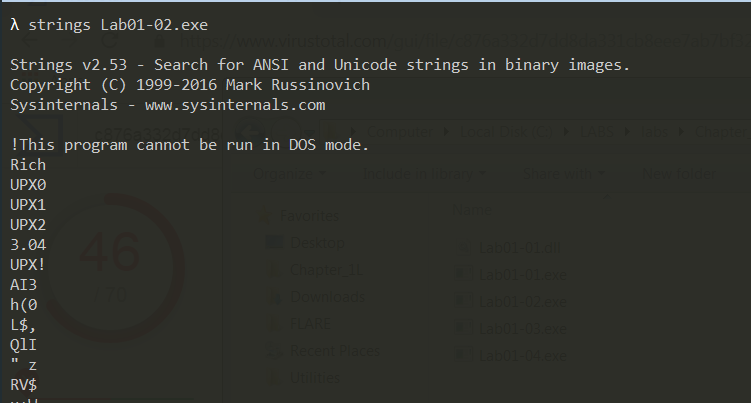
### 

### Обфусцированы \ упакованы - проверить статус. Если запакованы - распаковать.

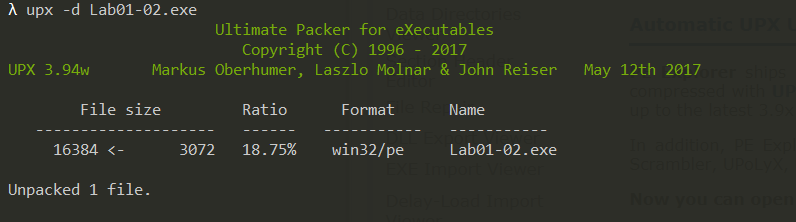
По классике, PEiD:



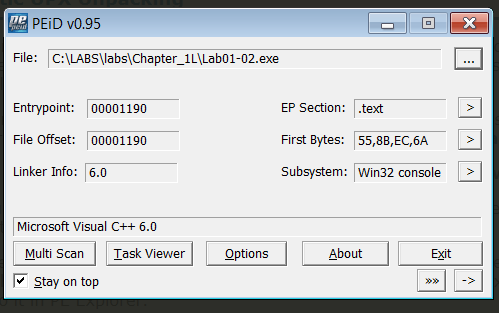
Nothing found :( Сейчас ещё чекнем через стрингс и сделаем выводы.



Зато много строчек с упаковщиком UPX. Делаем вывод что файл запакован через upx. Распакуем с ключем -d <.exe>



И…



Вот теперь распаковали и снова будем смотреть.

Много интересных импортов. В следующем вопросе опишу, что увидел.

### Какой-либо импорт намекает на то что делает малварь? Если да то какой импорт. Существуют ли какие-либо другие файлы или индикаторы на которые ты можешь обратить внимание на зараженных системах?

Посмотрим что там в strings:



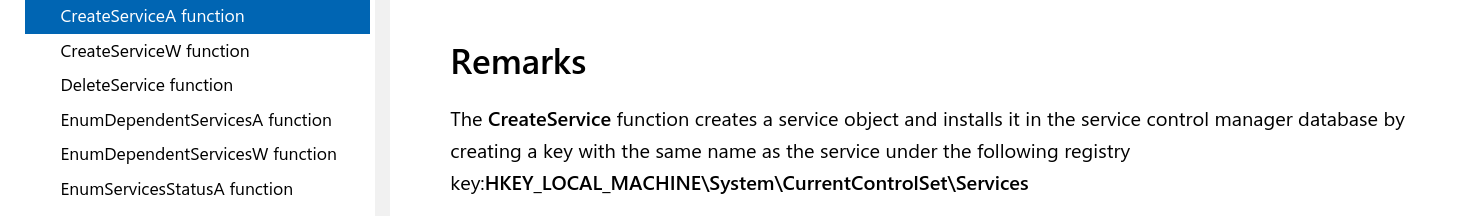
* **KERNEL32.DLL**
* **ADVAPI32.dll**
* MSVCRT.dll
* **WININET.dll**
* SystemTimeToFileTime
* GetModuleFileNameA
* CreateWaitableTimerA
* ExitProcess
* CreateMutexA
* CreateThread
* **CreateServiceA**
* **StartServiceCtrlDispatcherA**
* OpenSCManagerA
* **InternetOpenUrlA**
* **InternetOpenA**
* **Malservice**
* HGL345
* **http://www.malwareanalysisbook.com**
* Internet Explorer 8.0

Выделил полужирным, то что меня заинетерсовало)

Ну **kernel32** это стандарт, а вот **advapi32.dll** - библиотека позволяющая юзать такие функции как **CreateService**. Её рассмотрим отдельно))

Библиотека **wininet.dll** - отвечает за сетевую активность (малварь захочет в инет выйти).

Касательно функции **CreateService,** сначала посмотрел инфу на официальном сайте:



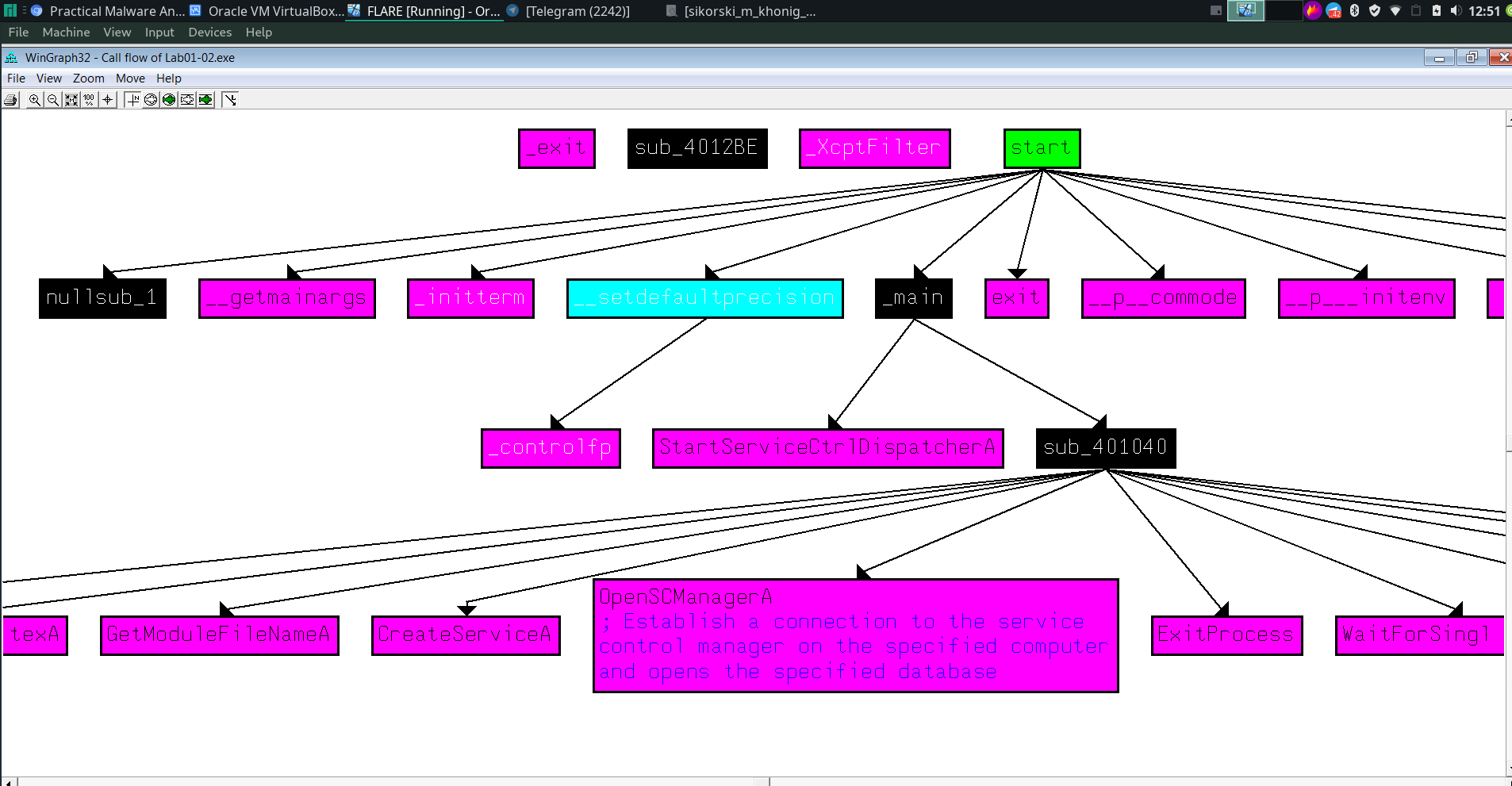
В общем, функция создает службу которая будет стартовать при загрузке компьютера. Добавляет ключи в реестр. Малвари обычно юзают для того, чтобы закрепиться в системе.

В частности, в нашем случае **CreateServiceA** создает объект службы с именем MalService (хорошее название).

**InternetOpenUrl** - функция, .использующая библиотеку wininet.dll для создания канала связи по url (разные протоколы http, https, ftp..)

Что можно сказать в общем про малваря исходя из импортов?

Малварь подгружает сетевую библиотеку, создает службу для закрепления в системе (хотя могут быть еще варианты), соединяется по интернету на адрес [www.malwareanalysisbook.com](http://www.malwareanalysisbook.com). С какими целями - сложно сказать, возможно ждет дальнейших команд от с2 сервера).



Граф от иды)

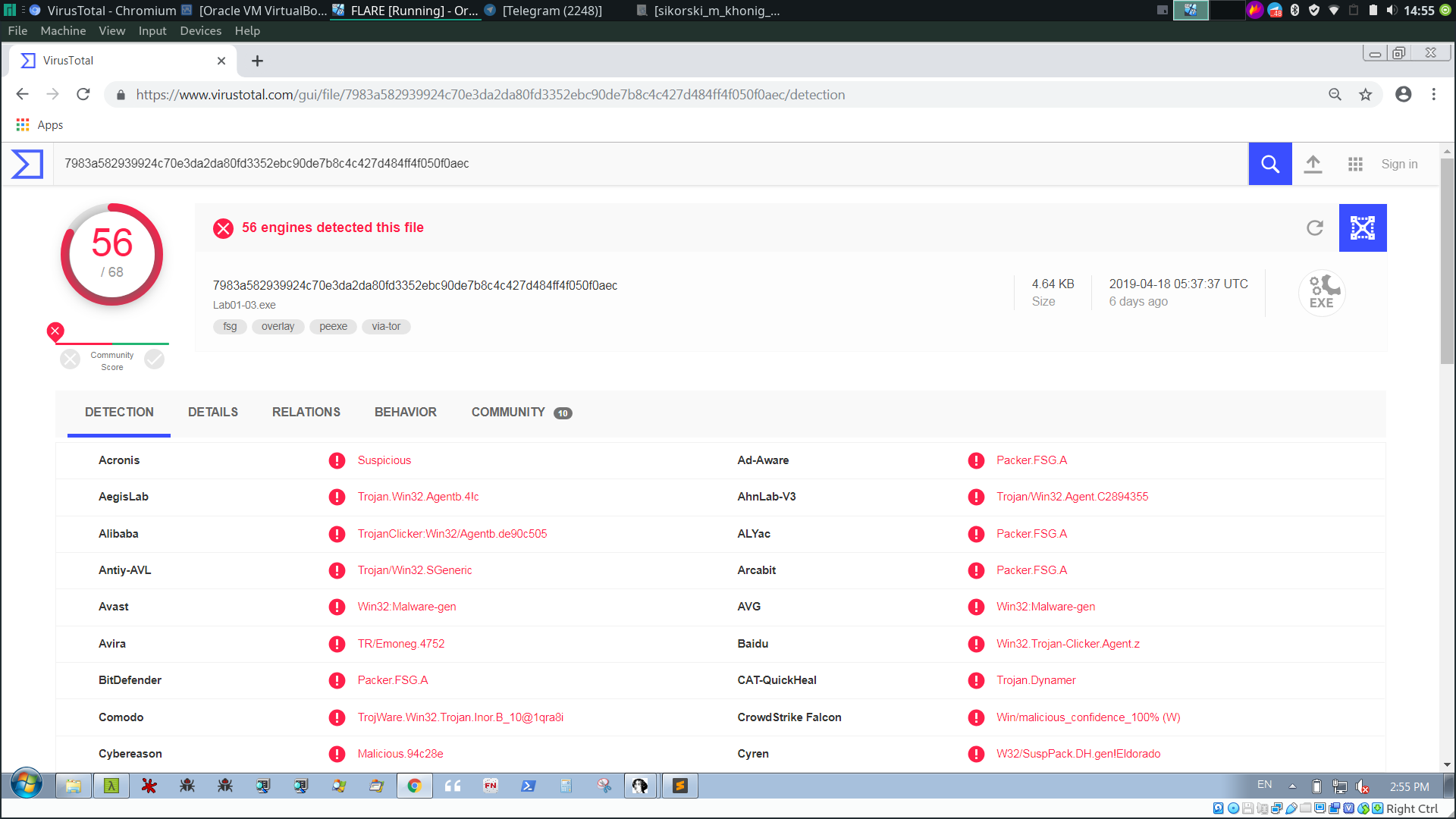
#### Task #1: LAB-1-3

Analyze the file Lab01-03.exe

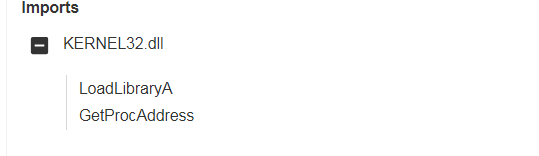
### Questions

1. **Загрузить файл на вирустотал. Чекнуть результат.**
2. **Обфусцированы \ упакованы - проверить статус. Если запакованы - распаковать.**
3. **Какой-либо импорт намекает на то что делает малварь? Если да то какой импорт.**
4. **Существуют ли какие-либо другие файлы или индикаторы на которые ты можешь обратить внимание на зараженных системах?**

### 1. вирустотал.ком

****

Анализ файла на вирустотал подтверждает, что это малварь. Что куда более интересно, это вкладка импортс.

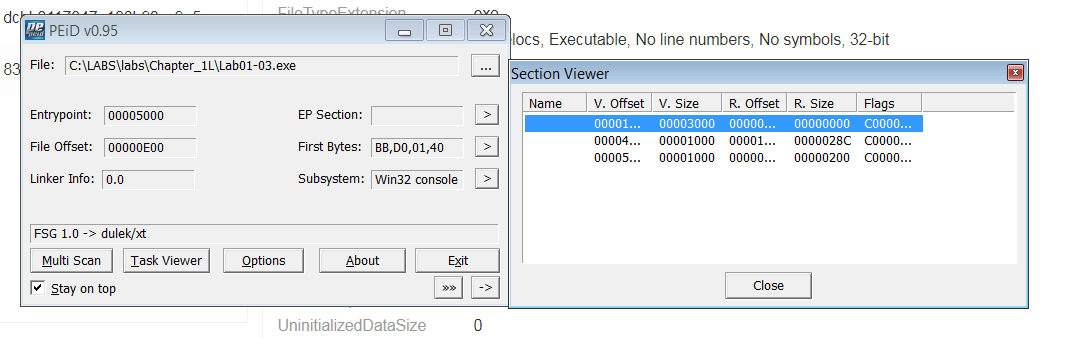
****

Собственно, видно, что количество импортов очень мало. Начинаем думать про обфускацию \ пакировку.

Надо понимать, что на самом деле dll могут быть импортированы не только статично, но и динамично. И вот тут как раз (для динамического импорта) нам нужны LoadLibrary и GetProcAddress (чтобы найти адрес нужной функции).

### 2. Обфускация \ пакировка

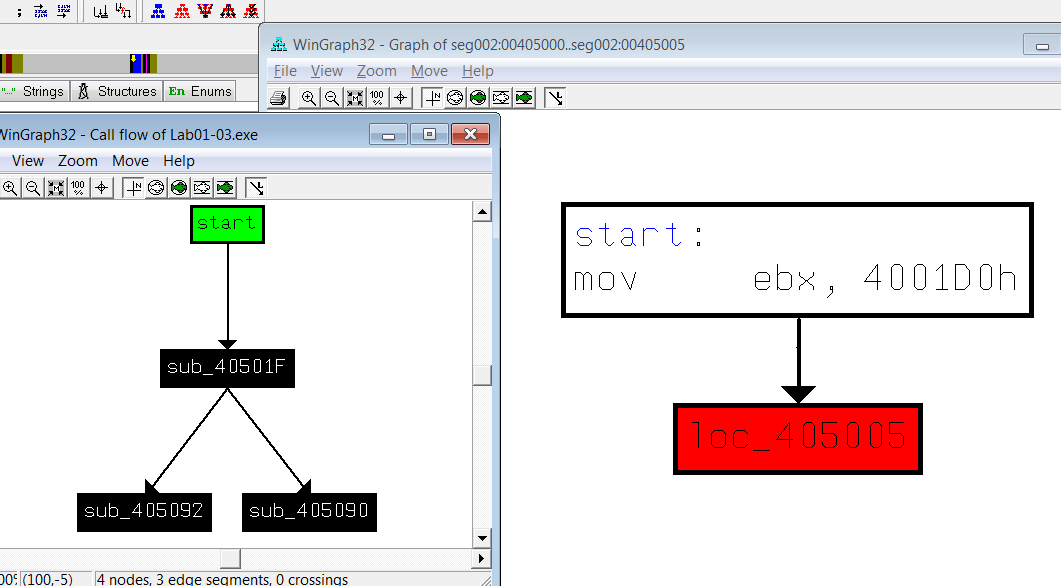
Посмотрим что нам покажет PEiD



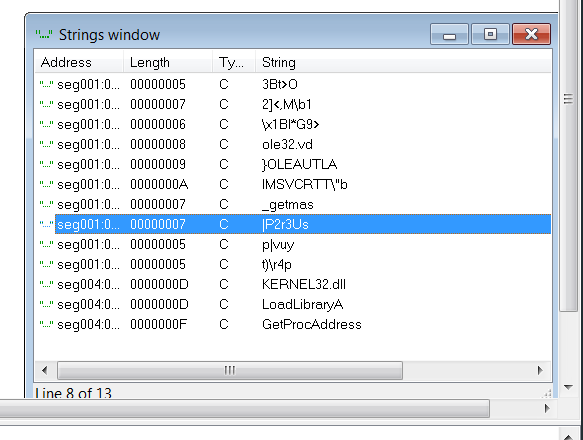
EP section -> NULL :) (безымянные секции)

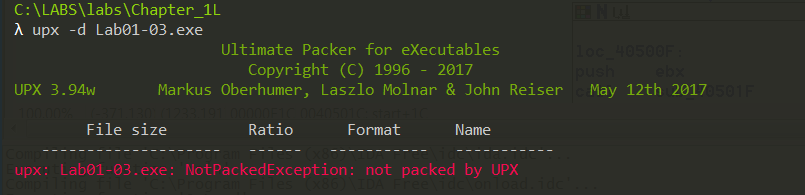
FSG 1.0 > dulek/xt - package. - в отличии от UPX информацию о распаковке сходу не нашёл.

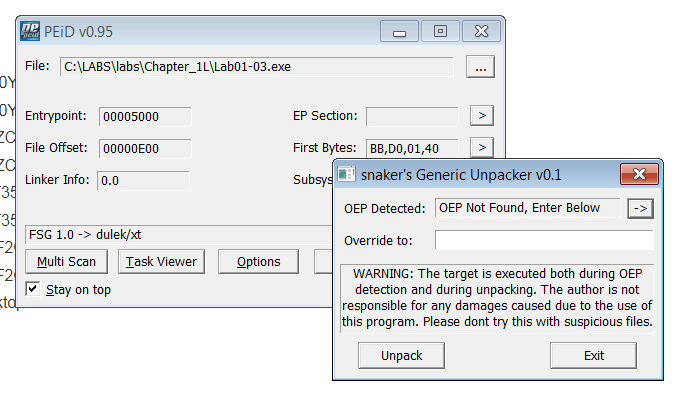
Делаем вывод: файл обфусцирован и запакован.

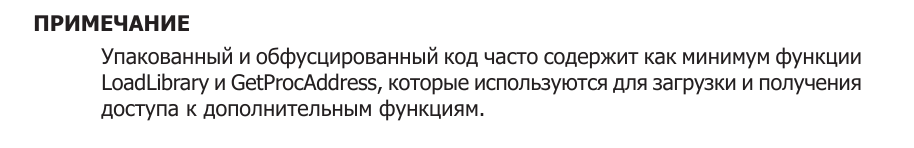


Печальный малоинформативный граф от Иды :(



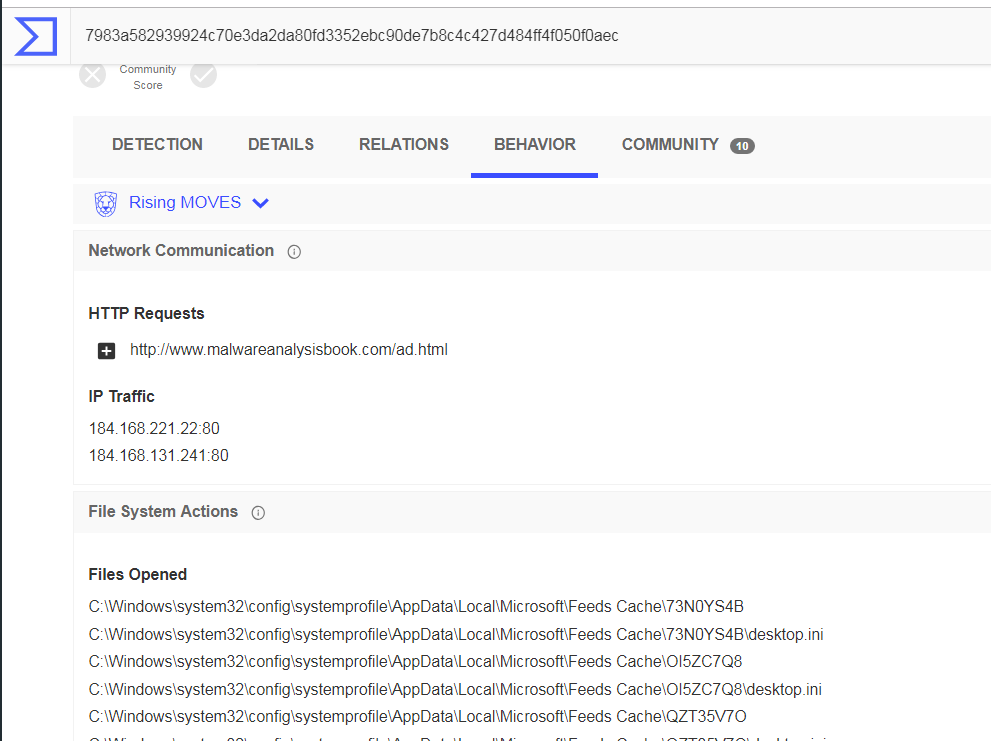






Вместо тысячи слов, эти скрины))

Короче, файл обфусцирован, не распаковав его что-то ковырять на статике не вариант (во всяком случае с моим текущим уровнем). Зато есть соблазн нажать **на волшебную вкладку “Behaviour” в вирустотал**.



Я понимаю, что в рамках текущей лабы не просят делать динамический анализ кода (а вирустотал как раз выдает вот эти данные на динамическом анализе). Поэтому не буду переписывать отчет, скажу просто что для таких малварей надо либо знать анатомию упаковщика (и юзать олли дбг) либо использовать динамический анализ.

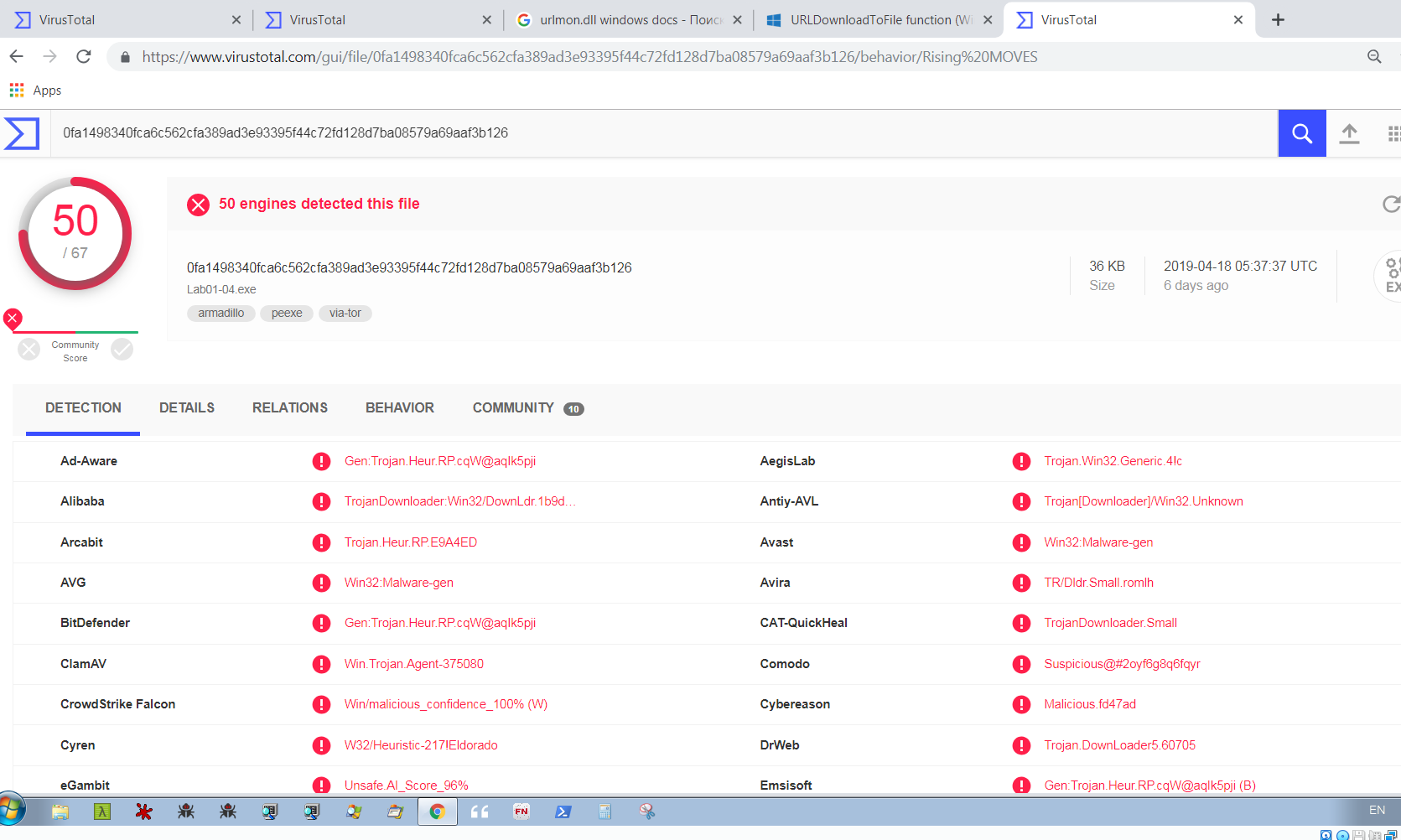
#### Task #1: LAB-1-4

Analyze the file Lab01-04.exe

### Questions

1. **Загрузить файл на вирустотал. Чекнуть результат.**
2. **Обфусцированы \ упакованы - проверить статус. Если запакованы - распаковать.**
3. **Дата компилляции**
4. **Какой-либо импорт намекает на то что делает малварь? Если да то какой импорт.**
5. **Существуют ли какие-либо другие файлы или индикаторы на которые ты можешь обратить внимание на зараженных системах?**

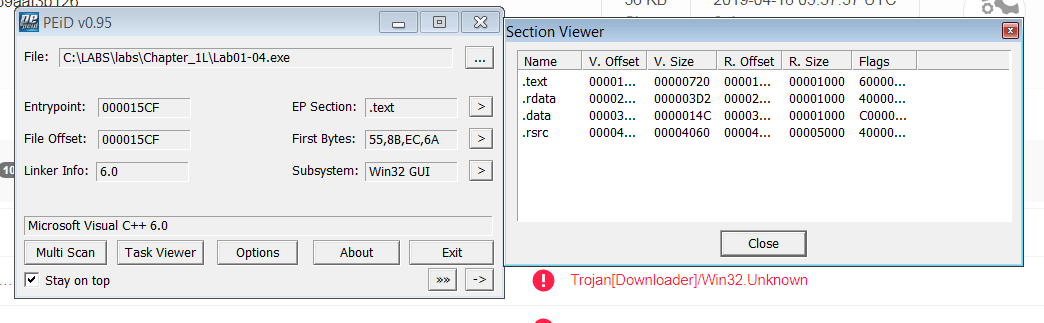
### Вирус тотал



Как всегда. Малварь палится.

### 2. Статус

PEiD говорит что файл не упакован. Наличие удобочитаемых стрингов говорит что нету обфускации.



### 3. Дата компиляции



Прикольно, прямо из будущего :) Теперь не буду доверять virustotal :D (если серьезно, именно эту информацию можно исказить разработчику малваря, если захотеть)

### 4. Индикаторы

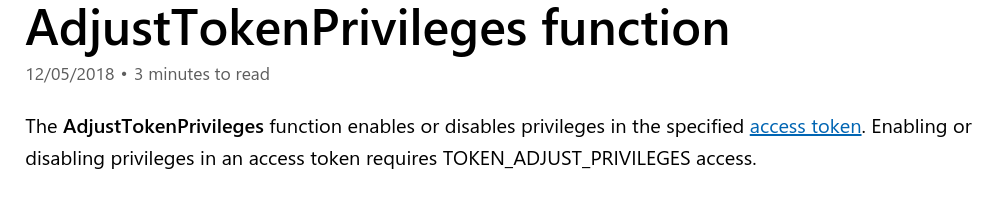
* OpenProcess
* GetCurrentProcess
* CreateRemoteThread
* GetProcAddress
* LoadLibraryA
* WinExec
* WriteFile
* CreateFileA
* FindResourceA
* GetModuleHandleA
* GetWindowsDirectoryA
* MoveFileA
* GetTempPathA
* KERNEL32.dll
* AdjustTokenPrivileges
* LookupPrivilegeValueA
* OpenProcessToken
* ADVAPI32.dll
* winlogon.exe
* SeDebugPrivilege
* sfc\_os.dll
* \system32\wupdmgr.exe
* psapi.dll
* \winup.exe
* GetWindowsDirectoryA
* WinExec
* GetTempPathA
* KERNEL32.dll
* URLDownloadToFileA
* \winup.exe
* \system32\wupdmgrd.exe
* <http://www.practicalmalwareanalysis.com/updater.exe>

Я оставил самые интересные для меня strings.

Начнем, например **CreateFileA** создает файл. Потом **MoveFileA** перемещает его. А **GetWindowsDirectory** находит путь до директории с Windows (можем предложить что малварь будет туда что-то закидывать). Тут как раз строчка из стрингов **\system32\wupdmgr.exe** намекает что возможно будет изменен или заменен файл по этому адресу.

Библиотека **sfc\_os**.dll нужна для функций описанных ниже (связанных с привилегиями).

Инфа по функции с микрософта.

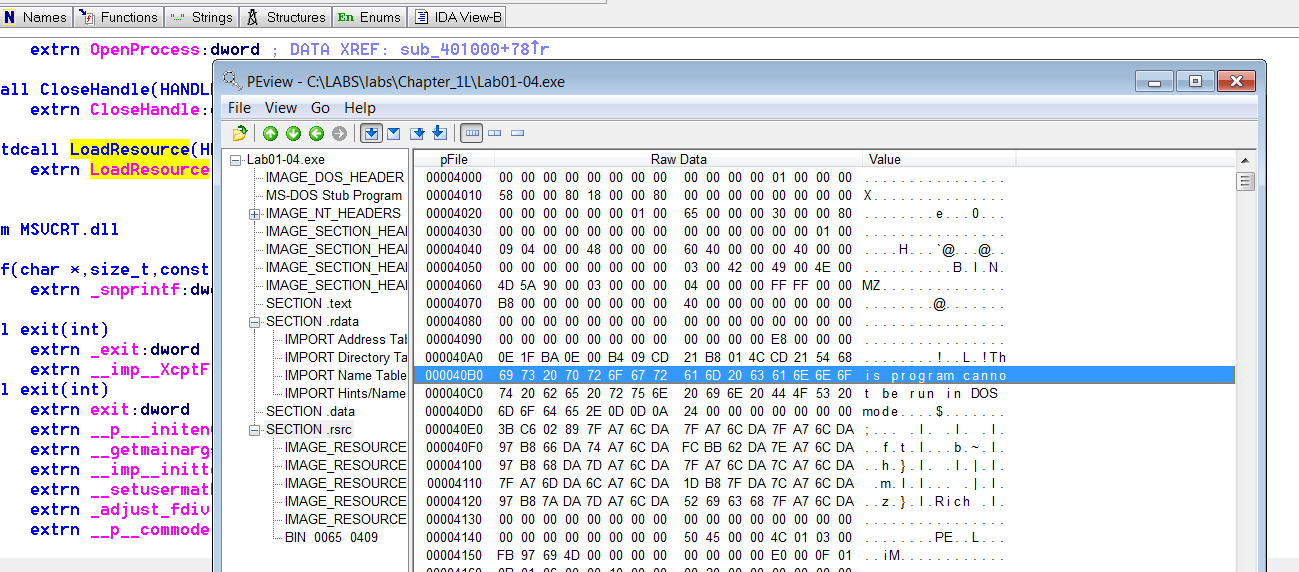


А также:

**SeDebugPrivilege -** когда гуглил информацию об этой функции находил что-то вроде “Take great care when granting SeDebugPrivilege to users or groups.” И прочие предупреждения. Достаточно опасная штука.

Могу предположить, что малварь повышает себе права для каких-то действий. Без определенных прав невозможно совершить подмену этого файла. Такие файлы как wupdmgr.exe обычно защищены системой. Поэтому необходимо сначала снять защиту.

Один важный момент в этом малваре это анализ его внутренностей через peview:



Что интересно? То что внутри lab01-04.exe есть еще один PE файл. Это можно проследить разными способами. Во-первых, самый наглядный - это просто просмотр по выводу из strings: \

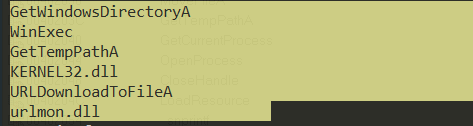
> !This program cannot be run in DOS mode. (встречается дважды)

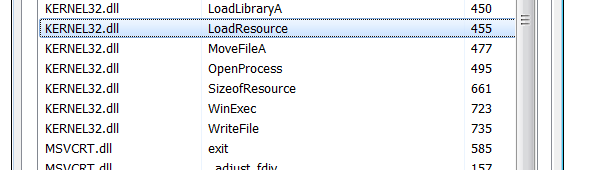
> LoadResource



То есть на выходе извлекается файл, с предположительным названием WinUp.exe. После чего, предположительно, с помощью вызова системной функции GetWindowsDirectoryA малварь копирует себя в папку Windows.

###### Kill chain от внутреннего PE file’

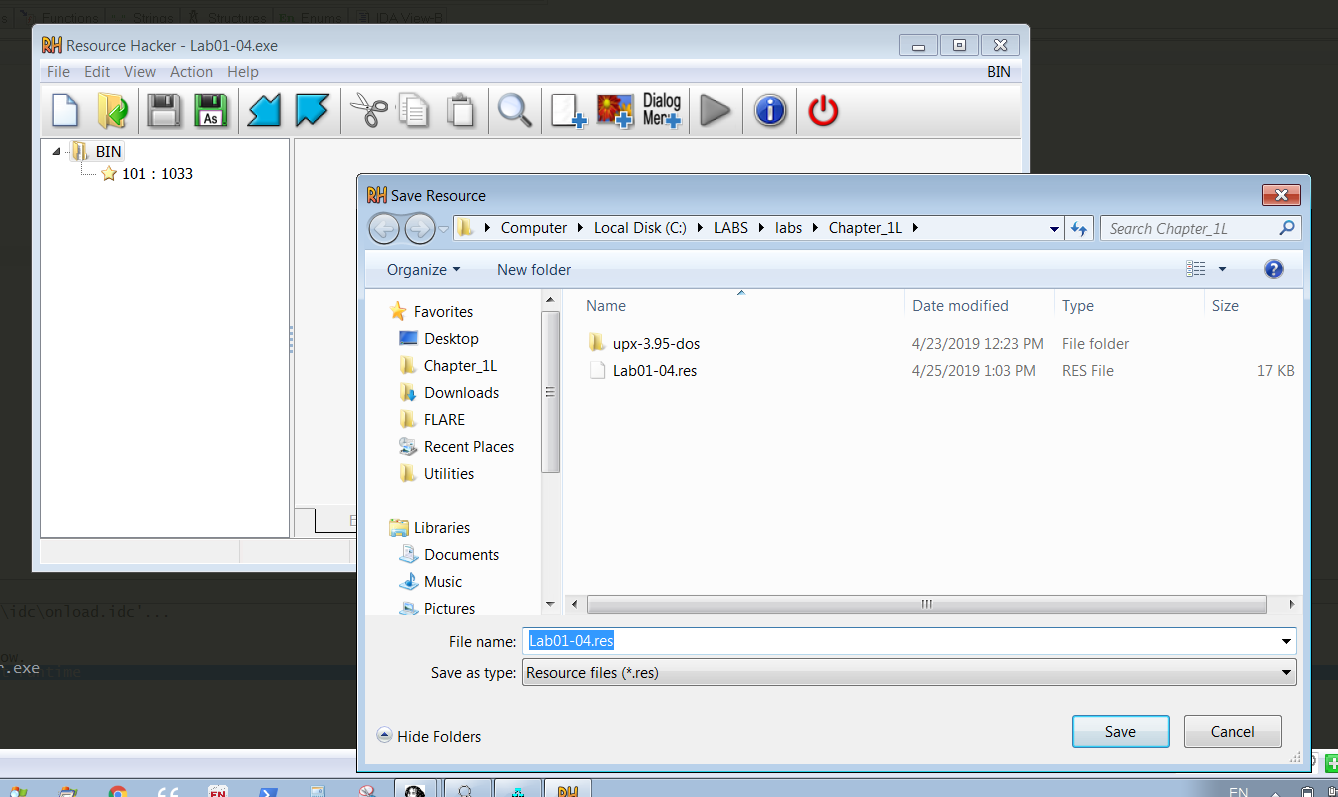




Далее, мы видим функцию **WinExec** (функция которая запускает файл, наш малварь)

**URLDownloadToFileA** (из библиотеки urlmon.dll) говорит сама за себя, что-то скачивает по сети в файл.

Судя по названию (хотя нельзя доверять только имени) файл возможно будет использоваться для обновления, либо дозагрузки других модулей малваря.



Скрин с ресурс хакера, видим что есть ресурс подключенный.

#### Лабораторная работа 3.1

## Проанализируйте вредоносный код в файле Lab03-01.exe, используя инструменты для динамического анализа.

Вопросы

### 1. Какие строки и импорты функций содержит этот вредонос?

### 2. Какими локальными индикаторами он обладает?

### 3. Существуют ли какие-либо сетевые сигнатуры, подходящие для этого вредоноса? Если да, то какие?

### 

### Какие строки и импорты функций содержит этот вредонос?

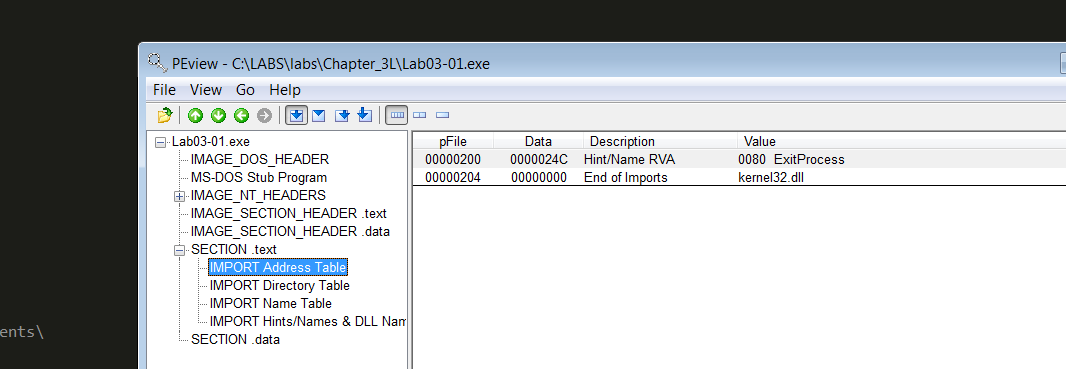
Подготовив идеальную среду для динамического анализа думал, что быстро справлюсь с этой лабораторной работы. В результате - потратил полдня на многочисленные танцы с бубном вокруг дебиана-докера-инетсим-винды пытаясь понять, ПОЧЕМУ нету сетевой активности от малварей. Wireshark ничего интересного не ловит, готовый контейнер с inetsim тоже не получает подозрительных логов. Вобщем, to cut a long story short, тупо надо запускать вирусы на windows XP…. :(

### В общем, по факту, теперь у меня есть:

1. Windows 7 Flare (для анализа)
2. Windows XP (для малварей :) )
3. Debian с контейнером inetsim для перехватки логов сетевой активности.
4. Manjaro based хост для управления всего и всем :)

Фух, вроде можно преступать (стандартные меры типа снэпшоты, реестр дампы и прочее сделал)

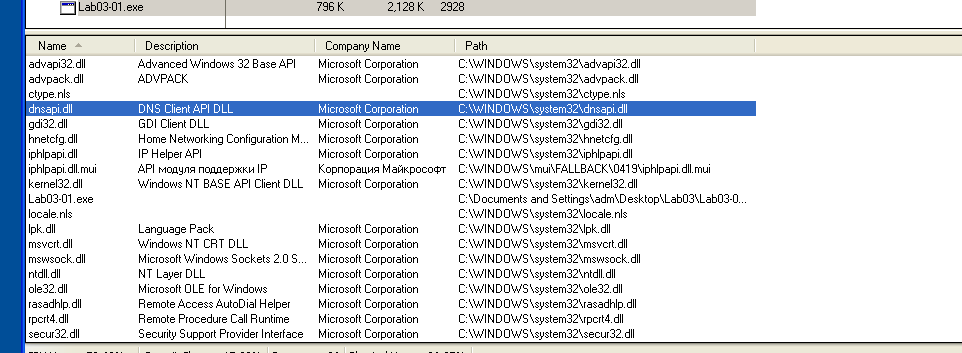
Сначала посмотрим, собственно через PEVIEW на импорты.



Круто! Есть импорт kernel32.dll.

А теперь посмотрим, что реально у нас отлавливает procexplorer для запущенного файла Lab03-01.exe

### ЛОКАЛЬНАЯ АКТИВНОСТЬ

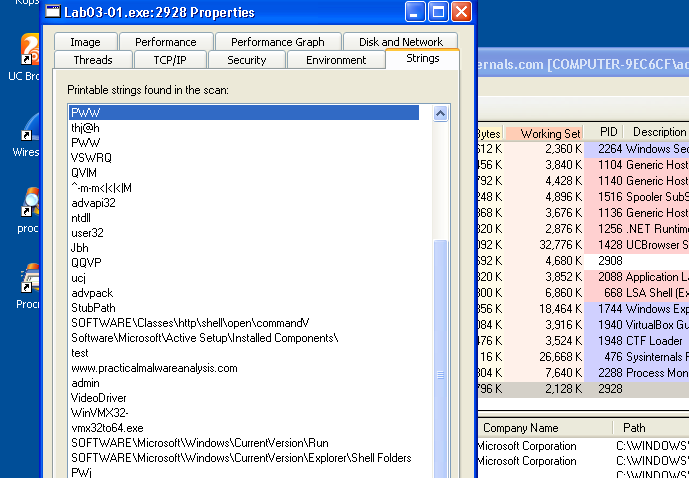


Немного побольше списочек получился))

Из интересного - сетевые библиотеки ntdll.dll dnsapi.dll ws2 и другие. Будем ждать сетевую активностью

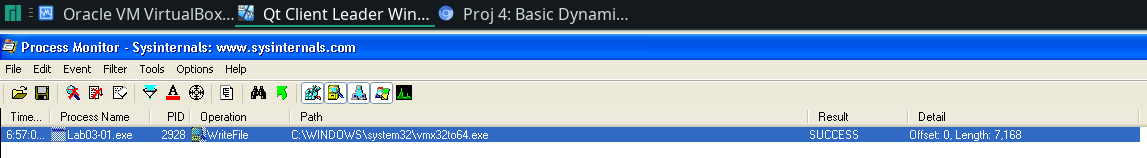
Advapi32.dll тоже известная библиотека для работы с реестром. Посмотрим потом что там с ним)

К слову, забыл упомянуть strings из procexp’a ->

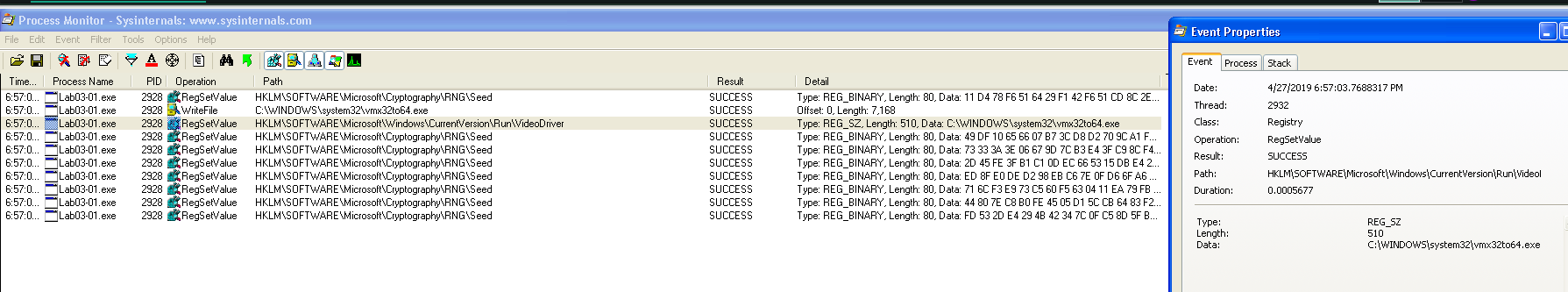


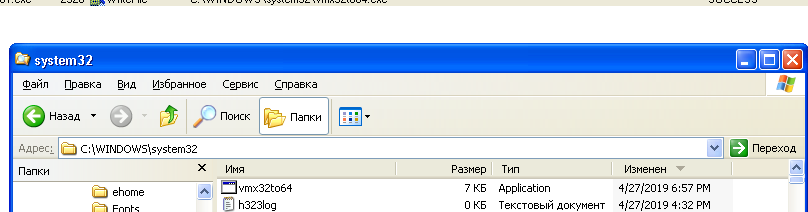
Тоже супер много чего полезного для дальнейшего анализа. Особенное внимание сразу на [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com) , vmx32to64.exe, VideoDriver, ветки с реестром еще какие-то тут тоже. В общем, стринги в открытой форме - это всегда приятно :)

А еще очень удобный тулз для динамического анализа это procmon:



Крутой фильтр на название файла (лаб-03) и тип операции - очень упрощают анализ. Видим как наш малварь записывает файл vmx32to64.exe. И в реестр тоже))





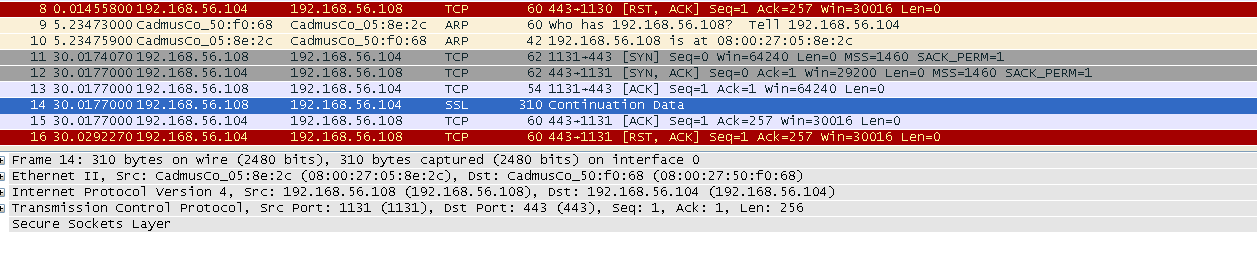
Проверил, действительно создал (сортировка по дате).

Создал в реестре запись (что подтвердило предварительный анализ)

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver:C:\WINDOWS\system32\vmx32to64.exe

### СЕТЕВАЯ АКТИВНОСТЬ

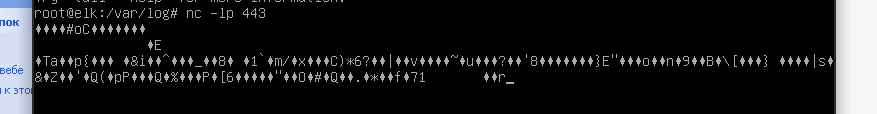
Как было понятно из сетевых библиотек (ntdll ws\_32 wsh2\_cpip) - малварь, почти наверняка, будет иметь сетевую активность. + еще в strings есть явные следы сетевой активности. Осталось только подтвердить это используя Wireshark & inetsim docker container logs.



На скрине с wireshark’oм хорошо видны tcp handshake’и и что-то похоже на https запросы. А вот ниже inetsim logs показывают как малварь отправляет что-то по ssl на 443 порт.

# 

Чтобы совсем хорошо разглядеть посмотрем в nc -lp 443:



#### Лабораторная работа #3.2

Проанализируйте вредоносный код в файле Lab03-02.exe, используя инструменты для динамического анализа.

### Вопросы

### 1. Как сделать так, чтобы данный вредонос себя установил?

### 2. Как позволить этому вредоносу запуститься после установки?

### 3. Как найти процесс, в котором он выполняется?

### 4. Какие фильтры можно установить в procmon, чтобы извлечь нужную информацию?

### 5. Какими локальными индикаторами обладает вредонос?

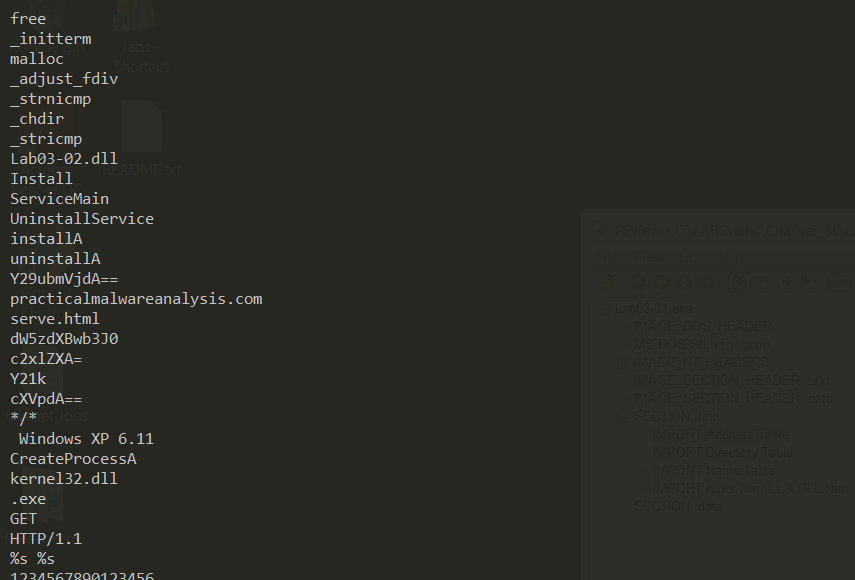
### 6. Существуют ли для него какие-либо подходящие сетевые сигнатуры?

## 

## 

### Установка вредоноса

## Имеем вредонос в виде dll файла. Ничто не мешает нам проанализировать его strings



## И много чего другого. Конкретно тут видно как можно установить этот малварь. Rundll32 <lab03-02.dll> Install

## Practialmalware.com serve.html HTTP/1.1 и многое другое возможно предсказывает сетевую активность.

## **Еще много чего инетесного можно увидеть в этих стрингах**

## **RegSetValueExA RegCreateKeyA (работа с реестром) +** SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

## **CreateServiceA DeleteService OpenServiceA SetServiceStatus** Работа вируса со службами

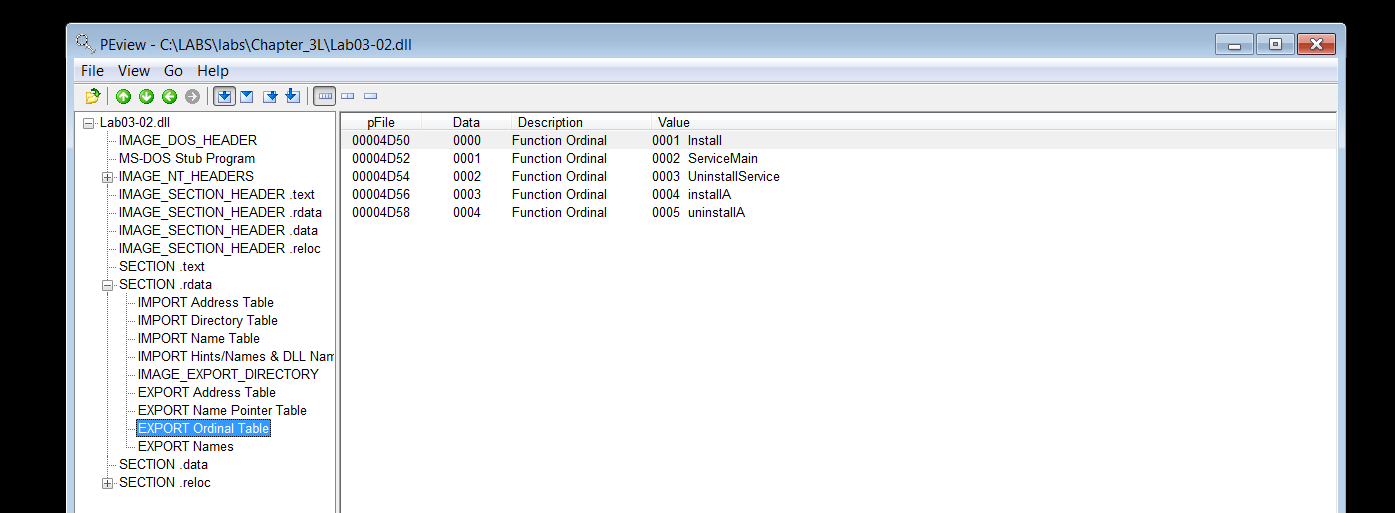
## **InternetReadFile HttpQueryInfoA HttpSendRequest InternetConnectA** Сетевая активность

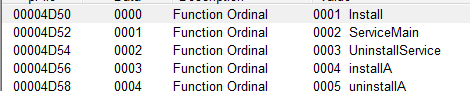
## 

Теперь по вопросу КАК ЗАПУСТИТЬ DLL нам поможет книга :) Из вариантов - запускать через rundll32.exe <name.dll> <argument> ЛИБО изменить dll header и сделать выполняемый файл. Выберем первое))

Тепреь вопрос, с какими аргументами надо запустить библиотеку? Для этого можно воспользоваться IDA PRO, а можно и через PEVIEW, глянуть export ordinal table. Да, забыл сказать ,что можно запускать как в таком формате rundll32.exe \*dll, Install либо через ординалы, в виде rundll32 \*.dll #1{2,3,4,5 в зависмости от функционала).

Сам функционал малваря вот тут смотрим:

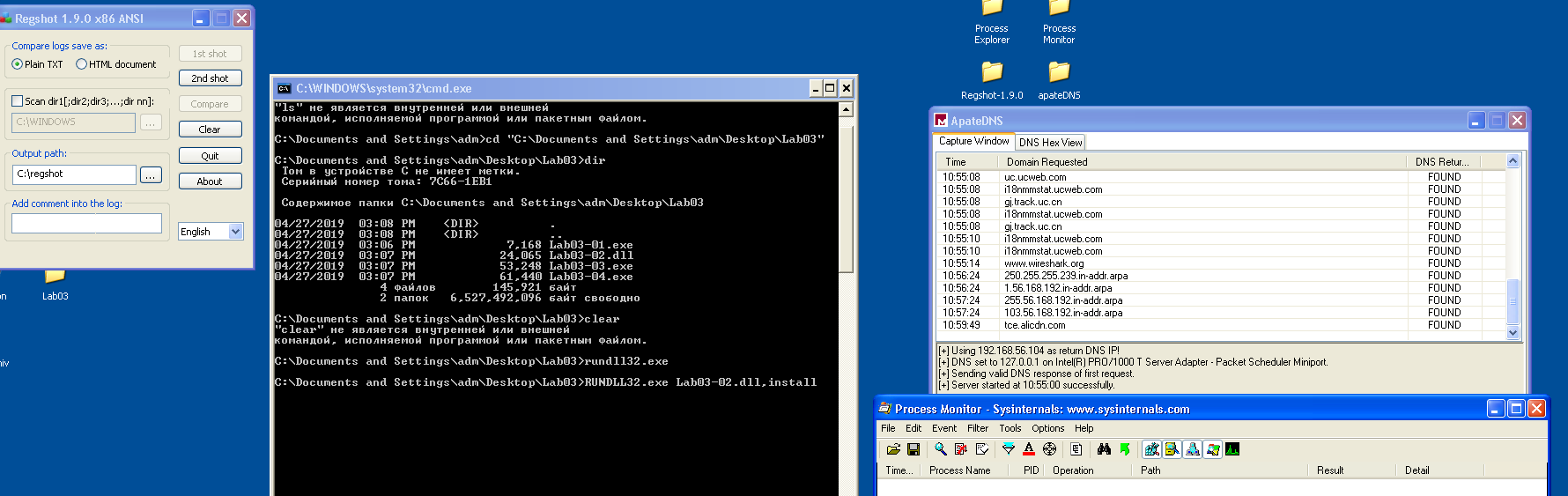


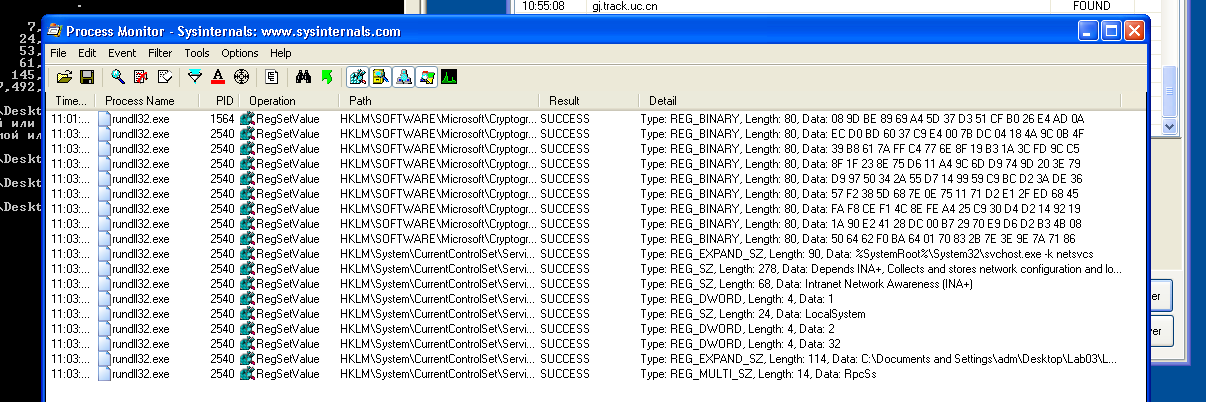


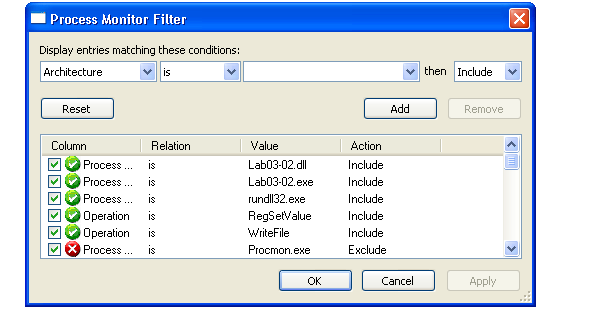
Удобно. Даже удаляет за собой малварь)) возможно :)

Ну мы однозначно посмотрим его Install, ServiceMain, InstallA подробнее.

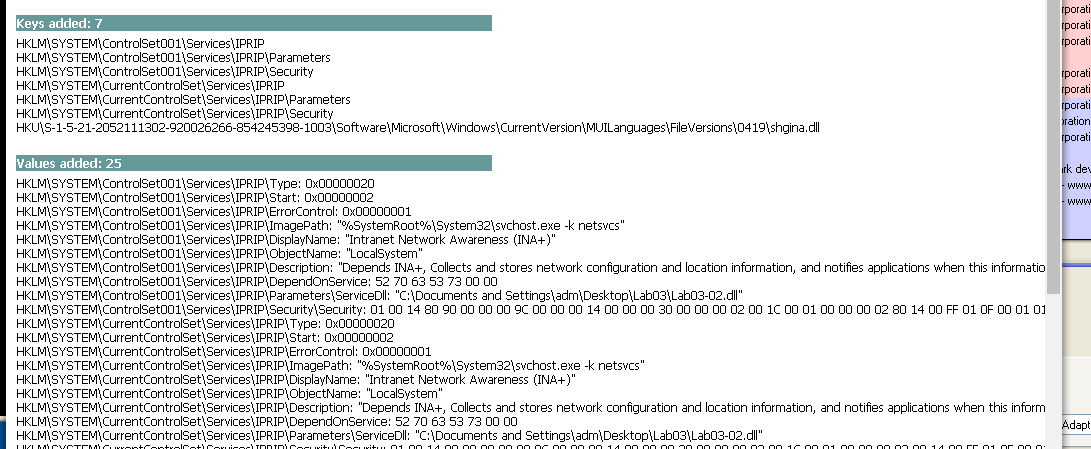
Сделаем регшоты и начнем запускать наш вирус.







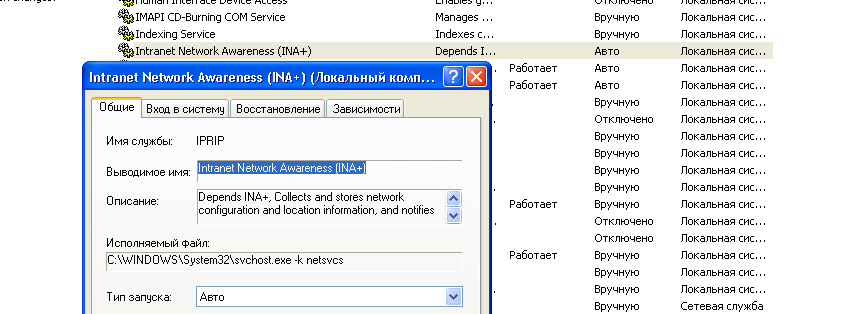




Вот, собственно наделал много скриншотов вверху. Сейчас поподробнее распишу что видел. Во-первых, я запустил вирус через rundll32.exe с аргументами Install, InstallA. После этого в процесс мониторе (фильтры выставил, скрин сделал) показались строки о добавлении в реестр записей. В финале - делаем второй шот - и анализируем логи.

Самое важное, что видим, это создание службы IPRIP c IMAGEPATH=svchost.exe -k netsvcs с именем Intranet Network Awareness.

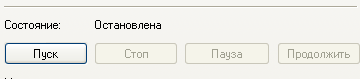
Сразу же и проверим (services.msc)



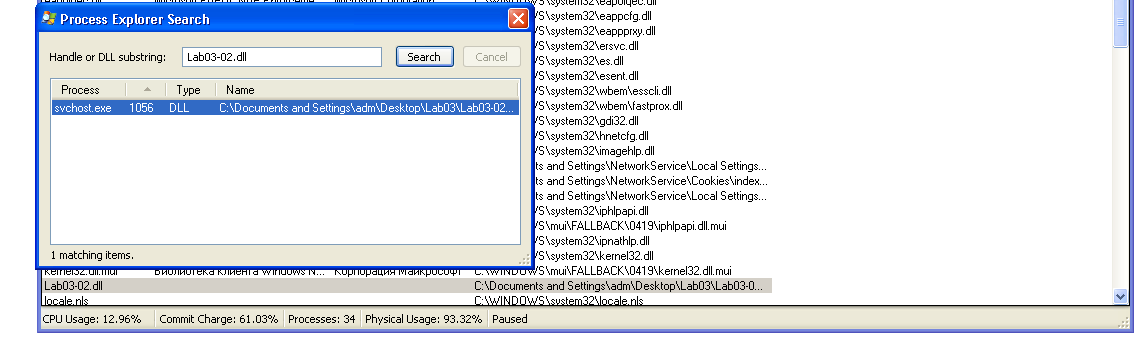
Есть!)

### 2. Как запустить малваря после установки

Ну тут по-моему очевидно, процесс запуска службы обычный. Вирус прописал себя в службы, типа запуска авто. Мы перезагружать ради этого компьютер не будем, и запустим его сейчас:



Теперь поищем нашу dll в procexp.



Находит её в svchost.exe, узнали PID 1056 вредоноса.

### 

### 4. Какие фильтры можно установить в procmon, чтобы извлечь нужную информацию?

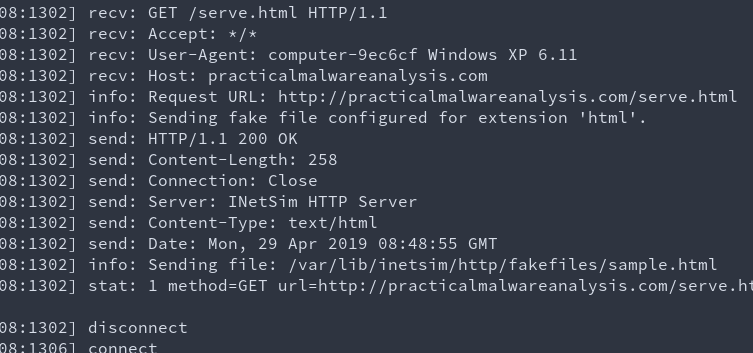
Скриншот своих фильтров уже делал выше. Теперь, с учетом полученного пида, можно его добавить в фильтры.

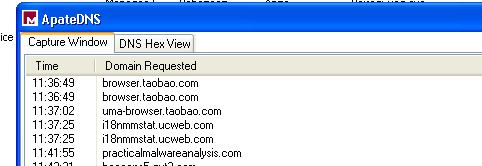
### 5. Локальные индикаторы

Собственно, все уже расписывал, поэтому сухо и по фактам: добавляет службу INA+, портит регистр :) (добавляет IPRIP разделы)

### 6. Сетевая активность

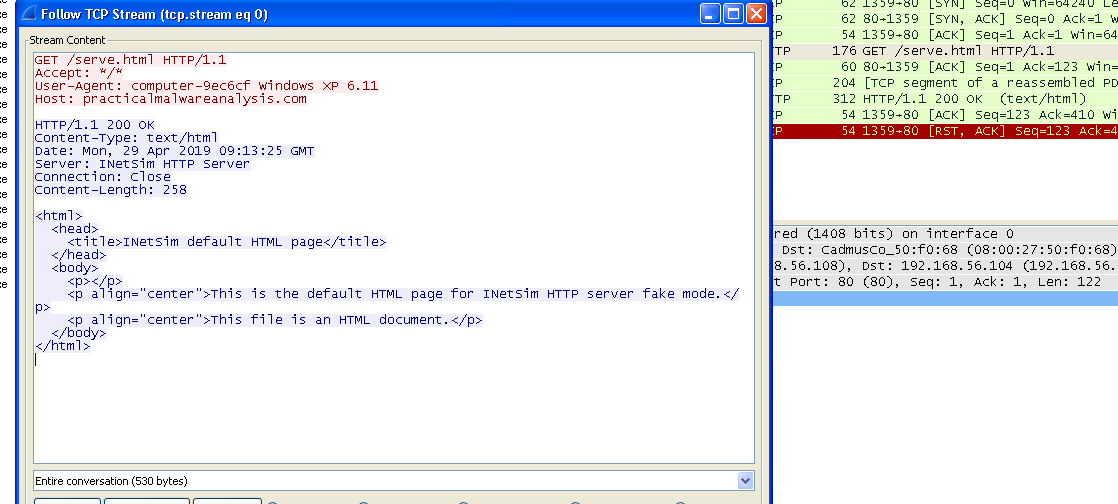
inetsim -docker-based сервер по-прежнему запущен, поэтому проверяем логи:





Вобщем, малварь пытается законнектится по странице practicalmalware.com/serve.html в надежде (возможно) для организации бэкдора или еще каких-то целей малваря. На данный момент страница недоступна. :)

* Забыл сразу заскринить скриншот с вайршарка:



Все уже подтверждалось выше.

#### Лабораторная работа

#### #3.03

Запустите вредоносный файл Lab03-03.exe и отследите его работу с помощью инструментов для базового динамического анализа в безопасной среде.

### TASKS:

### 1. Что можно заметить при мониторинге

### этого вредоноса с помощью Process Explorer?

### 2. Можете ли вы обнаружить какие-либо

### динамические изменения в памяти?

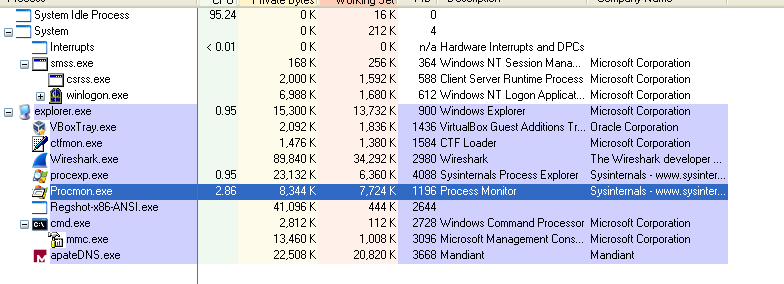
### 3. Какими локальными индикаторами обладает вредонос?

### 4. Для чего он предназначен?

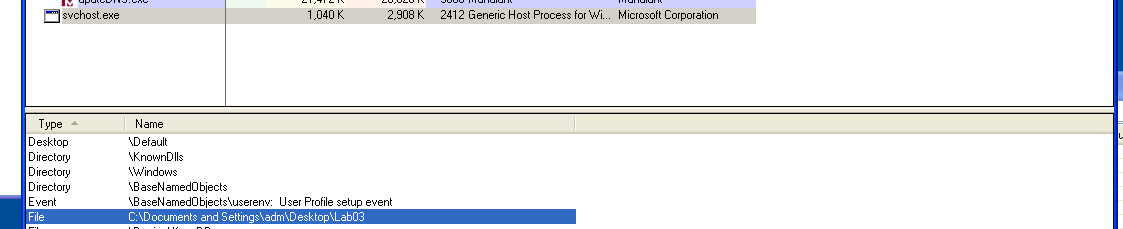
### Что можно заметить при мониторинге вредоноса с помощью Process Explorer?

### 

Без лишних слов, врубим procexp сделаем скрин, и запустим вирус.



На секунду загорелся Lab03-03.exe, потом сразу исчез, но появился svchost.exe, с виду как хороший, но… )



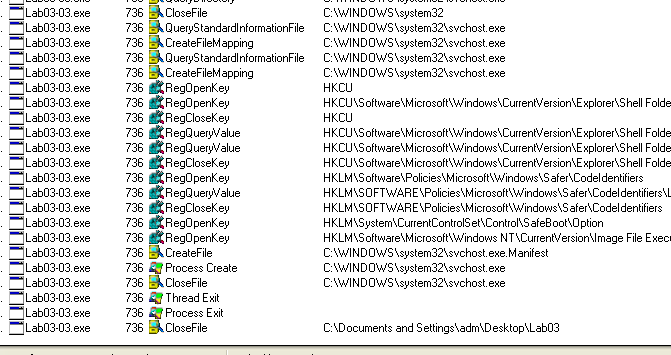
Всегда, когда начинаю сомневаться в подлинности процесса, проверяю свойства этого процесса. В частности тут я посмотрел handles этого процесса (по сути, хэндлы - это адрес, по которому хранится разная инфа по процессу). В procmon’e очень удобно нажать ctr+h и смотрим:



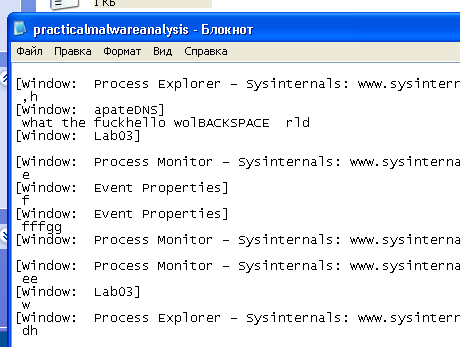
Думаю в оригинальном svchost такого не увидим)) Если остались ещё какие-то сомнения можно почекать strings у файлов, поискать отличия. Можно также сделать дамп памяти процесса, и в дебагере чтото отреверсить. Можно даже правой клавишей мыши и Sent to VirusTotal :D

### 2. Можете ли вы обнаружить какие-либо

### динамические изменения в памяти?



В папке где запускали вирус появился текстовый файл. Практически сразу стало понятно, что это keygrabber:



### 3. Какими локальными индикаторами обладает малварь

Ну как минимум создает процесс svchost.exe по факту создает кейграббер. + файл с записанными клавишами в корне папке, где был запущен малварь.

### 4. Для чего он предназначен?

Сетевой активности не обнаружил (во всяком случае никаких логов на инетсиме, вайршарк ничего аномального не показал). Предназначен для кейграббинга:)

Лабораторная работа

#### #3.04

.

### TASKS:

### 1. Что произойдет, когда вы запустите этот файл?

### 2. Что препятствует динамическому анализу?

### 3. Есть ли какие-то другие способы запустить эту программу?

### Что произойдет если запустить этот малварь?

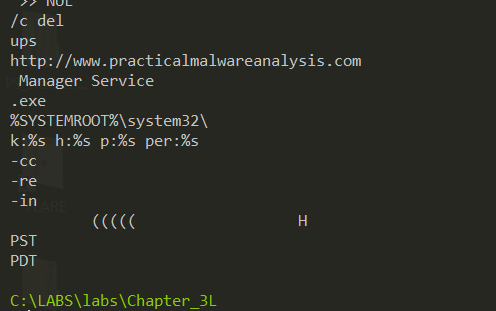
Ну по факту, файл самовыпилился. Пропал. Удалился. :) (в итоге скачал заново и постараюсь разобраться, анализируя регшот, procmon, procexp).

UPDATE: ничего интересного в регшоте и процмоне не обнаружил :(

HKU\S-1-5-21-2052111302-920026266-854245398-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR\_EHACNGU:P:\Qbphzragf naq Frggvatf\nqz\Qrfxgbc\Yno03\Êîïèÿ Yno03-04.rkr: 01 00 00 00 06 00 00 00 F0 FC DA 43 79 FE D4 01

HKU\S-1-5-21-2052111302-920026266-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\adm\Desktop\Lab03\Êîïèÿ Lab03-04.exe: "Êîïèÿ Lab03-04"

Посмотрел через strings.



### 2. Что препятствует динамическому анализу?

На самом деле, если я правильно понял, то для запуска малварю нужно скормить правильный(ые) аргументы. Иначе он выпиливается вызовом del через cmd.

### 3. Другие способы запуска малваря

В таких случаях очень помогают дебагеры, дойдя до точки вызова del перенаправить ход программы.

Либо отреверсить программу и понять, из-за чего программа выпиливается.