# 01. Подготовка рабочего окружения 02. Анализ семпла Lab01: динамический анализ 03. Продолжаем исследование. Смотрим реестр 04. Запускаем сетевую акулу Wireshark 05. Что нам покажет Process Explorer? 06. Возвращаемся к OllyDbg 07. Заключение С прошлого номера мы запустили цикл статей про такую интересную вайтхетотрасль, как анализ малвари. Интересно в ней то, что исследователь малвари занимается все тем же взломом, причем программ, авторы которых не очень хотели

Содержание статьи

бы, чтобы их творения взламывали :), но при этом хакеру-исследователю совершенно не стоит опасаться юридических претензий от авторов малвари. В прошлой статье мы разобрали теоретические вопросы, литературу и хорошие онлайн-ресурсы, а сегодня, дорогие друзья, будем практиковаться в анализе malware-кода, основываясь на рабочих образцах вредоносов. Подготовка рабочего окружения

Все эксперименты по анализу малвари мы будем выполнять в нашей лаборатории, это заранее подготовленная виртуальная среда с предустановленной Windows XP. Да-да,

## старушка ХР нам очень даже подойдет, поскольку некоторые изучаемые образцы могут вызывать ошибки при запуске на новых версиях ОС. И к тому же все программные

для быстрого отката в случае необходимости.

инструменты проверены и гарантированно будут работать на ХР. Образцы малвари, приведенной в этой статье, можно найти здесь. Каждый изучаемый бинарный код вредоноса мы будем называть лабами (Labs). Помни, при распаковке архива с лабами антивирус будет распознавать файлы соответствующим образом, что, если вдуматься, очень логично :).

И еще один совет. Поскольку мы будем запускать малварь, выполнять код пошагово в отладчике или мониторить активность вредоноса в системе, в результате этих действий может пострадать операционная система, а именно реестр, системные файлы и прочее. Поэтому перед началом любых экспериментов рекомендуем создавать снимки системы (snapshots)

Анализ семпла Lab01: динамический анализ Используемые инструменты: IDA Pro;

#### PEiD; RegShot; Procmon;

INetSim;

- Wireshark; Process Explorer;
- OllyDbg.

JEHER

☑ .data:00401943

PEiD v0.95

80000000



Другие статьи в выпуске:

Содержание выпуска Подписка на «Хакер»

Address Ordinal Name Library m 00400200 ExitProcess kernel32 Просмотр функции ExitProcess системной библиотеки kernel32

Xakep #215. Второй фактор

Итак, первым делом запускаем PEview и смотрим импорт функций, который использует этот

вредонос. Видим, что используется функция ExitProcess из системной библиотеки kernel32.

А вот и сам импорт в подробностях: Address Length String Type kernel32.dll ■ .text:0040025A 0000000D ☑ .data:00400EF7 00000005 C \b1\a1G 🖼 .data:00401087 C 00000007 \n6I\*h<8 🗹 .data:004010A7 C ^-m-m<|<|<|M\rM\r^ 00000010 🔽 .data:00401247 00000006 C ntdll ☑ .data:0040125E 00000007 user32 ☑ .data:004013AB C ��ദ[♠\n= 80000000 😨 .data:004014D3 0000000C unico... jjjjjj 🗹 .data:004014F7 80000000 advpack 🖼 .data:00401623 80000000 C StubPath 🗹 .data:0040162F 00000029 C SOFTWARE\\Classes\\http\\shell\\open\\commandV ☑ .data:0040165B 00000035 Software\\Microsoft\\Active Setup\\Installed Components\\ ☑ .data:0040169C C 00000022 www.practicalmalwareanalysis.com ☑ .data:004016D4 00000007 C admin\t\r ☑ .data:004016E2 VideoDriver 0000000B WinVMX32-🖼 .data:004016F1 00000009 C 🖫 .data:004016FD 0000000D C vmx32to64.exe

AppData

Так-так, мы видим ключи реестра, которые прописывает вредонос после своего запуска.

vmx32to64.exe, маскирующийся под драйвер видеоадаптера с именем WinVMX32.

peectpa SOFTWARE\Classes\http\shell\open\commandV (IExplorer.exe) и

Software\Microsoft\Active Setup\Installed Components\.

Обращаем внимание на присутствие некоторой DNS-записи веб-ресурса и создаваемый файл

У нас есть подсказка, мы должны отследить сетевую активность ресурса http://www.practicalmalwareanalysis.com. Мы можем также отслеживать и проверять ключи

 $\times$ 

...

Окно PEview с подробностями импорта

Первым делом мы должны разобраться с файлом для vmx32to64.exe, который вредонос создает после своего запуска и копирует в папку C:\Windows\system32. Запускаем анализатор PEiD, видим, что файл ничем не упакован.

00000208 Entrypoint: EP Section: > .text 00000208 File Offset: First Bytes: B8,00,04,40 > Linker Info: 5.12 Subsystem: Win32 GUI > PEncrypt 3.1 Final -> junkcode Multi Scan Task Viewer Exit Options About

C:\Users\User\Desktop\Practical Malware Analysis Labs\BinaryCollecti

Stay on top >>> -> Анализ бинарного файла с помощью PEiD Однако используются некоторые фичи для затруднения отладки ехе-файла. Ниже приведен скриншот из отладчика OllyDbg. Labes-81.08488670 DWORD PTR SS: [EBP-9CA] 80808246 (NO,NB,E,BE,NS,PE,GE,LE) 4F4 atdil.KiFastSystemCallRe Просмотр malware в отладчике OllyDbg

По адресу 0х401259 был выполнен вызов к 0х401265. Это опкод, который вызывает обратный

адрес 0х40125е выполнения в стеке. По первому адресу, 0х401265, был сделан вызов к

некотором аргументе LPCSTR, передаваемом в... массив символов! Обратный адрес

библиотеке kernel32.LoadLibraryA. Но мы-то знаем, что функция LoadLibrary нуждается в

Запускаем RegShot. HKU\S-1-5-21-1993962763-484061587-682003330-500\Software\Microsoft\Windows\Currentversion\Explorer\Complg32\OpensaveMRU\\* HKU\S-1-5-21-1993962763-484061587-682003330-500\Software\Microsoft\Windows\Currentversion\Explorer\Complg32\OpensaveMRU\hiv HKU\S-1-5-21-1993962763-484061587-682003330-500\Software\Microsoft\Windows NT\CurrentVersion\TaskManager Values added: 15 HKLM\SOFTWARE\Microsoft\windows\CurrentVersion\Run\VideoDriver: 43 3A 5C 57 49 4E 44 4F 57 53 5C 73 79 73 74 65 6D 33 32 5C 76 6D 78 33 3 HKU\S-1-5-21-1993962763-484061587-682002330\_500\Software\Microsoft\windows\CurrentVersion\Explorer\EileExts\ hiv\onenWith ist\a: "Benchot-

Control

App Mar

App Mar

App Pat

App Applets

Control

Data

(value not set)

%systemroot%\system32\dumprep 0 -k

C:\WINDOW5\system32\vmx32to64.exe.

C:\Program Files\VMware\VMware Tools\VMwareTray.exe

C:\Program Files\VMware\VMware Tools\VMwareUser.exe

Результат анализа в RegShot

□ CurrentVers Name

Applets
 Control

- CSCSett

### DateTim Output path Из лога RegShot мы выяснили, что вредонос пытается выполнить команду C:\WINDOWS\system32\vmx32to64.exe при своем запуске.

Clear

случайных 256 байт данных через порт 80 и 443.

.....>q...x.....W.6x.....E.#...5,.{2J..Qk}

!This program cannot be run in DOS mode.

CONNECT %s:%i HTTP/1.0

Rich .text .data ExitProcess kernel32.dll cks=u ttp=

QSRW PWW thj@h

...%..<...1.\o.?}.%.....H..CL...g?.[.....!XK;. ....t.;.[....q...(-\* ...j.y.../K.3]<.]!v.e..]...!C

-Compare logs save as: -

Scan dir1[;dir2;dir3;...;dir nn]:

Follow TCP Stream

-Stream Content

0x40125e заворачивает вызов опкодом в библиотеку user32

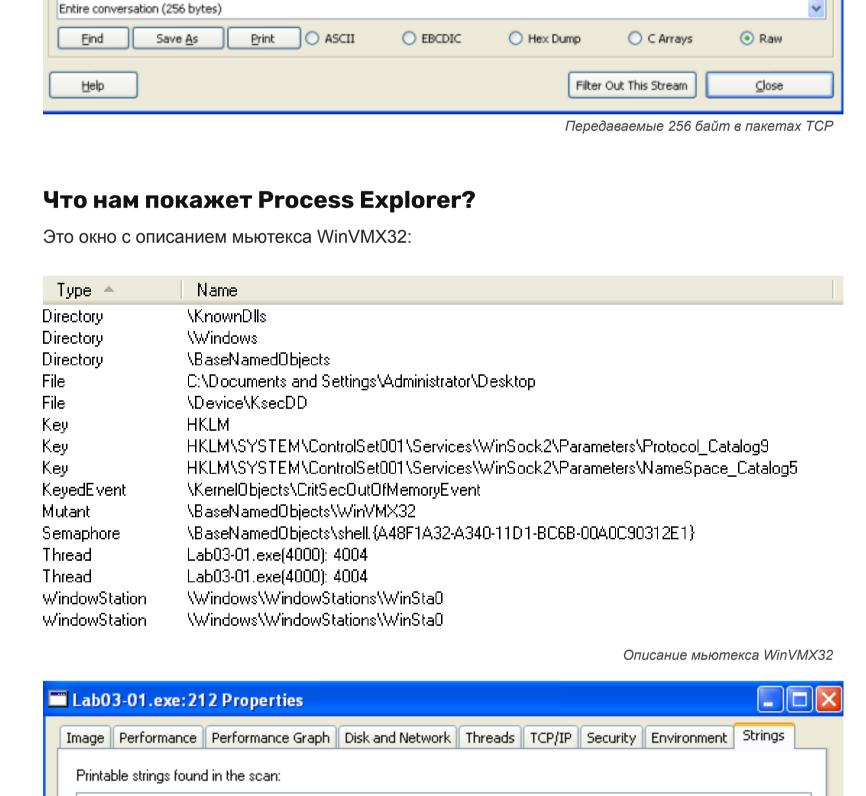
Продолжаем исследование. Смотрим реестр

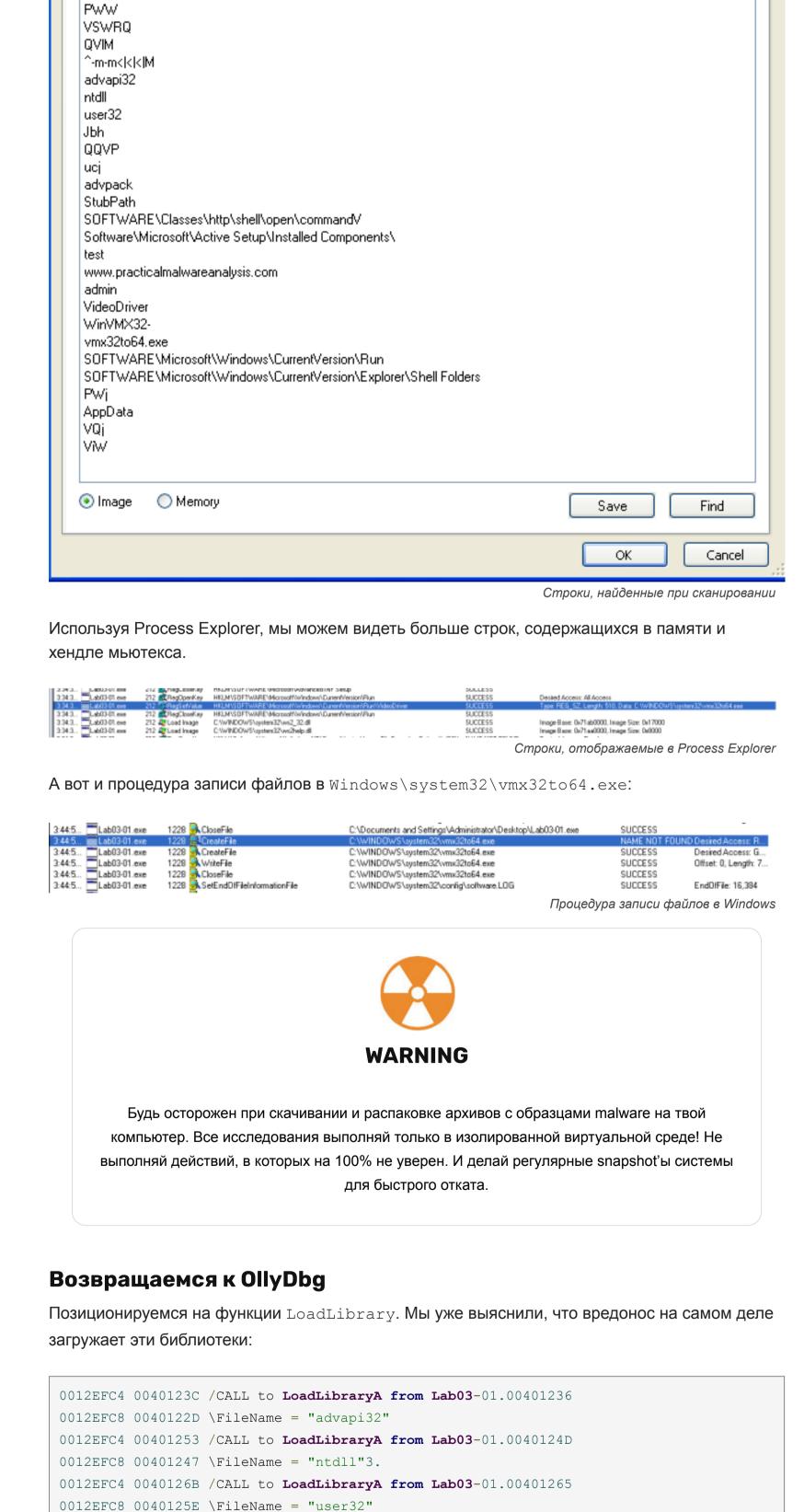
```
Хотим узнать подробности?
Запускаем сетевую акулу Wireshark
   2 0.00014500 Vmware_7e:95:94
                                 Vmware_0b:14:51
                                                              60 192.168.1.100 is at 00:0c:29:7e:95:94
                                                             92 Standard query 0x6043 A www.practicalmalwareanalysis.com
108 Standard query response 0x6043 A 192.168.1.100
    3 0.00015300192.168.1.101
    4 0.00691700192.168.1.100
  5 0.00750800192.168.1.101
                                 192.168.1.100
                                                             62 vfo > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   6 0.00760400192.168.1.100
                                 192.168.1.101
                                                            62 https > vfo [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
   7 0.00762500 192.168.1.101
                                 192,168,1,100
                                                              54 vfo > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
   8 0.00768500 192.168.1.101
                                 192.168.1.100
                                                             310 Continuation Data
                                                   SSL
                                                              60 https > vfo [ACK] Seq=1 Ack=257 win=30016 Len=0
   9 0.00813800192.168.1.100
                                 192.168.1.101
                                                              60 who has 192,168,1,101? Tell 192,168,1,100
  11 5.01424400 Vmware_7e:95:94
                                 Vmware_0b:14:51 ARP
  12 5.01428400 vmware_0b:14:51
                                 Vmware_7e:95:94
                                                             42 192.168.1.101 is at 00:0c:29:0b:14:51
                                                                                              Анализ сетевых пакетов в Wireshark
```

Мы видим запрос на сайт <a href="http://www.practicalmalwareanalysis.com">http://www.practicalmalwareanalysis.com</a> и соединение SSL. Если

приглядеться внимательно, то можно увидеть, что в пакетах ТСР присутствует отправка

Помним, что, помимо ключей реестра, в импорте мы нашли некую DNS-запись веб-ресурса.





### Thread Lab03-01.exe(1348): 460 Lab03-01.exe(1348): 460 Thread Нашли! Машина инфицирована.

Ну и напоследок картинки из IDA Pro.

.data:004011F7

No export peb+30h found 0:011> dt nt!\_PEB 7efde000

Заключение

ntdll!\_PEB +0x000 InheritedAddressSpace : 0 ''

+0x001 ReadImageFileExecOptions: 0 ''
+0x002 BeingDebugged : 0x1 ''
+0x003 BitField : 0 ''
+0x003 ImageUsesLargePages : 0y0
+0x003 IsProtectedProcess : 0y0

+0x004 Mutant : 0xffffffff Void

Key

KeyedEvent

Semaphore

0012EFC8 004014F7 \FileName = "advpack"

0012EFC4 00401505 /CALL to LoadLibraryA from Lab03-01.004014FF

Проверяем, открыт ли мьютекс WinVMX32 в оперативной памяти.

\KernelObjects\CritSecOutOfMemoryEvent

NBaseNamedObjects\WinVMX32

А что же с замаскированным файлом WinVMX32? Тут все просто: если vmx32to64.exe создан

\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

jnz.

Мьютекс WinVMX32

short loc\_4011EF

edi

и находится в C:\WINDOWS\system32, то, скорее всего, процесс запущен в памяти.

HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters

```
.data:004011F9
                                   pop
.data:004011FA
                                            eax, large <mark>fs</mark>:30h
                                   MOV
.data:00401200
                                            eax, [eax+OCh]
                                   MOV
                                            esi, [eax+1Ch]
.data:00401203
                                   MOV
                                   lodsd
.data:00401206
                                            dword ptr [eax+8]
.data:00401207
                                   push
 .data:0040120A
                                            [ebp+var_4C1]
                                   pop
                                            4134D1ADh
                                   push
 .data:00401210
.data:00401215
                                             [ebp+var 4C1]
                                   push
.data:0040121B
                                   push
                                            sub_400A70
                                   call
.data:0040121D
                                                    Получим вызов kernel-based
0:011> !peb+30h
```

```
+0x003 IslegacyProcess : 0y0
+0x003 IslmageDynamicallyRelocated : 0y0
+0x003 SkipPatchingUser32Forwarders : 0y0
+0x003 SpareBits : 0y000
+0x004 Mutant : 0xfffffff Void
      +0x004 Mutant
                                                        : 0xffffffff Void
      +0x008 ImageBaseAddress : 0x00400000 Void
      +0x00c Ldr : 0x77260200 _PEB_LDR_DATA
+0x010 ProcessParameters : 0x00821738 _RTL_USER_PROCESS_PARAMETERS
      +0x014 SubSystemData : (null)
                                                                                  Обращаем внимание на смещение peb + 30h & 0ch offset
0:011> !peb+30h
No export peb+30h found
0:011> dt nt!_PEB 7efde000
ntdll!_PEB
      +0x000 InheritedAddressSpace : 0 ''
     +0x000 InheritedAddressSpace : 0 '
+0x001 ReadImageFileExecOptions : 0 '
+0x002 BeingDebugged : 0x1 '
+0x003 BitField : 0 '
+0x003 ImageUsesLargePages : 0y0
+0x003 IsProtectedProcess : 0y0
+0x003 IsLegacyProcess : 0y0
+0x003 IsImageDynamicallyRelocated : 0y0
+0x003 SkipPatchingUser32Forwarders : 0y0
+0x003 SpareBits : 0y000
+0x004 Mutant : 0xffffffff
```

+0x014 SubSystemData : (null) Листинг функции

+0x008 ImageBaseAddress : 0x00400000 Void +0x00c Ldr : 0x77260200 \_PEB\_LDR\_DATA +0x010 ProcessParameters : 0x00821738 \_RTL\_USER\_PROCESS\_PARAMETERS

Анализ каждого отдельного образца malware — это часто творческий процесс. Заранее трудно предугадать, что ждет исследователя впереди. Используй как можно больше инструментов и методов для всестороннего анализа и получения исчерпывающего заключения о функциональности.

INFO

Поздравляю, ты прошел боевое крещение и стал крутым крэкером устаревшей малвари :).

Конечно, до настоящего аналитика еще долгая дорога, но ты уже смог разобраться, как можно, используя разнообразные инструменты и подходы, самостоятельно изучать любые образцы малвари. В следующих статьях нас ждут крутые и более сложные вредоносы.

Скачание ислатитем! – SuperSliv.Biz - Присоединяйся!