



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно  
&& видно?



Напишите в чат, если есть проблемы!

Ставьте  если все хорошо

# Динамический анализ кода

Распаковка, просмон, fiddler/wireshark, api  
monitor



1

**Распаковка**

- ✓ Очень мало строк
- ✓ Очень мало функций в таблице импорта (\*)
- ✓ Высокая энтропия ( $> 6$ ) → мало «пустых» мест в файле

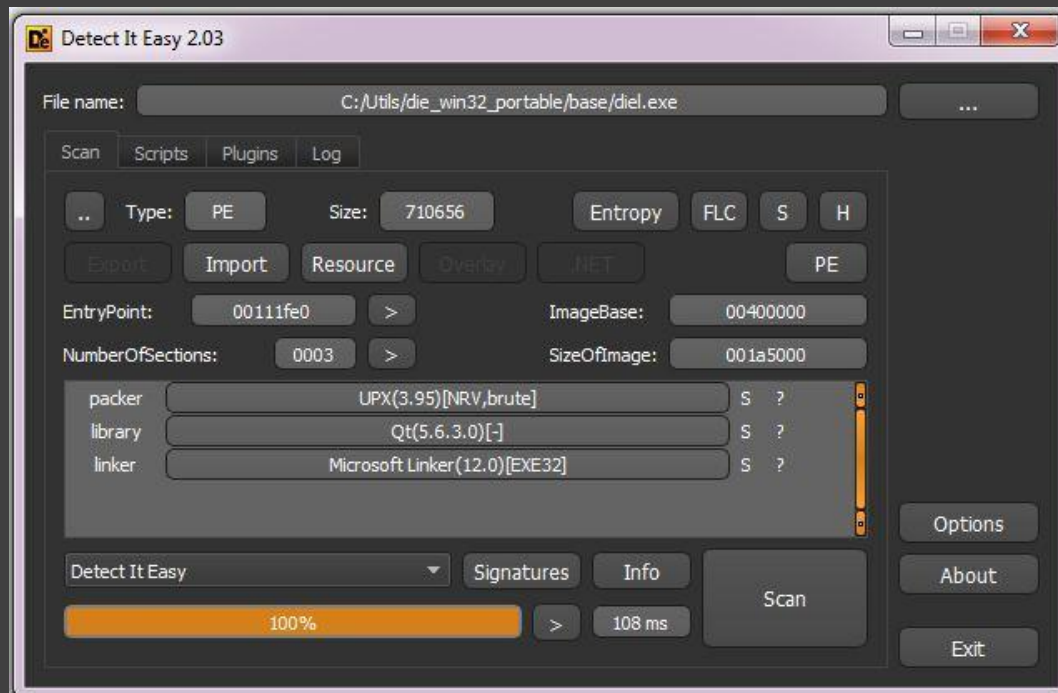
```
KERNEL32.dll•  
DLG_ABOUT  
DLG_REGIS•  
3333330•  
WndProc•  
crackme.EXE•  
v18.03N4n  
"Gisa&m  
@ wSr{k{H  
pP!llhu  
USER32.dql  
WindowR  
BitvmPp  
y0[0'1?  
E"%xft!  
4gMpApbpoTu6  
@K@u@A@  
LoadLibraryA•  
GetProcAddress•
```



```
0 LoadLibraryA | KERNEL32.dll  
0 GetProcAddress | KERNEL32.dll
```

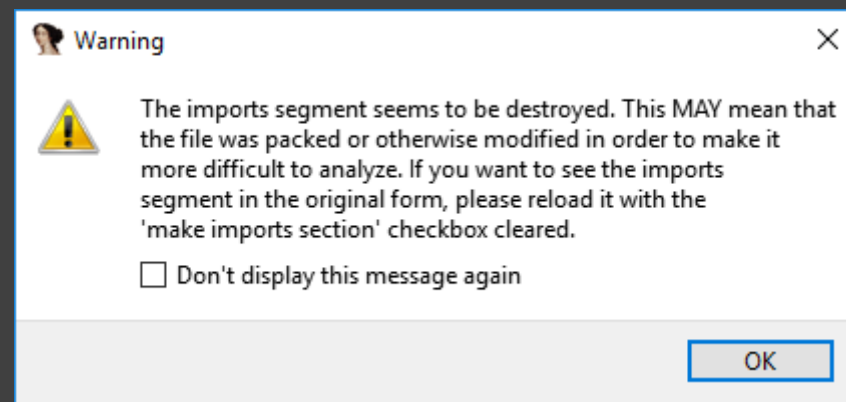
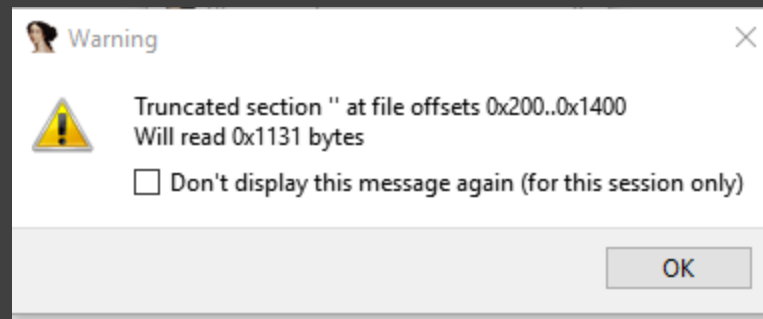


## Анализатор упаковщиков

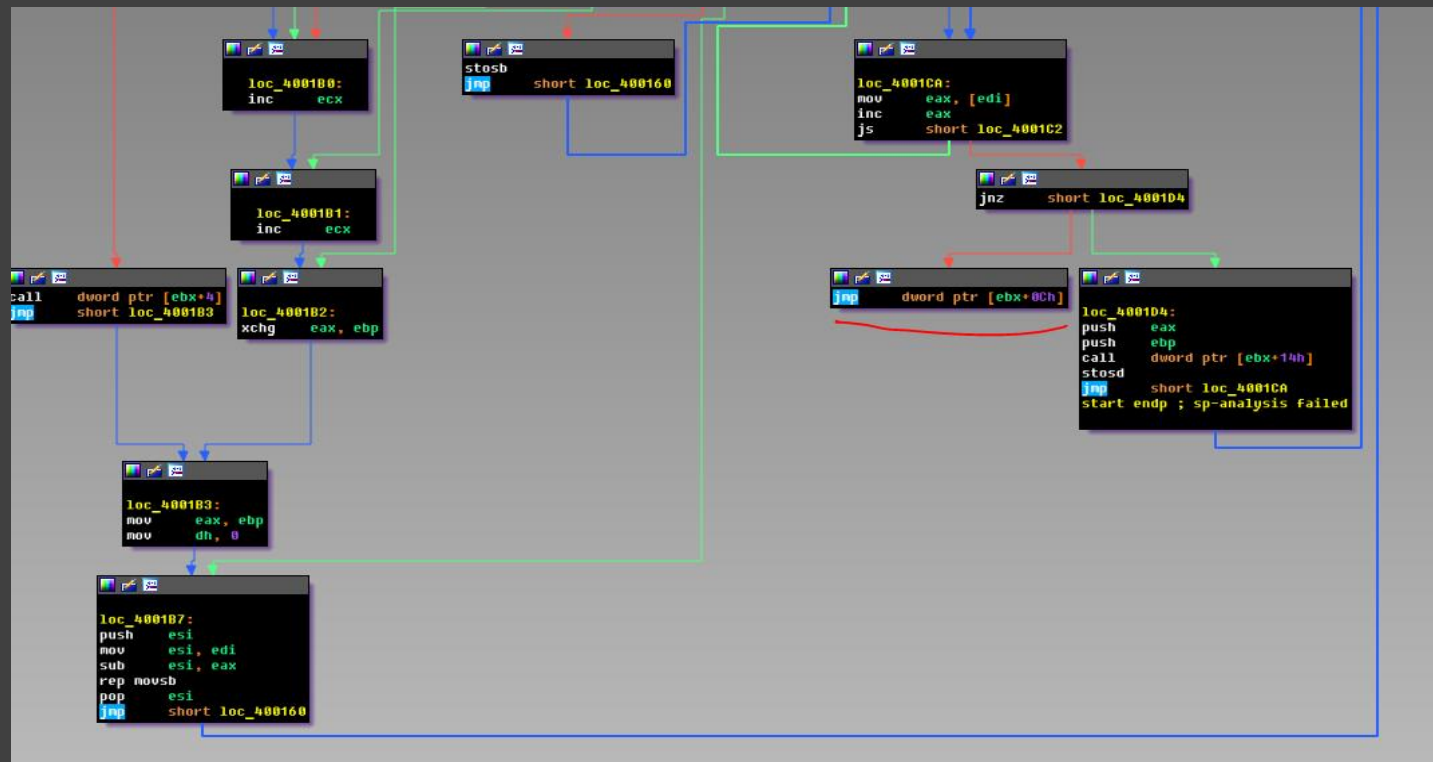


<http://ntinfo.biz/index.html>

## Отладка упакованного PE файла



Устанавливаем breakpoint в «конец»



Устанавливаем breakpoint в «конец»

●	004001BA	2B F0	sub esi,eax
●	004001BC	F3 A4	repe movsb
●	004001BE	5E	pop esi
●	004001BF	^ EB 9F	jmp crackme.400160
●	004001C1	5E	pop esi
→	004001C2	AD	lodsd
●	004001C3	97	xchg edi,eax
●	004001C4	AD	lodsd
●	004001C5	50	push eax
●	004001C6	FF 53 10	call dword ptr ds:[ebx+10]
●	004001C9	95	xchg ebp,eax
→	004001CA	8B 07	mov eax,dword ptr ds:[edi]
●	004001CC	40	inc eax
●	004001CD	^ 78 F3	js crackme.4001C2
●	004001CF	^ 75 03	jne crackme.4001D4
●	● 004001D1	FF 63 0C	jmp dword ptr ds:[ebx+C]
→	004001D4	50	push eax
●	004001D5	55	push ebp
●	004001D6	FF 53 14	call dword ptr ds:[ebx+14]
●	004001D9	AB	stosd
●	004001DA	^ EB EE	jmp crackme.4001CA
●	004001DC	33 C9	xor ecx,ecx
●	004001DE	41	inc ecx
→	004001DF	FF 13	call dword ptr ds:[ebx]
●	004001E1	13 C9	adc ecx,ecx
●	004001E3	FF 13	call dword ptr ds:[ebx]
●	004001E5	^ 72 F8	jb crackme.4001DF
●	004001E7	C3	ret
●	004001E8	02 D2	add dl,d1
●	004001EA	^ 75 05	jne crackme.4001F1
●	004001EC	8A 16	mov dl,byte ptr ds:[esi]

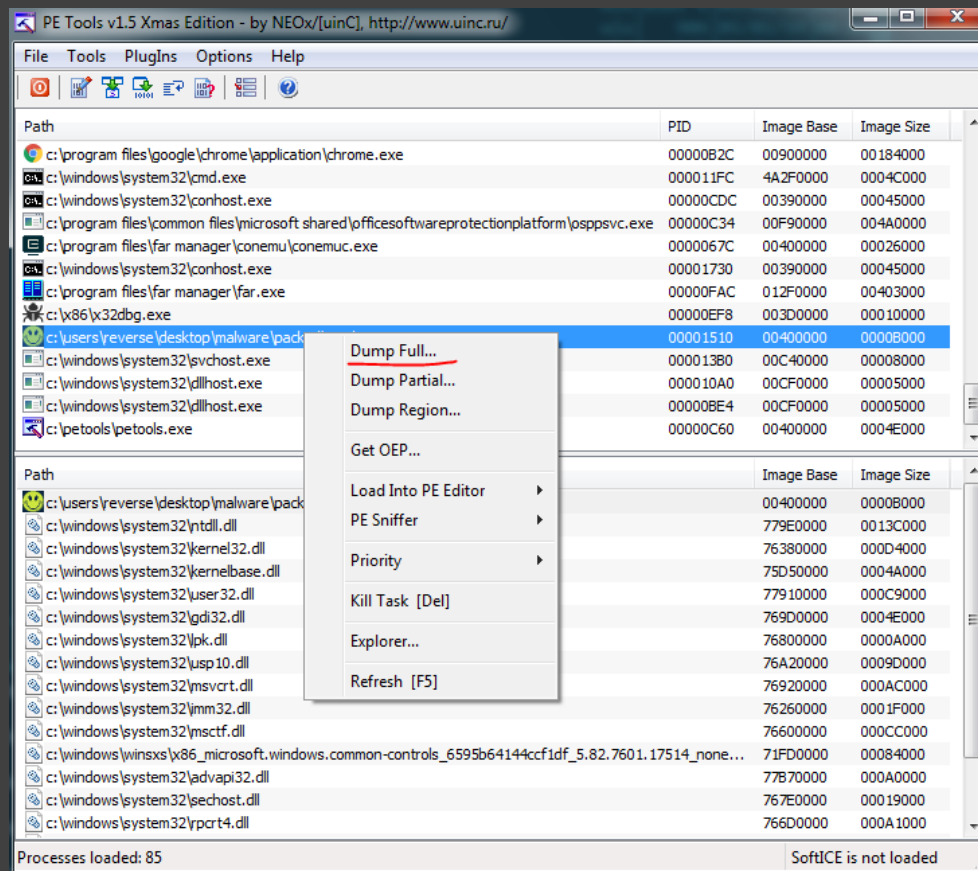
Замечаем вызовы API функций, строки...

004001C4	AD	108D	push
004001C5	50		push eax
004001C6	FF 53 10		call dword ptr ds:[ebx+10]
004001C9	95		xchg ebp,eax
004001CA	8B 07		mov eax,dword ptr ds:[edi]
004001CC	40		inc eax
004001CD	^ 78 F3		js crackme.4001C2
004001CF	^ 75 03		jne crackme.4001D4
004001D1	^ FF 63 0C		jmp dword ptr ds:[ebx+C]
004001D4	50		push eax
004001D5	55		push ebp
004001D6	FF 53 14		call dword ptr ds:[ebx+14]
004001D9	AB		stosd
004001DA	^ EB EE		jmp crackme.4001CA
004001DC	33 C9		xor ecx,ecx

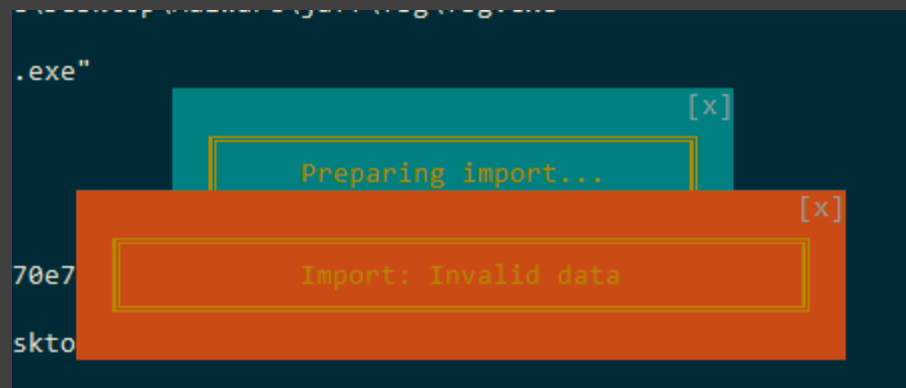
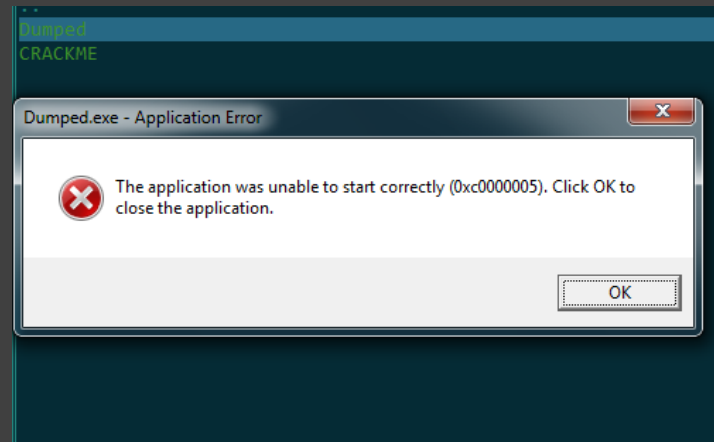
00401000	6A 00		push 0	
00401002	E8 FF 04 00 00		call <crackme.GetModuleHandleA>	
00401007	A3 CA 20 40 00		mov dword ptr ds:[4020CA],eax	
0040100C	6A 00		push 0	
0040100E	68 F4 20 40 00		push crackme.4020F4	
00401013	E8 A6 04 00 00		call <crackme.FindWindowA>	
00401018	0B C0		or eax,eax	
0040101A	^ 74 01		je crackme.40101D	
0040101C	C3		ret	
0040101D	C7 05 64 20 40 00 03		mov dword ptr ds:[402064],4003	
00401027	C7 05 68 20 40 00 28		mov dword ptr ds:[402068],<crackme.WndProc>	
00401031	C7 05 6C 20 40 00 00		mov dword ptr ds:[40206C],0	
00401038	C7 05 70 20 40 00 00		mov dword ptr ds:[402070],0	
00401045	A1 CA 20 40 00		mov eax,dword ptr ds:[4020CA]	
0040104A	A3 74 20 40 00		mov dword ptr ds:[402074],eax	
0040104F	^ 73 14 50 40 00		mov eax,qword ptr ds:[405014],eax	
0040104E	^ 77 C9 50 40 00		mov eax,qword ptr ds:[4050C9],eax	
00401053	^ C1 02 10 50 40 00		mov eax,qword ptr ds:[405050],eax	

4020F4:"No need to disasm the code!"

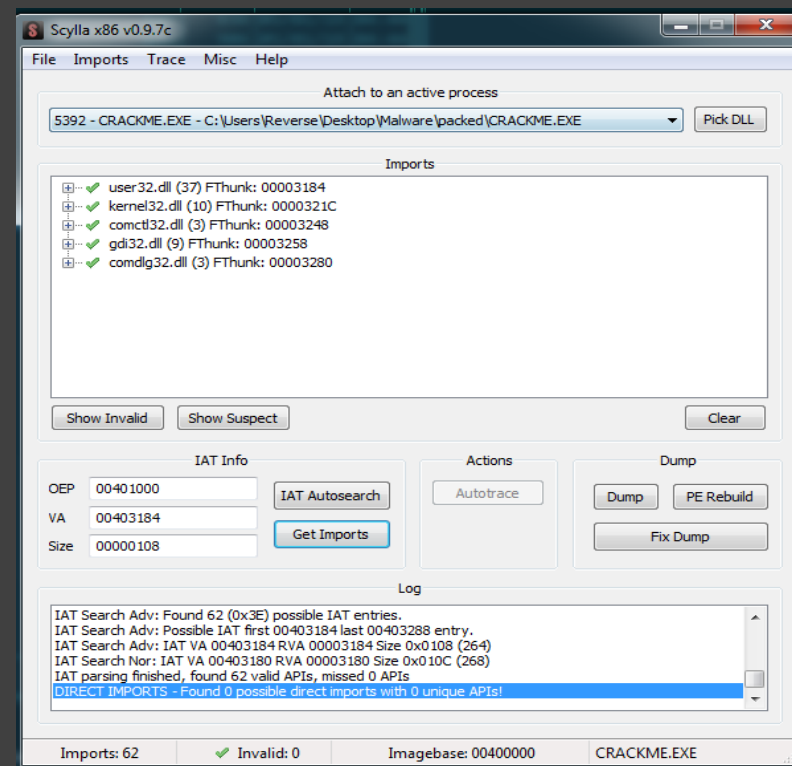
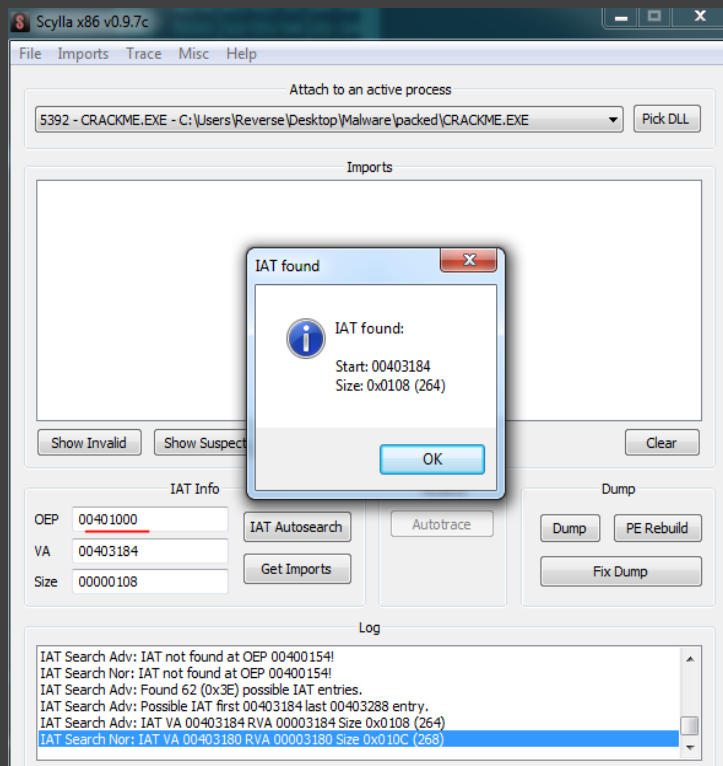
1. Находим наш процесс в списке
2. ПКМ → Dump Fill...



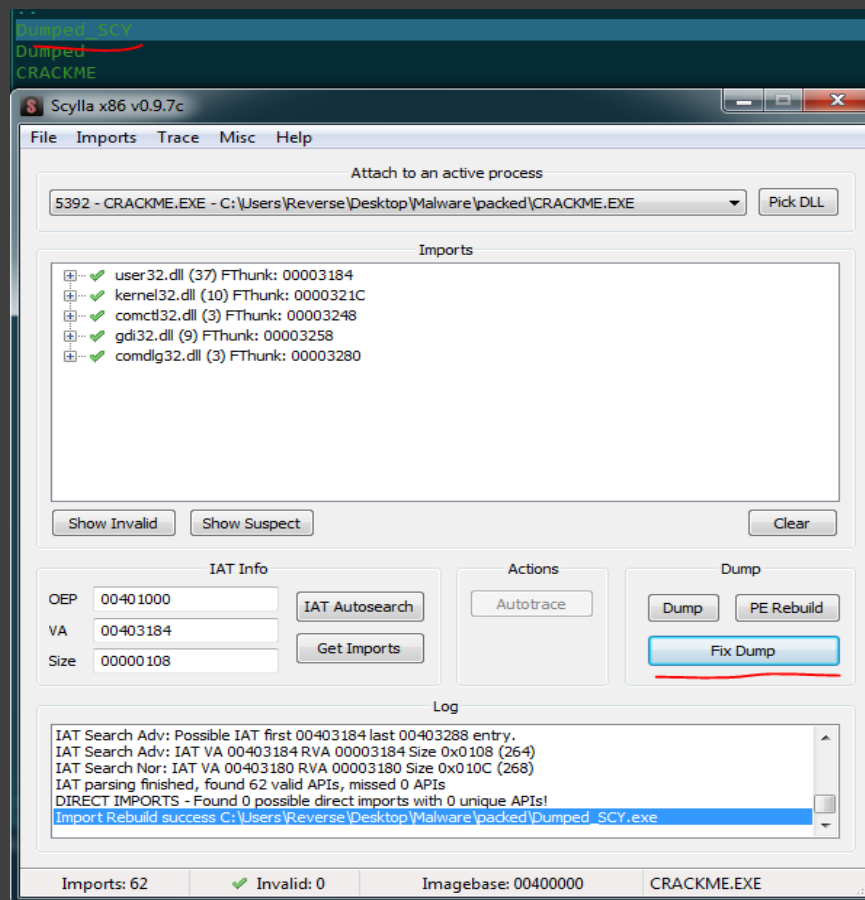
Сдампленный PE файл не отработает



1. Выбираем наш процесс (он всё ещё под отладкой)
2. В OEP выставляем наш адрес (0x401000)
3. Жмём IAT AutoSearch
4. Жмём Get Imports



1. Жмём Fix Dump
2. Выбираем наш дамп









## Автоматический дамп и восстановление IAT

Pd32.exe –pid xxxx

```

CRACKME_EXE_PID1510_ADVAPI32.dll_77B70000_x86      dll 659456
CRACKME_EXE_PID1510_ntdll.dll_779E0000_x86      dll 1268 K
CRACKME_EXE_PID1510_USER32.dll_77910000_x86      dll 831488
CRACKME_EXE_PID1510_SHELL32.dll_76CC0000_x86      dll 12 M
CRACKME_EXE_PID1510_USP10.dll_76A20000_x86      dll 647168
CRACKME_EXE_PID1510_GDI32.dll_769D0000_x86      dll 323584
CRACKME_EXE_PID1510_msvcrt.dll_76920000_x86      dll 716800
CRACKME_EXE_PID1510_COMDLG32.dll_76810000_x86      dll 507904
CRACKME_EXE_PID1510_LPK.dll_76800000_x86      dll 45056
CRACKME_EXE_PID1510_sechost.dll_767E0000_x86      dll 106496
CRACKME_EXE_PID1510_SHLWAPI.dll_76780000_x86      dll 360448
CRACKME_EXE_PID1510_RPCRT4.dll_766D0000_x86      dll 688128
CRACKME_EXE_PID1510_MSCTF.dll_76600000_x86      dll 839680
CRACKME_EXE_PID1510_kernel32.dll_76380000_x86      dll 888832
CRACKME_EXE_PID1510_IMM32.DLL_76260000_x86      dll 131072
CRACKME_EXE_PID1510_KERNELBASE.dll_75D50000_x86      dll 307200
CRACKME_EXE_PID1510_COMCTL32.DLL_71FD0000_x86      dll 544768
CRACKME_EXE_PID1510_CRACKME.EXE_400000_x86      exe 49152
pd32.exe 146944
    
```

Name	PID	Verified signer	CPU	File name
chrome.exe	2736	Google LLC		C:\Program Files\Google\...chrom
CRACKME.EXE	5392			C:\Users\Reverse\Des...CRACKM

```

CPU Usage: 10.85% Physical memory: 1.6 GB (53.32%) Processes: 85
pd32.exe -pid 5392
    
```

## Автоматический дамп и восстановление IAT

The screenshot shows a debugger window with the following components:

- Registers:**
  - eax: 0x39
  - ecx: 0xbffff4a0
  - edx: 0x100
  - ebx: 0xb7ffeff4
  - esp: 0xbffff528
  - ebp: 0xbffff548
- Locals:**
  - SPLIT-CODE.COM
  - reverse engineering tools
- Main Text Area:**

Process Dump: Dump memory modules to disk  
by geoff mcdonald

Process Dump is a Windows reverse-engineering tool to dump malware memory components back to disk for analysis. It uses an aggressive import reconstruction approach to make analysis easier, and supports 32 and 64 bit modules. Dumping of regions without PE headers is supported and in these cases PE headers and import tables will automatically be generated. Process Dump supports creation and use of a clean-hash database, so that dumping of clean files such as kernel32.dll can be skipped.

Process Dump comes in .zip format and supports Windows x86 and x64:

  - [Download: pd.exe v2.1 for Windows 32 and 64 bit](#)

This tool depends on Microsoft Visual C++ 2015 Redistributable:

  - [Microsoft Visual C++ 2015 Redistributable Package](#)

Source Code

The source code for Process Dump is available through GitHub. Contributions are welcome:

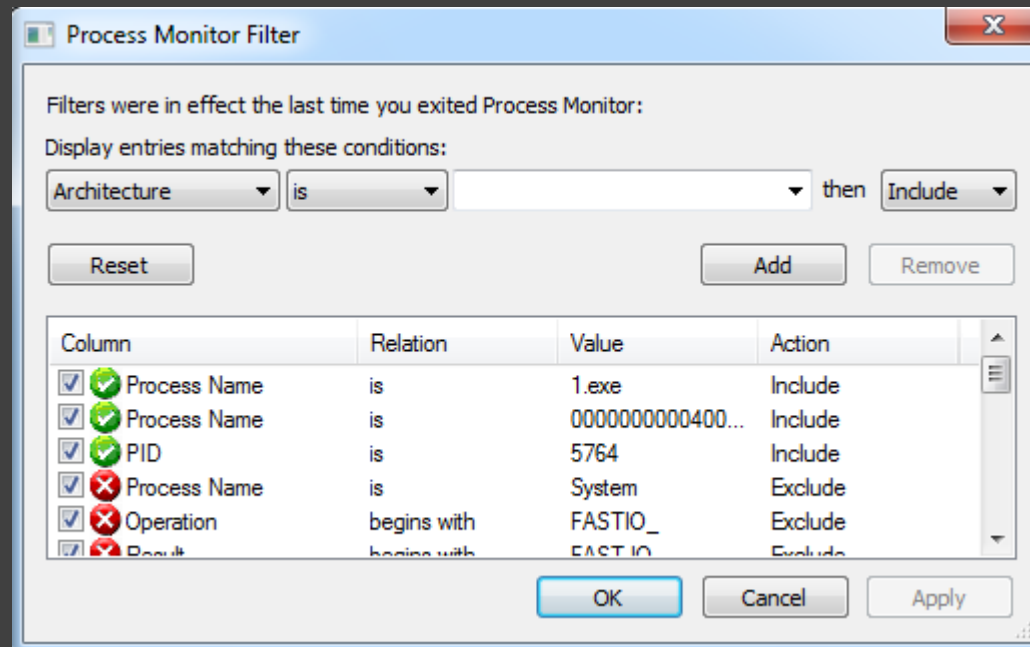
  - <https://github.com/glmcdona/Process-Dump>

At the bottom of the window, there is a URL: <http://split-code.com/processdump.html>

2

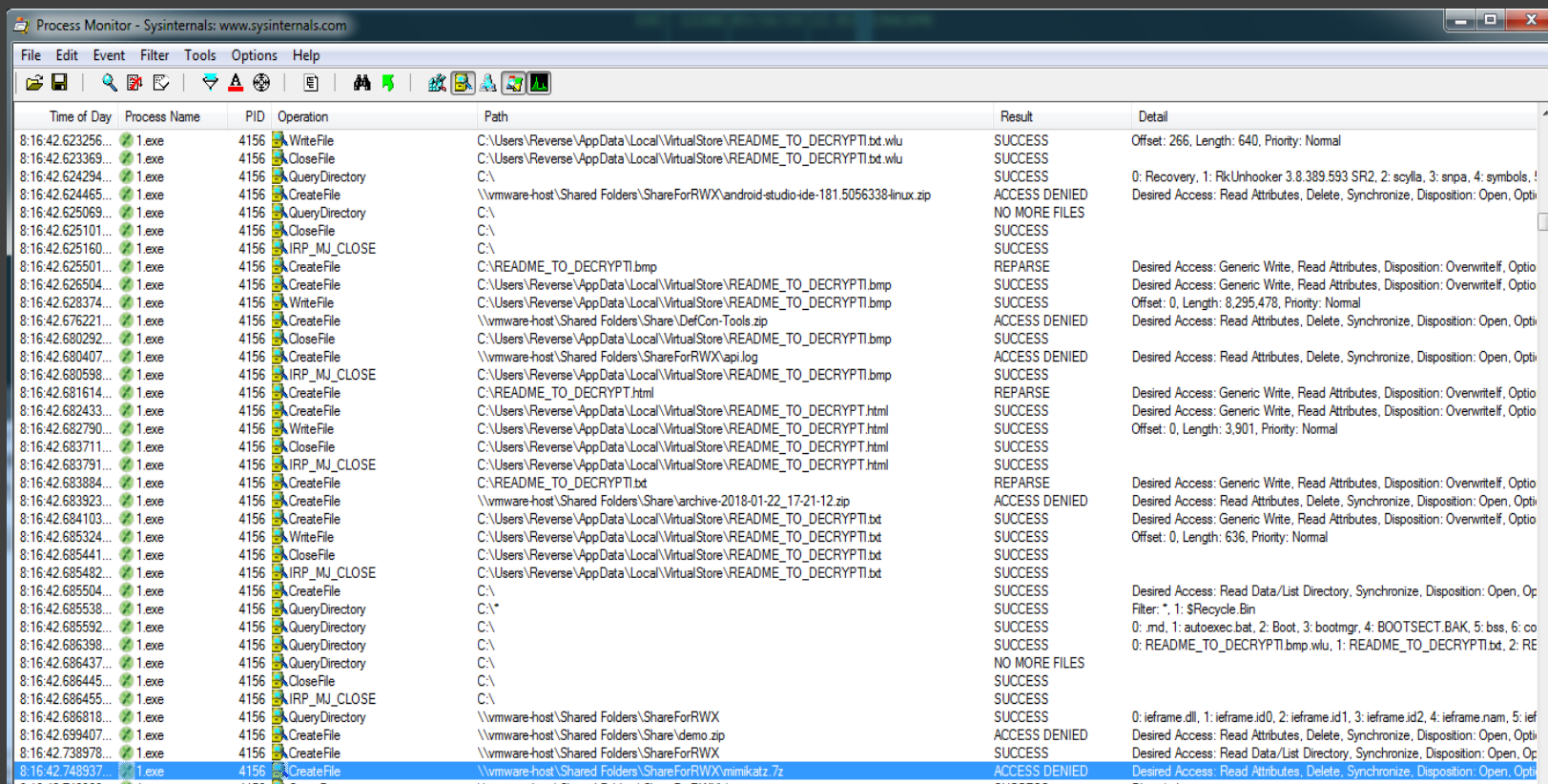
**ProcMon**

1. Запускаем ProcMon
2. Выставляем нужные фильтры (Ctrl + L)



# Задача – определить активность программы

Можно отфильтровать вывод по категориям событий: реестр, доступ к файлам, сетевая активность и тд



Time of Day	Process Name	PID	Operation	Path	Result	Detail
8:16:42.623256...	1.exe	4156	WriteFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bt.wlu	SUCCESS	Offset: 266, Length: 640, Priority: Normal
8:16:42.623369...	1.exe	4156	CloseFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bt.wlu	SUCCESS	
8:16:42.624294...	1.exe	4156	QueryDirectory	C:\	SUCCESS	
8:16:42.624465...	1.exe	4156	CreateFile	\\vmware-host\Shared Folders\ShareForRWX\android-studio-ide-181.5056338-linux.zip	ACCESS DENIED	0: Recovery, 1: RkUnhooker 3.8.389.593 SR2, 2: scylla, 3: snpa, 4: symbols, 5: ...
8:16:42.625069...	1.exe	4156	QueryDirectory	C:\	NO MORE FILES	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Opti...
8:16:42.625101...	1.exe	4156	CloseFile	C:\	SUCCESS	
8:16:42.625160...	1.exe	4156	IRP_MJ_CLOSE	C:\	SUCCESS	
8:16:42.625501...	1.exe	4156	CreateFile	C:\README_TO_DECRYPTI.bmp	REPARSE	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Optio...
8:16:42.626504...	1.exe	4156	CreateFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bmp	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Optio...
8:16:42.628374...	1.exe	4156	WriteFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bmp	SUCCESS	Offset: 0, Length: 8,295,478, Priority: Normal
8:16:42.676221...	1.exe	4156	CreateFile	\\vmware-host\Shared Folders\Share\DefCon-Tools.zip	ACCESS DENIED	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Opti...
8:16:42.680292...	1.exe	4156	CloseFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bmp	SUCCESS	
8:16:42.680407...	1.exe	4156	CreateFile	\\vmware-host\Shared Folders\ShareForRWX\api.log	ACCESS DENIED	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Opti...
8:16:42.680598...	1.exe	4156	IRP_MJ_CLOSE	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bmp	SUCCESS	
8:16:42.681614...	1.exe	4156	CreateFile	C:\README_TO_DECRYPTI.html	REPARSE	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Optio...
8:16:42.682433...	1.exe	4156	CreateFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.html	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Optio...
8:16:42.682790...	1.exe	4156	WriteFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.html	SUCCESS	Offset: 0, Length: 3,901, Priority: Normal
8:16:42.683711...	1.exe	4156	CloseFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.html	SUCCESS	
8:16:42.683791...	1.exe	4156	IRP_MJ_CLOSE	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.html	SUCCESS	
8:16:42.683884...	1.exe	4156	CreateFile	C:\README_TO_DECRYPTI.bt	REPARSE	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Optio...
8:16:42.683923...	1.exe	4156	CreateFile	\\vmware-host\Shared Folders\Share\archive-2018-01-22_17-21-12.zip	ACCESS DENIED	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Opti...
8:16:42.684103...	1.exe	4156	CreateFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bt	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Optio...
8:16:42.685324...	1.exe	4156	WriteFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bt	SUCCESS	Offset: 0, Length: 636, Priority: Normal
8:16:42.685441...	1.exe	4156	CloseFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bt	SUCCESS	
8:16:42.685482...	1.exe	4156	IRP_MJ_CLOSE	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bt	SUCCESS	
8:16:42.685504...	1.exe	4156	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Op...
8:16:42.685538...	1.exe	4156	QueryDirectory	C:\*	SUCCESS	Filter: *, 1: \$Recycle Bin
8:16:42.685592...	1.exe	4156	QueryDirectory	C:\	SUCCESS	0: .md, 1: autoexec.bat, 2: Boot, 3: bootmgr, 4: BOOTSECT.BAK, 5: bs, 6: co...
8:16:42.686398...	1.exe	4156	QueryDirectory	C:\	SUCCESS	0: README_TO_DECRYPTI.bmp.wlu, 1: README_TO_DECRYPTI.bt, 2: RE...
8:16:42.686437...	1.exe	4156	QueryDirectory	C:\	NO MORE FILES	
8:16:42.686445...	1.exe	4156	CloseFile	C:\	SUCCESS	
8:16:42.686455...	1.exe	4156	IRP_MJ_CLOSE	C:\	SUCCESS	
8:16:42.686818...	1.exe	4156	QueryDirectory	\\vmware-host\Shared Folders\ShareForRWX	SUCCESS	0: ieframe.dll, 1: ieframe.id0, 2: ieframe.id1, 3: ieframe.id2, 4: ieframe.nam, 5: ief...
8:16:42.699407...	1.exe	4156	CreateFile	\\vmware-host\Shared Folders\Share\demo.zip	ACCESS DENIED	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Opti...
8:16:42.738978...	1.exe	4156	CreateFile	\\vmware-host\Shared Folders\ShareForRWX	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Op...
8:16:42.748937...	1.exe	4156	CreateFile	\\vmware-host\Shared Folders\ShareForRWX\mmikatz.7z	ACCESS DENIED	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Opti...

Как найти место в PE файле, где вызвалась нужная функция, например, `CreateFile`?

8:16:42.625501...	1.exe	4156	CreateFile	C:\README_TO_DECRYPT1.bmp	REPARSE
8:16:42.626504...	1.exe	4156	CreateFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPT1.bmp	SUCCESS
8:16:42.628374...	1.exe	4156	WriteFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPT1.bmp	SUCCESS

1. Жмём Enter по интересующему событию
2. Переходим на вкладку Stack

# Определение места вызова функций в коде

Как найти место в PE файле, где вызвалась нужная функция, например, CreateFile?

Event Properties

Event | Process | Stack

Frame	Module	Location	Address	Path
K 0	FLTMGR.SYS	FltRequestOperationStatusCallback + 0xeb5	0x8bd27aeb	C:\Windows\system32\DRIVERS\FLTMGR.SYS
K 1	FLTMGR.SYS	FltGetIrpName + 0xc5c	0x8bd2a9f0	C:\Windows\system32\DRIVERS\FLTMGR.SYS
K 2	FLTMGR.SYS	FltProcessFileLock + 0x18b2	0x8bd3e1fe	C:\Windows\system32\DRIVERS\FLTMGR.SYS
K 3	FLTMGR.SYS	FltProcessFileLock + 0x1f6b	0x8bd3e8b7	C:\Windows\system32\DRIVERS\FLTMGR.SYS
K 4	ntkmlpa.exe	IoCallDriver + 0x64	0x82a8d593	C:\Windows\system32\ntkmlpa.exe
K 5	ntkmlpa.exe	NtClose + 0xf2f	0x82c9d2a9	C:\Windows\system32\ntkmlpa.exe
K 6	ntkmlpa.exe	ObCreateObject + 0x8c4	0x82c7cac5	C:\Windows\system32\ntkmlpa.exe
K 7	ntkmlpa.exe	ObOpenObjectByName + 0x165	0x82c8ced6	C:\Windows\system32\ntkmlpa.exe
K 8	ntkmlpa.exe	NtAllocateVirtualMemory + 0x1f52	0x82c839b4	C:\Windows\system32\ntkmlpa.exe
K 9	ntkmlpa.exe	NtCreateFile + 0x34	0x82ca7218	C:\Windows\system32\ntkmlpa.exe
K 10	ntkmlpa.exe	ZwYieldExecution + 0xb56	0x82a941ea	C:\Windows\system32\ntkmlpa.exe
U 11	ntdll.dll	NtCreateFile + 0xc	0x77a255d4	C:\Windows\System32\ntdll.dll
U 12	KernelBase.dll	CreateFileW + 0x1d1	0x75d5aa21	C:\Windows\System32\KernelBase.dll
U 13	kernel32.dll	CreateFileW + 0x4a	0x763cca0	C:\Windows\System32\kernel32.dll
U 14	1.exe	1.exe + 0x5504	0x405504	C:\Users\Reverse\Desktop\Malware\jaff\1.exe
U 15	kernel32.dll	BaseThreadInitThunk + 0x12	0x763d3c45	C:\Windows\System32\kernel32.dll
U 16	ntdll.dll	RtlInitializeExceptionChain + 0xef	0x77a437f5	C:\Windows\System32\ntdll.dll
U 17	ntdll.dll	RtlInitializeExceptionChain + 0xc2	0x77a437c8	C:\Windows\System32\ntdll.dll



3

**Fiddler/WireShark**



## Remcos RAT traffic

2017-10-27-Remcos-RAT-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.27.101	185.145.45.131	TCP	66	50439 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=14...
2	0.180358	185.145.45.131	10.10.27.101	TCP	66	2404 → 50439 [SYN, ACK] Seq=0 Ack=1 Win=8192 L...
3	0.180464	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [ACK] Seq=1 Ack=1 Win=66560 Len=0
4	0.182342	10.10.27.101	185.145.45.131	104asdu	596	<ERR prefix 254 bytes> <- I (12801,20257) ASDU=...
5	0.418778	185.145.45.131	10.10.27.101	104apci	86	2404 → 50439 [PSH, ACK] Seq=1 Ack=543 Win=1715...
6	0.420711	10.10.27.101	185.145.45.131	104apci	216	<ERR prefix 84 bytes> <- I (14914,12718) ASDU=...
7	0.938212	185.145.45.131	10.10.27.101	TCP	60	2404 → 50439 [ACK] Seq=33 Ack=705 Win=16896 Le...
8	9.669297	185.145.45.131	10.10.27.101	104apci	86	2404 → 50439 [PSH, ACK] Seq=33 Ack=705 Win=168...
9	9.671591	10.10.27.101	185.145.45.131	104asdu	216	<ERR prefix 84 bytes> <- I (14914,12718) ASDU=...
10	10.069290	185.145.45.131	10.10.27.101	TCP	60	2404 → 50439 [ACK] Seq=65 Ack=867 Win=16896 Le...
11	29.658417	185.145.45.131	10.10.27.101	104apci	86	2404 → 50439 [PSH, ACK] Seq=65 Ack=867 Win=168...
12	29.661530	10.10.27.101	185.145.45.131	104asdu	216	<ERR prefix 84 bytes> <- I (14914,12718) ASDU=...

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 > Ethernet II, Src: HewlettP\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear\_b6:93:f1 (20:e5:2a:b6:93:f1)  
 > Internet Protocol Version 4, Src: 10.10.27.101, Dst: 185.145.45.131  
 > Transmission Control Protocol, Src Port: 50439, Dst Port: 2404, Seq: 0, Len: 0

```

0000  20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00  .*.....G...E.
0010  00 34 00 ab 40 00 80 06 ed 95 0a 0a 1b 65 b9 91  .4.@.....e.
0020  2d 83 c5 07 09 64 e5 e8 83 85 00 00 00 80 02  ....d...
0030  20 00 0a b3 00 00 02 04 05 b4 01 03 03 08 01 01  .....
0040  04 02  ..
    
```

2017-10-27-Remcos-RAT-traffic.pcap | Packets: 47 · Displayed: 47 (100.0%) | Profile: Default



## Общение с СС

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2017-10-27-Remcos-RAT-traffic.pcap

```
00000180 8d 01 c7 8d 7d b4 29 35 c6 dc a1 c4 e4 48 82 82 ...}.)5 ....H..
00000190 53 f2 57 8c 3f c4 cc 4f 10 00 c6 d7 3f 3f 67 4e S.W.?.0 ....?gN
000001A0 80 52 75 53 d0 7c 19 af 0a 32 93 a2 c2 30 7e ce .RuS.|... .2...0~.
000001B0 d3 57 4c cd f7 bf fb ab ef b3 51 66 9f af 5a c7 .WL..... ..Qf..Z.
000001C0 da aa 74 09 be 17 9d c0 46 2f 71 e2 99 d8 b7 0f .t..... F/q.....
000001D0 bb 46 cc 6f c8 2b 5f d4 d3 49 4b 17 c4 47 e4 b8 .F.o+_ .IK..G..
000001E0 f6 5c 81 25 a8 de fb 09 70 e5 b9 de 5a f7 72 4d .\%.... p...Z.rM
000001F0 bc 9f 08 2f 9e 8f 0f db a9 71 cc b3 c7 fd fc 95 .\./..... q.....
00000200 52 c1 ad 24 84 31 b5 0b d4 7a 2b d5 0e 2e 99 af R..$.1.. .z+....
00000210 b2 a7 b6 8f 7f 70 4a 62 55 02 79 db cb 51 .....p3b U.y..Q
00000220 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 be 8d da b1 ec ....]... .0.....
00000230 c5 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 98 36 ....3...; ...7..6
00000240 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 3c 8d da b1 ec ....]... .0.<....
00000250 c3 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 e7 06 ...3...; ...7...
00000260 b2 8c f0 0a 7f 01 c0 01 45 1c c2 7a 14 4f 74 cf ..... E..z.Ot.
00000270 57 b0 58 25 56 1d 0a 26 77 7f 19 c1 fd cc a3 2a W.X%V..& w.....*
00000280 94 14 be 5d ca 39 d1 ee eb 10 8d 10 33 34 d4 46 ...].9.. ....34.F
00000290 a2 84 02 03 68 3d 84 74 5d 63 21 7a 83 81 70 04 ...h=t ]clz..p.
00000300 06 2d be 32 3e 81 1c 34 45 e8 d1 aa 31 02 0c 1a -->..4 E...1..
00000310 b0 da 3e 8d b1 65 02 9a 1d 9a 7c 50 a0 5c da 62 -->..e.. ..|P.\.b
00000320 69 44 9c 61 d1 b1 a2 2a 71 7c 10 1d 24 5f 40 1b ID.a...* q|..$.@.
00000330 45 49 68 85 1d 6c 0c 61 9b eb 20 23 97 b5 8f 68 Eih..l.a .. #...h
00000340 64 96 d.
00000350 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 be 8d da b1 ec ....]... .0.....
00000360 c5 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 98 36 ....3...; ...7..6
00000370 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 3c 8d da b1 ec ....]... .0.<....
00000380 c3 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 e7 06 ...3...; ...7...
00000390 b2 8c f0 0a 7f 01 c0 01 45 1c c2 7a 14 4f 74 cf ..... E..z.Ot.
00000400 57 b0 58 25 56 1d 0a 26 77 7f 19 c1 fd cc a3 2a W.X%V..& w.....*
00000410 94 14 be 5d ca 39 d1 ee eb 10 8d 10 33 34 d4 46 ...].9.. ....34.F
00000420 a2 84 02 03 68 3d 84 74 5d 63 21 7a 83 81 70 04 ...h=t ]clz..p.
00000430 06 2d be 32 3e 81 1c 34 45 e8 d1 aa 31 02 0c 1a -->..4 E...1..
00000440 b0 da 3e 8d b1 65 02 9a 1d 9a 7c 50 a0 5c da 62 -->..e.. ..|P.\.b
00000450 69 44 9c 61 d1 b1 a2 2a 71 7c 10 1d 24 5f 40 1b ID.a...* q|..$.@.
00000460 45 49 6a 83 1f 6e 0c 61 9b eb 20 23 97 b4 80 6a EIj..n.a .. #...j
00000470 61 90 a.
00000480 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 be 8d da b1 ec ....]... .0.....
00000490 c5 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 98 36 ....3...; ...7..6
00000500 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 3c 8d da b1 ec ....]... .0.<....
00000510 c3 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 e7 06 ...3...; ...7...
00000520 b2 8c f0 0a 7f 01 c0 01 45 1c c2 7a 14 4f 74 cf ..... E..z.Ot.
00000530 57 b0 58 25 56 1d 0a 26 77 7f 19 c1 fd cc a3 2a W.X%V..& w.....*
00000540 94 14 be 5d ca 39 d1 ee eb 10 8d 10 33 34 d4 46 ...].9.. ....34.F
```

15 client pkt(s), 14 server pkt(s), 28 turn(s).

Entire conversation (2826 bytes) Show and save data as Hex Dump Stream 0

Find:

Находим интересный нам параметр → ПКМ Apply as Filter

The screenshot shows the Wireshark interface with a packet list on the left and a detailed view on the right. A context menu is open over the packet list, and a sub-menu is open over the 'Apply as Filter' option.

No.	Time	Source	Destination	Protocol	Length	Info
9	9.671591	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
12	29.661530	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
15	49.760630	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
18	69.730428	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
21	89.780764	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
24	109.970912	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
27	130.041301	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
30	150.010861	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
33	170.200288	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
36	190.170170	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
39	210.319899	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
42	230.349741	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
45	250.469869	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0
47	261.369061	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [PSH, ACK] Seq=10850439, Win=0, Len=0

The detailed view shows the following information:

- Ethernet II, Src: Hewlett-Packard (08:00:27:00:00:00), Dst: Hewlett-Packard (08:00:27:00:00:00)
- Internet Protocol Version 4, Src: 10.10.27.101, Dst: 185.145.45.131
- TCP, Src Port: 50439, Dst Port: 2404, Seq: 10850439, Win: 0, Len: 0

Фильтры по протоколам

Фильтры по портам

2017-10-27-Remcos-RAT-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.10.27.101

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.27.101	185.145.45.131	TCP	66	50439 → 2404 [SYN] Seq=0 Win=8192
3	0.180464	10.10.27.101	185.145.45.131	TCP	54	50439 → 2404 [ACK] Seq=1 Ack=1 Wi
4	0.182342	10.10.27.101	185.145.45.131	104asdu	596	<ERR prefix 254 bytes> <- I (1280
6	0.420711	10.10.27.101	185.145.45.131	104apci	216	<ERR prefix 84 bytes> <- I (14914
9	9.671591	10.10.27.101	185.145.45.131	104asdu	216	<ERR prefix 84 bytes> <- I (14914
12	29.661530	10.10.27.101	185.145.45.131	104asdu	216	<ERR prefix 84 bytes> <- I (14914
15	10.768630	10.10.27.101	185.145.45.131	104asdu	216	<ERR prefix 84 bytes> <- I (14914

Фильтры по протоколам

Фильтры по портам

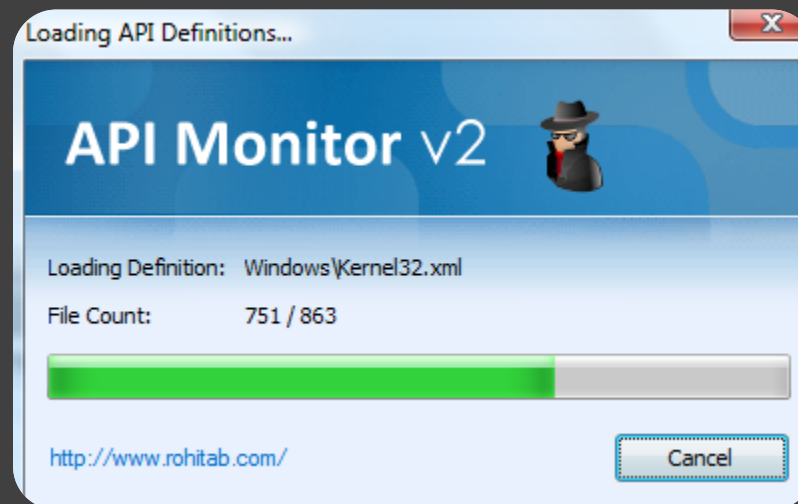
Фильтр	Описание
ip.src	ip отправителя
ip.dst	ip получателя
ip.addr	ip отправителя или получателя
http   dns	Показать только http и dns
http contains <b>user-agent</b>	Поиск « <b>user-agent</b> »

Оператор	Описание
eq, ==	Равно
ne, !=	Не равно
gt, >	Больше, чем
lt, <	Меньше, чем
ge, >=	Больше, либо равно
le, <=	Меньше, либо равно

4

**API monitor**

Позволяет проследить, какие функции вызываются программой с возможностью просмотра параметров



<http://www.rohitab.com/apimonitor>

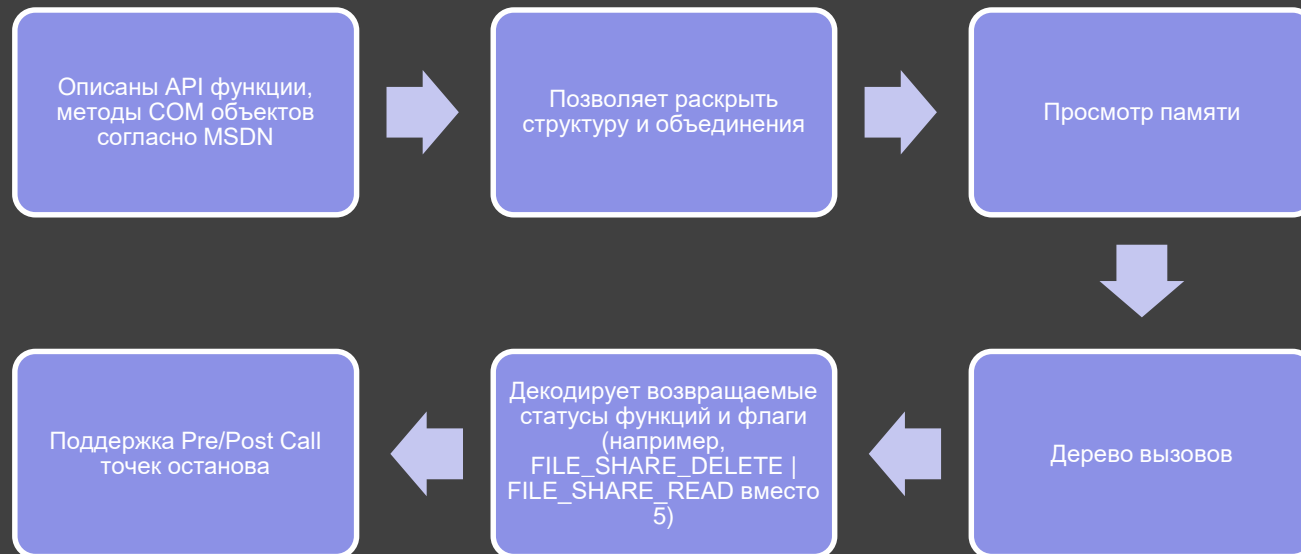
Позволяет проследить, какие функции вызываются программой с возможностью просмотра параметров

The screenshot displays the API Monitor v2 (Alpha-r6) 32-bit interface. The main window shows a list of API calls with columns for PID, TID, Module, API, Return, and Error. A call to `NtCreateFile` is highlighted, and a tooltip shows its parameters: `FileHandle`, `DesiredAccess`, `ObjectAttributes`, `Length`, `RootDirectory`, and `ObjectName`. The `ObjectAttributes` parameter is expanded to show its fields: `Length`, `RootDirectory`, `ObjectAttributes`, `ObjectAttributes`, `Length`, `RootDirectory`, and `ObjectAttributes`. The `ObjectAttributes` field is further expanded to show its fields: `Length`, `RootDirectory`, `ObjectAttributes`, `ObjectAttributes`, `Length`, `RootDirectory`, and `ObjectAttributes`. The `ObjectAttributes` field is further expanded to show its fields: `Length`, `RootDirectory`, `ObjectAttributes`, `ObjectAttributes`, `Length`, `RootDirectory`, and `ObjectAttributes`. The `ObjectAttributes` field is further expanded to show its fields: `Length`, `RootDirectory`, `ObjectAttributes`, `ObjectAttributes`, `Length`, `RootDirectory`, and `ObjectAttributes`.

#	Type	Name	Pre-Call Value	Post-Call Value
1	PHANDLE	FileHandle	0x0030f1b = NULL	0x0030f1b = NULL
2	ACCESS_MASK	DesiredAccess	GENERIC_WRITE   SYNCHRONIZE   128	GENERIC_WRITE   SYNCHRONIZE   128
3	OBJECT_ATTRIBUTES	ObjectAttributes	0x0030f19c	0x0030f19c
	OBJECT_ATTRIBUTES	ObjectAttributes	(Length = 24, RootDirectory = NULL, ObjectName = ...)	(Length = 24, RootDirectory = NULL, ObjectName = ...)
	ULONG	Length	24	24
	HANDLE	RootDirectory	NULL	NULL
	PUNICODE_STRING	ObjectName	0x0030f1d8	0x0030f1d8
	UNICODE_STRING	ObjectName	(Length = 60, MaximumLength = 538, Buffer = 0x...)	(Length = 60, MaximumLength = 538, Buffer = 0x...)
	USHORT	Length	60	60

The interface also shows a list of running processes on the left, including `MSOSYNC.EXE`, `ONENOTEM.EXE`, `OUTLOOK.EXE`, `SearchProtocolHost.exe`, `SecureCRT.exe`, `Skype.exe`, `skypePM.exe`, `Snagit32.exe`, and `SnagitEditor.exe`. The bottom status bar shows the system is ready, with 24.22 MB of memory used and the mode set to Standard.

## Возможности инструмента



5

**SandBox**

# Это система для автоматического исследования вредоносного ПО




## Страница из отчёта



Cuckoo Sandbox - Mozilla Firefox

Cuckoo Sandbox

file:///home/devil/Documents/cuckoo/storage/analyses/70/reports/report.html



Info File Signatures Screenshots Static Dropped Network Behavior

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2013-06-14 14:30:50	2013-06-14 14:31:19	29 seconds	0.6

File Details

File name	Trojan-GameThief.Win32.OnLineGames.ajnsq
File size	154624 bytes
File type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
CRC32	CCA89E8F
MD5	e78539cf73520b6358380a589464472a
SHA1	43a98b861b94355ca5805f956a684f4aa9f78c3b
SHA256	d7729ca84845bb0fec43a93ffa57cfe4cf1fcd9b3719eb7eebeea894308484e0
SHA512	dd19acc613452af7b762516b2ebafdf2b3e8368626f24cb879b1cc937d413164c1c249513e7ccc6892ba70891b1068461c9715b4c99bd1878901c30ffd983b3c
Ssdeep	1536:vIsIwXI2IuIJkuvfZ/AuwtICVmG04D60FcK5vcZ5FCt\lURZwZxUSTP:y7ZFNyxfGx04iK5vyZox

Online системы:

[malwr.com](http://malwr.com)

[cuckoo.cert.ee](http://cuckoo.cert.ee)

[hybrid-analysis.com](http://hybrid-analysis.com)



O T U S

Вопросы???





Пакулов Артур

[A.Pakulov.Otus@Gmail.com](mailto:A.Pakulov.Otus@Gmail.com)

Спасибо  
за внимание!

