

A decorative graphic on the left side of the slide consisting of overlapping geometric shapes. It includes a blue parallelogram, a light green parallelogram, and a dark grey parallelogram, all with black outlines, set against a dark blue background.

# Linux ELF Obfuscation



Митьо, за ELF-чета  
не сме говорили!

Намокрих  
пурата!

Давай python-я!!!

Къде  
попаднах!





# Как работи.

lspec\_objdump (home/sergi/PycharmProjects/Interrimintin)

```
lspeci: file format elf64-x86-64
lspeci
architecture: i386:x86-64, flags 0x00000150:
HAS_SYMS, DYNAMIC, D_PAGED
start address 0x000000000002b70
```

Опаа!

```
Program Header:
PHDR off 0x0000000000000040 vaddr 0x0000000000000040 paddr 0x0000000000000040 align 2**3
      filesz 0x00000000000002d8 memsz 0x00000000000002d8 flags r--
INTERP off 0x0000000000000318 vaddr 0x0000000000000318 paddr 0x0000000000000318 align 2**0
      filesz 0x000000000000001c memsz 0x000000000000001c flags r--
LOAD off 0x0000000000000000 vaddr 0x0000000000000000 paddr 0x0000000000000000 align 2**12
      filesz 0x0000000000000d78 memsz 0x0000000000000d78 flags r--
LOAD off 0x0000000000000200 vaddr 0x0000000000000200 paddr 0x0000000000000200 align 2**12
      filesz 0x0000000000000c30 memsz 0x0000000000000c30 flags r-x
LOAD off 0x000000000000f000 vaddr 0x000000000000f000 paddr 0x000000000000f000 align 2**12
      filesz 0x0000000000005e98 memsz 0x0000000000005e98 flags r--
LOAD off 0x0000000000001580 vaddr 0x0000000000001580 paddr 0x0000000000001580 align 2**12
      filesz 0x0000000000000e28 memsz 0x0000000000000e28 flags rw-
DYNAMIC off 0x00000000000015bc0 vaddr 0x00000000000015bc0 paddr 0x00000000000015bc0 align 2**3
      filesz 0x0000000000000210 memsz 0x0000000000000210 flags rw-
NOTE off 0x0000000000000038 vaddr 0x0000000000000038 paddr 0x0000000000000038 align 2**3
      filesz 0x0000000000000020 memsz 0x0000000000000020 flags r--
NOTE off 0x0000000000000038 vaddr 0x0000000000000038 paddr 0x0000000000000038 align 2**2
      filesz 0x0000000000000044 memsz 0x0000000000000044 flags r--
0x6474e553 off 0x0000000000000038 vaddr 0x0000000000000038 paddr 0x0000000000000038 align 2**3
      filesz 0x0000000000000020 memsz 0x0000000000000020 flags r--
EH_FRAME off 0x0000000000001398 vaddr 0x0000000000001398 paddr 0x0000000000001398 align 2**2
      filesz 0x00000000000001e4 memsz 0x00000000000001e4 flags r--
STACK off 0x0000000000000000 vaddr 0x0000000000000000 paddr 0x0000000000000000 align 2**4
      filesz 0x0000000000000000 memsz 0x0000000000000000 flags rw-
RELRO off 0x0000000000001580 vaddr 0x0000000000001580 paddr 0x0000000000001580 align 2**0
      filesz 0x0000000000000070 memsz 0x0000000000000070 flags r--
```

```
Dynamic Section:
NEEDED liblpc1.so.3
NEEDED libkmod.so.2
NEEDED libc.so.6
INIT 0x0000000000000200
FINI 0x0000000000000e28
```

вълшебен код

копираш  
криптираш

lspec\_objdump (home/sergi/PycharmProjects/Interrimintin)

```
lspeci_MODED: file format elf64-x86-64
lspeci_MODED
architecture: i386:x86-64, flags 0x00000150:
HAS_SYMS, DYNAMIC, D_PAGED
start address 0x00000000000a6ca3
```

мажеш

криптираш

```
Program Header:
PHDR off 0x0000000000000040 vaddr 0x0000000000000040 paddr 0x0000000000000040 align 2**3
      filesz 0x00000000000002d8 memsz 0x00000000000002d8 flags r--
INTERP off 0x0000000000000318 vaddr 0x0000000000000318 paddr 0x0000000000000318 align 2**0
      filesz 0x000000000000001c memsz 0x000000000000001c flags r--
LOAD off 0x0000000000000000 vaddr 0x0000000000000000 paddr 0x0000000000000000 align 2**12
      filesz 0x0000000000000d78 memsz 0x0000000000000d78 flags r--
LOAD off 0x0000000000000300 vaddr 0x0000000000000300 paddr 0x0000000000000300 align 2**12
      filesz 0x0000000000000c30 memsz 0x0000000000000c30 flags r-x
LOAD off 0x000000000000f000 vaddr 0x000000000000f000 paddr 0x000000000000f000 align 2**12
      filesz 0x0000000000005e98 memsz 0x0000000000005e98 flags r--
LOAD off 0x0000000000001680 vaddr 0x0000000000001680 paddr 0x0000000000001680 align 2**12
      filesz 0x0000000000000e28 memsz 0x0000000000000e28 flags rw-
LOAD off 0x0000000000001800 vaddr 0x0000000000001800 paddr 0x0000000000001800 align 2**12
      filesz 0x0000000000000c30 memsz 0x0000000000000c30 flags r--
LOAD off 0x0000000000005000 vaddr 0x0000000000005000 paddr 0x0000000000005000 align 2**12
      filesz 0x0000000000000200 memsz 0x0000000000000200 flags rwx
LOAD off 0x0000000000002800 vaddr 0x0000000000002800 paddr 0x0000000000002800 align 2**12
      filesz 0x0000000000000070 memsz 0x0000000000000070 flags r--
DYNAMIC off 0x00000000000016bc0 vaddr 0x00000000000016bc0 paddr 0x00000000000016bc0 align 2**3
      filesz 0x00000000000001d0 memsz 0x00000000000001d0 flags rw-
NOTE off 0x0000000000002800 vaddr 0x0000000000002800 paddr 0x0000000000002800 align 2**3
      filesz 0x0000000000000064 memsz 0x0000000000000064 flags r--
0x6474e553 off 0x0000000000002800 vaddr 0x0000000000002800 paddr 0x0000000000002800 align 2**3
      filesz 0x0000000000000020 memsz 0x0000000000000020 flags r--
EH_FRAME off 0x0000000000001498 vaddr 0x0000000000001498 paddr 0x0000000000001498 align 2**2
      filesz 0x00000000000001e4 memsz 0x00000000000001e4 flags r--
STACK off 0x0000000000000000 vaddr 0x0000000000000000 paddr 0x0000000000000000 align 2**4
      filesz 0x0000000000000000 memsz 0x0000000000000000 flags rw-
RELRO off 0x0000000000001680 vaddr 0x0000000000001680 paddr 0x0000000000001680 align 2**0
      filesz 0x0000000000000070 memsz 0x0000000000000070 flags r--
```

```
Dynamic Section:
NEEDED liblpc1.so.3
```

# Как работи.

## Статични промени по файла.

- Копира и криптира ELF код сегмента
- Маже по оригиналния код сегмент.
- Криптира сегмента със стрингове
- Генерира вълшебна структура описваща промените
- Компилира вълшебният код
- Вмъква вълшебния код като нов RWX сегмент и пренасочва входната точка към него.

## Промени по време на изпълнение.

- маха всички правата на оригиналния код сегмент така ще получим 11 сигнал когато се скочи на него
- декриптира сегмента с текст
- инсталира функция за обработка на SIGSEGV
- скача на оригиналната входна точка
- на всеки сигнал 11 декриптира 1 страница от копието на оригиналния код сегмент и я копира на оригиналното и място.



79e7976d095453db21347d90d304efc42f7b77e7af2c4f7497d615d3fbd981f

Search, Upload, Grid, Alerts, Sign in, Sign up



39 security vendors and 1 sandbox flagged this file as malicious



79e7976d095453db21347d90d304efc42f7b77e7af2c4f7497d615d3fbd981f  
ZenZ.x86

103.45 KB  
Size

2023-02-07 06:59:39 UTC  
3 days ago



elf 64bits detect-debug-environment service-scan

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Linux/Gafgyt.Gen28	ALYac	Gen.Variant.Trojan.Linux.Gafgyt.5
Antiy-AVL	Trojan.Linux.Gafgyt.anw	Arcabit	Trojan.Linux.Linux.Gafgyt.5
Avast	ELF.DDoS-Y [Trj]	Avast-Mobile	ELF.DDoS-S [Trj]
AVG	ELF.DDoS-Y [Trj]	Avira (no cloud)	EXP/ELF.Mirai.Z.A
BitDefender	Gen.Variant.Trojan.Linux.Gafgyt.5	BitDefenderTheta	Gen.NU.Mirai.36252
ClamAV	Unix.Trojan.Tsunami-6981155-0	Cynet	Malicious (score: 99)
Cyren	E64/Mirai.BE.gen/Camelot	DnWeb	Linux.Siggen.9999
Elastic	Linux.Trojan.Gafgyt	Emsisoft	Gen.Variant.Trojan.Linux.Gafgyt.5 (B)
eScan	Gen.Variant.Trojan.Linux.Gafgyt.5	ESET-NOD32	A Variant Of Linux/Gafgyt.AHW
Fortinet	Linux/Redis.TSULtr	GData	Gen.Variant.Trojan.Linux.Gafgyt.5
Google	Detected	Ikarus	Trojan.Linux.Gafgyt
Jiangmin	Backdoor.Linux.ifbo	Kaspersky	HEUR.Backdoor.Linux.Gafgyt.bi
MAX	Malware (ai Score=88)	MaxSecure	Trojan.Malware.121218.susgen
McAfee	GenericRXUI-VAI58ADAF13BB89	McAfee-GW-Edition	GenericRXUI-VAI58ADAF13BB89
Microsoft	Backdoor.Linux/Gafgyt.AX1xp	Rising	Backdoor.Gafgyt/Linux1.D054 (CLASSIC)
Sangfor Engine Zero	Suspicious Linux.Save.a	SentinelOne (Static ML)	Static AI - Malicious ELF
Sophos	Linux/DDoS-BI	Symantec	Trojan.Gen.NPE
Tencent	Linux.Backdoor.Gafgyt.RqI	Trellix (FireEye)	Gen.Variant.Trojan.Linux.Gafgyt.5
TrendMicro	Backdoor.Linux.BASHLITE.SMJC3	TrendMicro-HouseCall	Backdoor.Linux.BASHLITE.SMJC3
VIPRE	Gen.Variant.Trojan.Linux.Gafgyt.5	Acronis (Static ML)	Undetected



8 / 62

8 security vendors and no sandboxes flagged this file as malicious

c9b49ccd6a35bc78d735d09687084695ce03572bd980a62b8361ddb6b1415efb  
ZenZx86\_MODIFIED  
elf 64bits

1.28 MB  
Size

2023-02-10 13:08:30 UTC  
1 minute ago

ELF

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Linux/Gafgyt.Gen44	BitDefenderTheta	Gen:NR/Mirai.36276
ClamAV	Unix.Dropper.Mirai-7139232-0	Google	Detected
Gdinsoft (no cloud)	Suspicious.XOR_Encoded.botlyf	Kaspersky	HEUR:Backdoor.Linux.Gafgyt.bj
Sangfor Engine Zero	Suspicious.Linux.Save.a	ZoneAlarm by Check Point	HEUR:Backdoor.Linux.Gafgyt.bj
Acronis (Static ML)	Undetected	ALYac	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
CMC	Undetected	Cynet	Undetected
Cyren	Undetected	DrWeb	Undetected
Elastic	Undetected	Emsisoft	Undetected
eScan	Undetected	ESET-NOD32	Undetected
F-Secure	Undetected	Fortinet	Undetected
GData	Undetected	Ikarus	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
KTGW	Undetected	Kingsoft	Undetected
Lionic	Undetected	Malwarebytes	Undetected
MAX	Undetected	MaxSecure	Undetected
McAfee	Undetected	McAfee-GW-Edition	Undetected



# К'ъф е тоз вълшебен код?

```
a.out Makefile my_link.ld tintiri.c tintiri.h tintiri.o
serj@rocket:~/PycharmProjects/tintirimintiri/tintirimintiri$ objdump -x a.out

a.out:      file format elf64-x86-64
a.out
architecture: i386:x86-64, flags 0x00000112:
EXEC_P, HAS_SYMS, D_PAGED
start address 0x00000000babadca3

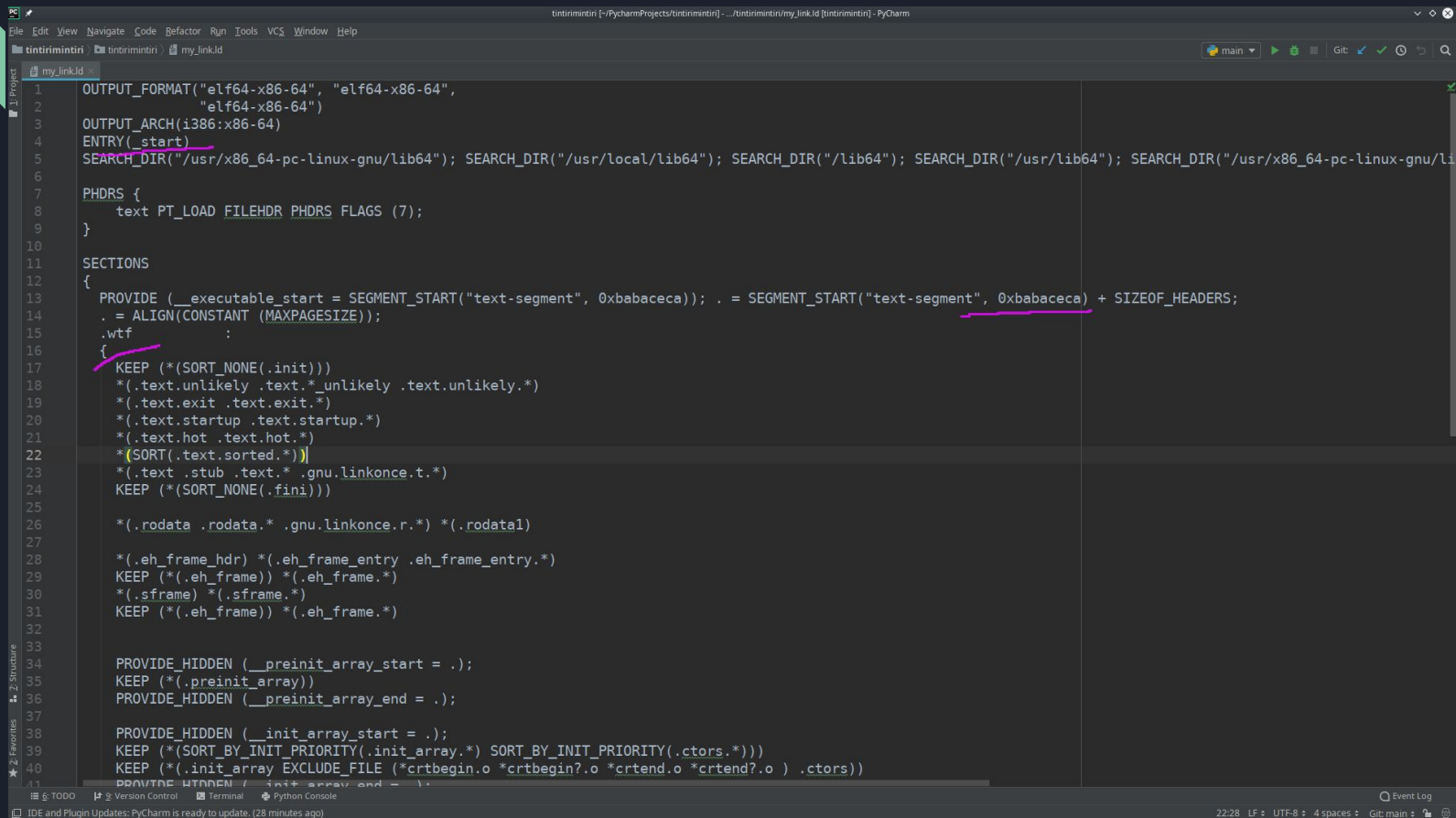
Program Header:
  LOAD off    0x0000000000000000 vaddr 0x00000000babac000 paddr 0x00000000babac000 align 2**12
    filesz 0x00000000000002cf8 memsz 0x00000000000002cf8 flags rwx

Sections:
Idx Name          Size      VMA           LMA           File off  Algn
 0 .wtf           00001cf8  00000000babad000 00000000babad000 00001000  2**5
                CONTENTS, ALLOC, LOAD, CODE, THREAD_LOCAL

SYMBOL TABLE:
0000000000000000 l    df *ABS* 0000000000000000 tintiri.c
0000000000000000 l    df *ABS* 0000000000000000 alloc.c
0000000000000000 l    df *ABS* 0000000000000000 errno_location.c
0000000000000000 l    df *ABS* 0000000000000000 sigaction.c
00000000babae070 l    df *ABS* 0000000000000000 __restore_rt
0000000000000000 l    df *ABS* 0000000000000000 sigfillset.c
0000000000000000 l    df *ABS* 0000000000000000 strncpy.c
0000000000000000 l    df *ABS* 0000000000000000 strtok_r.c
0000000000000000 l    df *ABS* 0000000000000000 strtoll.c
0000000000000000 l    df *ABS* 0000000000000000 strtoull.c
0000000000000000 l    df *ABS* 0000000000000000 __valgrind.c
0000000000000000 l    df *ABS* 0000000000000000 errno.c
0000000000000000 l    df *ABS* 0000000000000000 isalnum.c
0000000000000000 l    df *ABS* 0000000000000000 isspace.c
0000000000000000 l    df *ABS* 0000000000000000 isxdigit.c
0000000000000000 l    df *ABS* 0000000000000000 memccpy.c
0000000000000000 l    df *ABS* 0000000000000000 strcspn.c
0000000000000000 l    df *ABS* 0000000000000000 strspn.c
0000000000000000 l    df *ABS* 0000000000000000
```



# Как се прави вълшебен код? С вълшебен линкер скрипт.



```
1 OUTPUT_FORMAT("elf64-x86-64", "elf64-x86-64",
2             "elf64-x86-64")
3 OUTPUT_ARCH(i386:x86-64)
4 ENTRY(_start)
5 SEARCH_DIR("/usr/x86_64-pc-linux-gnu/lib64"); SEARCH_DIR("/usr/local/lib64"); SEARCH_DIR("/lib64"); SEARCH_DIR("/usr/lib64"); SEARCH_DIR("/usr/x86_64-pc-linux-gnu/li
6
7 PHDRS {
8     text PT_LOAD FILEHDR PHDRS FLAGS (7);
9 }
10
11 SECTIONS
12 {
13     PROVIDE (__executable_start = SEGMENT_START("text-segment", 0xbabaceca)); . = SEGMENT_START("text-segment", 0xbabaceca) + SIZEOF_HEADERS;
14     . = ALIGN(CONSTANT (MAXPAGESIZE));
15     .wtf
16     {
17         KEEP (*(SORT_NONE(.init)))
18         *(.text.unlikely .text.*_unlikely .text.unlikely.*)
19         *(.text.exit .text.exit.*)
20         *(.text.startup .text.startup.*)
21         *(.text.hot .text.hot.*)
22         *(SORT(.text.sorted.*))
23         *(.text .stub .text.* .gnu.linkonce.t.*)
24         KEEP (*(SORT_NONE(.fini)))
25
26         *(.rodata .rodata.* .gnu.linkonce.r.*) *(.rodata1)
27
28         *(.eh_frame_hdr) *(.eh_frame_entry .eh_frame_entry.*)
29         KEEP (*(eh_frame)) *(.eh_frame.*)
30         *(.sframe) *(.sframe.*)
31         KEEP (*(eh_frame)) *(.eh_frame.*)
32
33
34         PROVIDE_HIDDEN (__preinit_array_start = .);
35         KEEP (*(preinit_array))
36         PROVIDE_HIDDEN (__preinit_array_end = .);
37
38         PROVIDE_HIDDEN (__init_array_start = .);
39         KEEP (*(SORT_BY_INIT_PRIORITY(.init_array.*) SORT_BY_INIT_PRIORITY(.ctors.*)))
40         KEEP (*(init_array EXCLUDE_FILE (*crtbegin.o *crtbegin.o *crtend.o *crtend.o ) .ctors))
41         PROVIDE_HIDDEN (__init_array_end = .);
```

IDE and Plugin Updates: PyCharm is ready to update. (28 minutes ago)

22:28 LF UTF-8 4 spaces Git: main

# Как е статичния анализ?

The screenshot displays the CodeBrowser static analysis tool interface. The main window is divided into several panes:

- Program Trees:** Shows a hierarchical view of the program's structure, including modules like `hpci`, `hpci_data`, `hpci_dynamic`, and `hpci_data2`.
- Symbol Tree:** A tree view of symbols, with a pink oval highlighting a large section of functions starting with `FUN_0010380`.
- Functions - 189 items:** A table listing functions with columns for Name, Location, Function Signature, and Function Size. A pink oval highlights the `Function Size` column, and a pink line points to the value `375` for the function `undefined FUN_0010380`.
- Defined Strings - 680 items:** A table listing strings with columns for Location, String Value, String Representation, and Data Type. A pink oval highlights the `String Value` column, and a pink line points to the value `"JTM_deregisterTMConeTable"` for the string located at `00100375`.

The bottom of the window shows a status bar with various tool options like `Function Call Graph`, `Decompiler`, `Listing: hpci`, `Memory Map`, `Functions`, `Bytes: hpci`, `Defined Strings`, and `Function Graph`.

[illegible]

The screenshot displays the Ghidra IDE interface with several panels open:

- Program Trees**: Shows the loaded program structure, including segments like .text, .data, .bss, and various frame types.
- Symbol Tree**: Displays the current function being analyzed, listing imports, exports, functions, labels, classes, and namespaces.
- Main Assembly View**: Shows the disassembled code for the function `segment_2.1`. The code includes comments about loadable segments and RAM addresses. The assembly shows instructions for loading and storing data, with some instructions highlighted in green.
- Defined Strings - 112 items**: A list of string literals found in the program, such as "ELF", "lib64-linux-x86-64.so.2", "libc.so.6", etc.
- Error Dialog**: An "Analyzer Error" dialog box is displayed over the main view. It contains the following text:

```
Analysis Task: GCC Exception Handlers - class ghidra.program.models.scalar.Scalar cannot be cast to class java.lang.String (ghidra.program.models.scalar.Scalar is in unnamed module of loader ghidra.GhidraClassLoader @476384ee; java.lang.String is in module java.base of loader 'bootstrap')
```



CodeBrowser(2): hpcv1.MODED

File Edit Analysis Graph Navigation Search Select Tools Window Help

Program Tree 67 items

- hpcv1.MODED
  - data
  - dynamic
  - data.relno
  - fin\_array
  - init\_array
  - eh\_frame
  - pci\_filter\_match
  - kmdd\_load\_resources
  - memcopy
  - pci\_read\_block
  - pci\_set\_name\_list\_path
  - phssec
  - phsget
  - phs
  - init

Symbol Tree

- Imports
- CGFPGS
- Functions
  - DT\_FINI
  - DT\_INIT
  - gmon\_start
  - FUN\_00103C10
  - FUN\_00103C50
- Labels
- Classes
- Namespaces

Filter:

Data Type Manager

- Data Types
- BuiltInTypes
- hpcv1.MODED
- generic\_c1b\_64

Filter:

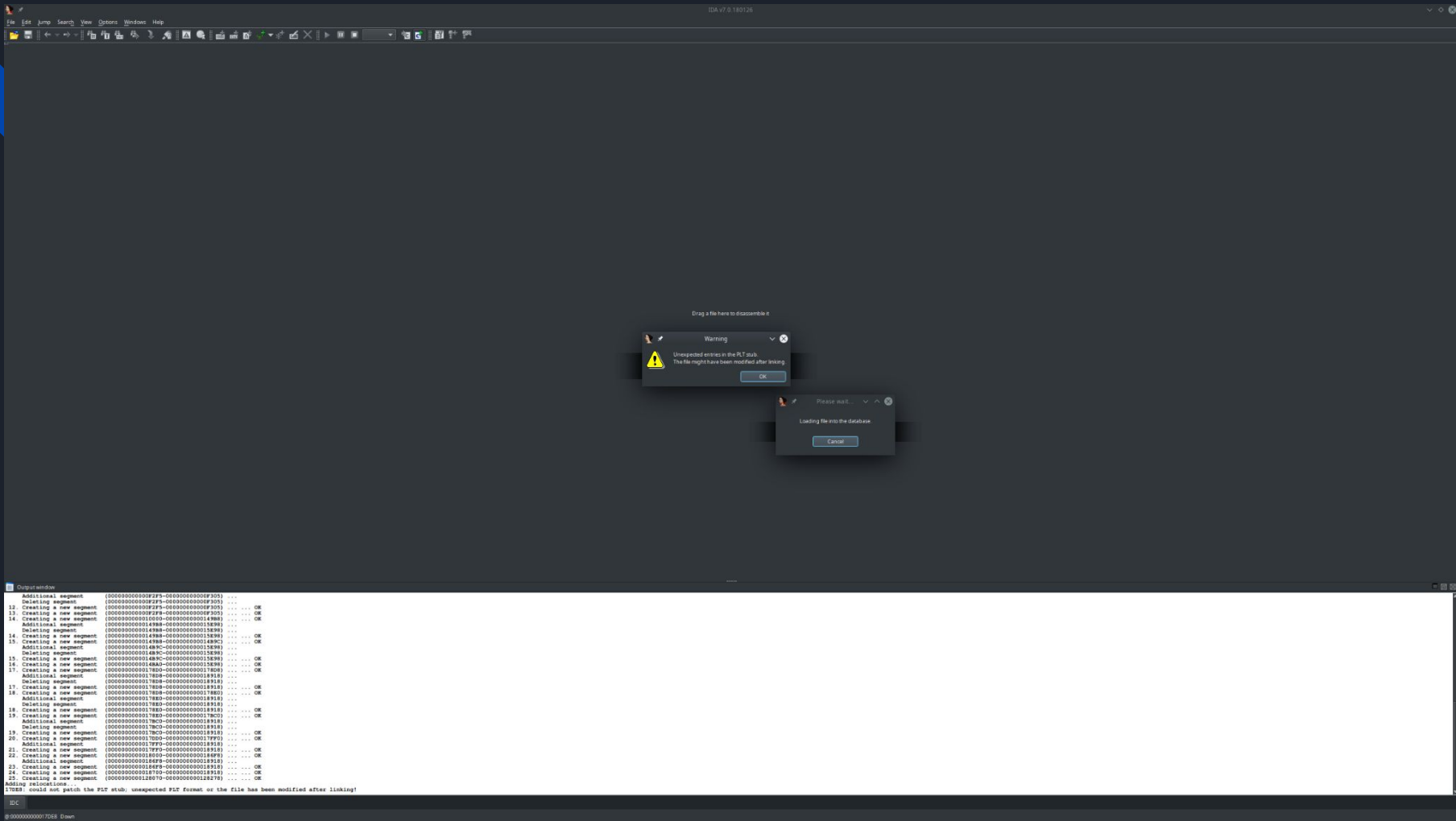
Function Call Graph \* Decompiler \* Listing: hpcv1.MODED \* Memory Map \* Functions \*

Defined Strings 112 items

Name	Location	Function Signature	Function Size	Location	String Value	String Representation	Data Type
DT_INIT	00103000	undefined DT_INIT()	27	00101b3b	__vfprintf_chk	"__vfprintf_chk"	ds
DT_FINI	00102f28	undefined DT_FINI()	13	00101b4a	__vsprintf_chk	"__vsprintf_chk"	ds
gmon_start	00220640	thunk undefined gmon_start()	1	00101b5a	exit	"exit"	ds
FUN_00103C10	00103C10	undefined FUN_00103C10()	1	00101b5f	fputc	"fputc"	ds
FUN_00103C50	00103C50	undefined FUN_00103C50()	1	00101b65	fputs	"fputs"	ds
__cxa_finalize	00229200	thunk undefined __cxa_finalize()	1	00101b6b	free	"free"	ds
pci_filter_match	002291f8	thunk undefined pci_filter_match()	1	00101b70	fwrite	"fwrite"	ds
kmdd_load_resources	002291e0	thunk undefined kmdd_load_resources()	1	00101b77	getopt	"getopt"	ds
memcopy	002291e8	thunk void * memcopy(void * __dest, void * __src, ...)	1	00101b7e	kmdd_list_next	"kmdd_list_next"	ds
pci_read_block	002291d0	thunk undefined pci_read_block()	1	00101b8d	kmdd_load_resources	"kmdd_load_resources"	ds
pci_set_name_list_path	002291d8	thunk undefined pci_set_name_list_path()	1	00101ba1	kmdd_module_get_module	"kmdd_module_get_module"	ds
realloc	002291d0	thunk void * realloc(void * __ptr, size_t __size)	1	00101b88	kmdd_module_get_name	"kmdd_module_get_name"	ds
fwrite	002291c8	thunk size_t fwrite(void * __ptr, size_t __size, ...)	1	00101bcd	kmdd_module_new_from_lookup	"kmdd_module_new_from_lookup"	ds
kmdd_module_get_module	002291c0	thunk undefined kmdd_module_get_module()	1	00101be9	kmdd_module_unref	"kmdd_module_unref"	ds
__sprintf_chk	002291b8	thunk undefined __sprintf_chk()	1	00101bf6	kmdd_module_unref_list	"kmdd_module_unref_list"	ds
__sprintf_chk	002291b0	thunk undefined __sprintf_chk()	1	00101c12	kmdd_new	"kmdd_new"	ds
strncpy	002291a8	thunk char * strncpy(char * __dest, char * __src, ...)	1	00101c1b	kmdd_unref	"kmdd_unref"	ds
pci_read_byte	002291a0	thunk undefined pci_read_byte()	1	00101c26	malloc	"malloc"	ds
pci_read_word	00229198	thunk undefined pci_read_word()	1	00101c2d	memcopy	"memcopy"	ds
pci_scan_bus	00229190	thunk undefined pci_scan_bus()	1	00101c34	memset	"memset"	ds
pci_lookup_name	00229188	thunk undefined pci_lookup_name()	1	00101c3b	optarg	"optarg"	ds
pci_setup_cache	00229180	thunk undefined pci_setup_cache()	1	00101c42	optind	"optind"	ds
pci_fill_info	00229178	thunk undefined pci_fill_info()	1	00101c49	pci_alloc	"pci_alloc"	ds
strncpy	00229170	thunk int strncpy(char * __s1, char * __s2)	1	00101c53	pci_cleanup	"pci_cleanup"	ds
__stack_chk_fail	00229168	thunk undefined __stack_chk_fail()	1	00101c5f	pci_fill_info	"pci_fill_info"	ds
qsort	00229160	thunk void qsort(void * __base, size_t __nmem, ...)	1	00101c6d	pci_filter_init	"pci_filter_init"	ds
pci_get_param	00229158	thunk undefined pci_get_param()	1	00101c7d	pci_filter_match	"pci_filter_match"	ds
pci_filter_parse_slot	00229150	thunk undefined pci_filter_parse_slot()	1	00101c8e	pci_filter_parse_id	"pci_filter_parse_id"	ds
strchr	00229148	thunk char * strchr(char * __s, int __c)	1	00101c92	pci_filter_parse_slot	"pci_filter_parse_slot"	ds
fputc	00229140	thunk int fputc(int __c, FILE * __stream)	1	00101c98	pci_free_dev	"pci_free_dev"	ds
kmdd_module_unref_list	00229138	thunk undefined kmdd_module_unref_list()	1	00101cc5	pci_get_dev	"pci_get_dev"	ds
readlink	00229130	thunk ssize_t readlink(char * __path, char * __b...	1	00101cd1	pci_get_method_name	"pci_get_method_name"	ds
fputs	00229128	thunk int fputs(char * __s, FILE * __stream)	1	00101ce5	pci_get_param	"pci_get_param"	ds
pci_get_method_name	00229120	thunk undefined pci_get_method_name()	1	00101cf3	pci_get_string_property	"pci_get_string_property"	ds
pci_cleanup	00229118	thunk undefined pci_cleanup()	1	00101d0b	pci_init	"pci_init"	ds
kmdd_module_new_from_lookup	00229110	thunk undefined kmdd_module_new_from_lookup()	1	00101d14	pci_lookup_method	"pci_lookup_method"	ds
pci_read_vpd	00229108	thunk undefined pci_read_vpd()	1	00101d26	pci_lookup_name	"pci_lookup_name"	ds
kmdd_unref	00229100	thunk undefined kmdd_unref()	1	00101d38	pci_read_block	"pci_read_block"	ds
pci_filter_parse_id	002290f8	thunk undefined pci_filter_parse_id()	1	00101d45	pci_read_byte	"pci_read_byte"	ds
strchr	002290f0	thunk char * strchr(char * __s, int __c)	1	00101d53	pci_read_vpd	"pci_read_vpd"	ds
kmdd_module_unref	002290e8	thunk undefined kmdd_module_unref()	1	00101d60	pci_read_word	"pci_read_word"	ds
__vfprintf_chk	002290e0	thunk undefined __vfprintf_chk()	1	00101d6e	pci_scan_bus	"pci_scan_bus"	ds
strlen	002290d0	thunk size_t strlen(char * __s)	1	00101d7b	pci_set_name_list_path	"pci_set_name_list_path"	ds
free	002290c8	thunk void free(void * __ptr)	1	00101d92	pci_set_param	"pci_set_param"	ds
kmdd_module_get_name	002290c0	thunk undefined kmdd_module_get_name()	1	00101da0	pci_setup_cache	"pci_setup_cache"	ds
fputc	002290b8	thunk int fputc(int __c, FILE * __stream)	1	00101db0	pci_walk_params	"pci_walk_params"	ds
pci_lookup_method	002290b0	thunk undefined pci_lookup_method()	1	00101dbd	putchar	"putchar"	ds
pci_filter_init	002290a8	thunk undefined pci_filter_init()	1	00101dc8	qsort	"qsort"	ds
__vsprintf_chk	00229098	thunk undefined __vsprintf_chk()	1	00101dce	readlink	"readlink"	ds
pci_alloc	00229090	thunk undefined pci_alloc()	1	00101dd7	realloc	"realloc"	ds
kmdd_new	00229088	thunk undefined kmdd_new()	1	00101de0	stderr	"stderr"	ds
__libc_start_main	00229080	thunk undefined __libc_start_main()	1	00101de6	stdout	"stdout"	ds
malloc	00229078	thunk void * malloc(size_t __size)	1	00101ded	strchr	"strchr"	ds
getopt	00229070	thunk int getopt(int __argc, char * * __argv, ...)	1	00101df4	strcmp	"strcmp"	ds
putchar	00229068	thunk int putchar(int __c)	1	00101dfb	strlen	"strlen"	ds
__printf_chk	00229060	thunk undefined __printf_chk()	1	00101e02	strncpy	"strncpy"	ds
exit	00229058	thunk void exit(int __status)	1	00101e0a	strchr	"strchr"	ds
kmdd_list_next	00229050	thunk undefined kmdd_list_next()	1	00101e12	LIBKMOD_5	"LIBKMOD_5"	ds
fputs	00229048	thunk int fputs(char * __s)	1	00101e1c	GLIBC_2.14	"GLIBC_2.14"	ds
__fprintf_chk	00229038	thunk undefined __fprintf_chk()	1	00101e27	GLIBC_2.4	"GLIBC_2.4"	ds
pci_net_string_property	00229030	thunk undefined pci_net_string_property()	1	00101e31	GLIBC_2.3.4	"GLIBC_2.3.4"	ds

Filter:

00100000 EIP64\_Ehdr (64)



IDA V7.6.180126

File Edit Jump Search View Options Windows Help

File Edit Jump Search View Options Windows Help

...

Drag a file here to disassemble it

Warning

Unrecognized error(s) in the FLT stub  
The file might have been modified after linking  
Don't display this message again (for this session only)

OK Cancel

Press wait...

Go into the database

Output window

Deleting segment (00000000002F78-0000000000000000) ... OK

12. Creating a new segment (00000000002F78-0000000000000000) ... OK

13. Creating a new segment (00000000002F78-0000000000000000) ... OK

14. Creating a new segment (00000000001000-0000000000000000) ... OK

Additional segment (00000000001488-0000000000000000) ... OK

Deleting segment (00000000001488-0000000000000000) ... OK

14. Creating a new segment (00000000001488-0000000000000000) ... OK

15. Creating a new segment (00000000001488-0000000000000000) ... OK

Additional segment (0000000000148C-0000000000000000) ... OK

Deleting segment (0000000000148C-0000000000000000) ... OK

15. Creating a new segment (0000000000148C-0000000000000000) ... OK

16. Creating a new segment (0000000000148C-0000000000000000) ... OK

Additional segment (0000000000148D-0000000000000000) ... OK

Deleting segment (0000000000148D-0000000000000000) ... OK

16. Creating a new segment (0000000000148D-0000000000000000) ... OK

17. Creating a new segment (00000000001700-0000000000000000) ... OK

Additional segment (00000000001700-0000000000000000) ... OK

Deleting segment (00000000001700-0000000000000000) ... OK

17. Creating a new segment (00000000001700-0000000000000000) ... OK

18. Creating a new segment (00000000001700-0000000000000000) ... OK

Additional segment (00000000001700-0000000000000000) ... OK

Deleting segment (00000000001700-0000000000000000) ... OK

18. Creating a new segment (00000000001700-0000000000000000) ... OK

19. Creating a new segment (00000000001700-0000000000000000) ... OK

Additional segment (00000000001700-0000000000000000) ... OK

Deleting segment (00000000001700-0000000000000000) ... OK

19. Creating a new segment (00000000001700-0000000000000000) ... OK

20. Creating a new segment (00000000001700-0000000000000000) ... OK

Additional segment (00000000001700-0000000000000000) ... OK

Deleting segment (00000000001700-0000000000000000) ... OK

20. Creating a new segment (00000000001700-0000000000000000) ... OK

21. Creating a new segment (00000000001700-0000000000000000) ... OK

22. Creating a new segment (00000000001700-0000000000000000) ... OK

Additional segment (00000000001700-0000000000000000) ... OK

Deleting segment (00000000001700-0000000000000000) ... OK

22. Creating a new segment (00000000001700-0000000000000000) ... OK

23. Creating a new segment (00000000001700-0000000000000000) ... OK

24. Creating a new segment (00000000001700-0000000000000000) ... OK

Additional segment (00000000001700-0000000000000000) ... OK

Deleting segment (00000000001700-0000000000000000) ... OK

24. Creating a new segment (00000000001700-0000000000000000) ... OK

Adding relocations ...

170B9: could not patch the PIF stub: unexpected PIF format or the file has been modified after linking!

170F9: could not patch the PIF stub: unexpected PIF format or the file has been modified after linking!

IDC

@0000000000170B9 Down

[illegible]





Демо