oark

0.0.1

Generated by Doxygen 1.7.2

Thu Nov 25 2010 19:18:05

Contents

Chapter 1

Data Structure Index

1.1 Data Structures

Here are the data structures with brief descriptions:

Chapter 2

File Index

2.1 File List

Here is a list of all files with brief descriptions:

Chapter 3

Data Structure Documentation

3.1 _IDT_DESCRIPTOR Struct Reference

```
#include <common.h>
```

Data Fields

- WORD offset00_15
- WORD selector
- BYTE unused:5
- BYTE zeroes:3
- BYTE gateType:5
- BYTE DPL:2
- BYTE P:1
- WORD offset16_31

3.1.1 Field Documentation

3.1.1.1 BYTE DPL

3.1.1.2 BYTE gateType

3.1.1.3 WORD offset00_15

3.1.1.4 WORD offset16_31

3.1.1.5 BYTE P

3.1.1.6 WORD selector

3.1.1.7 BYTE unused

3.1.1.8 BYTE zeroes

The documentation for this struct was generated from the following file:

- common/common/common.h

3.2 _IDTR Struct Reference

```
#include <common.h>
```

Data Fields

- WORD nBytes
- WORD baseAddressLow
- WORD baseAddressHi

3.2.1 Field Documentation

3.2.1.1 WORD baseAddressHi

3.2.1.2 WORD baseAddressLow

3.2.1.3 WORD nBytes

The documentation for this struct was generated from the following file:

- common/common/common.h

3.3 _KGDTENTRY Struct Reference

`#include <idt.h>`

Data Fields

- WORD LimitLow
- WORD BaseLow
- ULONG HighWord

3.3.1 Field Documentation

3.3.1.1 WORD BaseLow

3.3.1.2 ULONG HighWord

3.3.1.3 WORD LimitLow

The documentation for this struct was generated from the following file:

- oark_usermode/oark_usermode/idt.h

3.4 _KIDTENTRY Struct Reference

`#include <idt.h>`

Data Fields

- WORD Offset
- WORD Selector
- WORD Access
- WORD ExtendedOffset

3.4.1 Field Documentation

3.4.1.1 WORD Access

3.4.1.2 WORD ExtendedOffset

3.4.1.3 WORD Offset

3.4.1.4 WORD Selector

The documentation for this struct was generated from the following file:

- oark_usermode/oark_usermode/idt.h

3.5 _KPCR Struct Reference

`#include <idt.h>`

Data Fields

- NT_TIB NtTib
- void * SelfPcr
- void * Prcb
- UCHAR Irql
- ULONG IRR
- ULONG IrrActive
- ULONG IDR
- PVOID KdVersionBlock
- PKIDTENTRY IDT
- PKGDTENTRY GDT

3.5.1 Field Documentation

3.5.1.1 PKGDTENTRY GDT

3.5.1.2 ULONG IDR

3.5.1.3 PKIDTENTRY IDT

3.5.1.4 UCHAR Irql

3.5.1.5 ULONG IRR

3.5.1.6 ULONG IrrActive

3.5.1.7 PVOID KdVersionBlock

3.5.1.8 NT_TIB NtTib

3.5.1.9 void* Prcb

3.5.1.10 void* SelfPcr

The documentation for this struct was generated from the following file:

- oark_usermode/oark_usermode/idt.h

3.6 READ_KERN_MEM_s Struct Reference

`#include <common.h>`

Data Fields

- void * src_address
- DWORD size
- MEM_SYM_TYP_t type
- void * dst_address

3.6.1 Field Documentation

3.6.1.1 void* dst_address

3.6.1.2 DWORD size

3.6.1.3 void* src_address

3.6.1.4 MEM_SYM_TYP_t type

The documentation for this struct was generated from the following file:

- common/common/common.h

Chapter 4

File Documentation

4.1 common/common/common.h File Reference

```
#include <WinDef.h>
```

Data Structures

- struct READ_KERN_MEM_s
- struct _IDT_DESCRIPTOR
- struct _IDTR

Defines

- #define OARK_VERSION "0.0.1"
- #define DEVICE_NAME "\\Device\\OARK_DRIVER"
- #define SYMLINK_NAME "\\DosDevices\\OARK_DRIVER"
- #define NAMEOF_DEVICE "\\\\.\\OARK_DRIVER"
- #define DRIVER_NAME "OARK_DRIVER.SYS"
- #define SERVICE_NAME "OARK_DRIVER"
- #define OARK_IOCTL_CHANGE_MODE CTL_CODE(FILE_DEVICE_UNKNOWN, 0x801, METHOD_OUT_DIRECT, FILE_READ_DATA | FILE_WRITE_DATA)
- #define IDT_HARDCODE_SIZE 0x7FF
- #define MAKEDWORD(a, b) ((unsigned int)(((WORD)(a)) | ((WORD)((WORD)(b))) << 16))

Typedefs

- typedef enum STATUS_e STATUS_t
- typedef enum MEM_SYM_TYP_e MEM_SYM_TYP_t
- typedef struct READ_KERN_MEM_s READ_KERN_MEM_t

- typedef struct _IDT_DESCRIPTOR IDT_DESCRIPTOR

- typedef struct _IDT_DESCRIPTOR * PIDT_DESCRIPTOR

- typedef struct _IDTR IDTR

Enumerations

- enum STATUS_e { ST_ERROR = 0, ST_OK }

- enum MEM_SYM_TYP_e { SYM_TYP_NULL = 0, SYM_TYP_KPCR, SYM_TYP_IDT }

4.1.1 Define Documentation

4.1.1.1 #define DEVICE_NAME "\\Device\\OARK_DRIVER"

4.1.1.2 #define DRIVER_NAME "OARK_DRIVER.SYS"

4.1.1.3 #define IDT_HARDCODE_SIZE 0x7FF

4.1.1.4 #define MAKEDWORD(*a, b*) ((unsigned int)(((WORD)(a)) | ((WORD)((WORD)(b))) << 16))

4.1.1.5 #define NAMEOF_DEVICE "\\\\.\\OARK_DRIVER"

4.1.1.6 #define OARK_IOCTL_CHANGE_MODE CTL_CODE(FILE_DEVICE_UNKNOWN, 0x801, METHOD_OUT_DIRECT, FILE_READ_DATA | FILE_WRITE_DATA)

4.1.1.7 #define OARK_VERSION "0.0.1"

4.1.1.8 #define SERVICE_NAME "OARK_DRIVER"

4.1.1.9 #define SYMLINK_NAME "\\DosDevices\\OARK_DRIVER"

4.1.2 Typedef Documentation

4.1.2.1 typedef struct _IDT_DESCRIPTOR IDT_DESCRIPTOR

4.1.2.2 typedef struct _IDTR IDTR

4.1.2.3 typedef enum MEM_SYM_TYP_e MEM_SYM_TYP_t

4.1.2.4 typedef struct _IDT_DESCRIPTOR * PIDT_DESCRIPTOR

4.1.2.5 typedef struct READ_KERN_MEM_s READ_KERN_MEM_t

4.1.2.6 typedef enum STATUS_e STATUS_t

4.1.3 Enumeration Type Documentation

4.1.3.1 enum MEM_SYM_TYP_e

Enumerator:

SYM_TYP_NULL

SYM_TYP_KPCR

SYM_TYP_IDT

4.1.3.2 enum STATUS_e

Enumerator:

ST_ERROR

ST_OK

4.2 oark_driver/oark_driver/buildnumber.h File Reference

Defines

- #define _FILE_VERSION_BUILD 47

4.2.1 Define Documentation

4.2.1.1 #define _FILE_VERSION_BUILD 47

4.3 oark_driver/oark_driver/drvcommon.h File Reference

Defines

- #define _ANSISTRING(text) #text
- #define ANSISTRING(text) _ANSISTRING(text)
- #define _WIDESTRING(text) L##text
- #define WIDESTRING(text) _WIDESTRING(text)
- #define PRESET_UNICODE_STRING(symbol, buffer)
- #define CREATE_XVER(maj, min, build) maj ## , ## min ## , 0, ## build
- #define CREATE_FVER(maj, min, build) maj ## . ## min ## .0. ## build
- #define CREATE_PVER(maj, min, build) maj ## . ## min
- #define DebugPrint /##/DbgPrint

4.3.1 Define Documentation

4.3.1.1 #define _ANSISTRING(*text*) #text

Copyright (c) 2010 - <company name="" here>="">

Useful macros

(File was in the PUBLIC DOMAIN - Created by: ddkwizard\.assarbad\.net)

4.3.1.2 #define _WIDESTRING(*text*) L##text

4.3.1.3 #define ANSISTRING(*text*) _ANSISTRING(text)

4.3.1.4 #define CREATE_FVER(*maj, min, build*) maj ## . ## min ## .0. ## build

4.3.1.5 #define CREATE_PVER(*maj, min, build*) maj ## . ## min

4.3.1.6 #define CREATE_XVER(*maj, min, build*) maj ## , ## min ## , 0, ## build

4.3.1.7 #define DebugPrint /##/DbgPrint

4.3.1.8 #define PRESET_UNICODE_STRING(*symbol, buffer*)

Value:

```
UNICODE_STRING symbol = \
            { \
            sizeof(WIDESTRING(buffer)) - sizeof(WCHAR), \
            sizeof(WIDESTRING(buffer)), \
            WIDESTRING(buffer) \
            };
```

4.3.1.9 #define WIDESTRING(*text*) _WIDESTRING(text)

4.4 oark_driver/oark_driver/drvversion.h File Reference

```
#include "buildnumber.h"
```

Defines

- #define TEXT_AUTHOR <author name(s)>
- #define PRD_MAJVER 1
- #define PRD_MINVER 0
- #define PRD_BUILD 0
- #define FILE_MAJVER 1
- #define FILE_MINVER 0
- #define FILE_BUILD _FILE_VERSION_BUILD
- #define DRV_YEAR 2010
- #define TEXT_WEBSITE <website>
- #define TEXT_PRODUCTNAME Supercool driver-based tool
- #define TEXT_FILEDESC The driver for the supercool driver-based tool
- #define TEXT_COMPANY <company name here>
- #define TEXT_MODULE oark_driver
- #define TEXT_COPYRIGHT Copyright \xA9 DRV_YEAR TEXT_COMPANY
- #define TEXT_INTERNALNAME oark_driver.sys

4.4.1 Define Documentation

4.4.1.1 #define DRV_YEAR 2010

4.4.1.2 #define FILE_BUILD _FILE_VERSION_BUILD

4.4.1.3 #define FILE_MAJVER 1

4.4.1.4 #define FILE_MINVER 0

4.4.1.5 #define PRD_BUILD 0

4.4.1.6 #define PRD_MAJVER 1

4.4.1.7 #define PRD_MINVER 0

4.4.1.8 #define TEXT_AUTHOR <author name(s)>

Copyright (c) 2010 - <company name="" here>="">
Defines for the version information in the resource file
(File was in the PUBLIC DOMAIN - Created by: ddkwizard\.assarbad\.net)

4.4.1.9 #define TEXT_COMPANY <company name here>

4.4.1.10 #define TEXT_COPYRIGHT Copyright \xA9 DRV_YEAR TEXT_COMPANY

4.4.1.11 #define TEXT_FILEDESC The driver for the supercool driver-based tool

4.4.1.12 #define TEXT_INTERNALNAME oark_driver.sys

4.4.1.13 #define TEXT_MODULE oark_driver

4.4.1.14 #define TEXT_PRODUCTNAME Supercool driver-based tool

4.4.1.15 #define TEXT_WEBSITE <website>

4.5 oark_driver/oark_driver/makefile.inc File Reference

4.6 oark_driver/oark_driver/oark_driver.cpp File Reference

```
#include <ntddk.h>
#include <string.h>
#include "oark_driver.h"
#include "common.h"
```

Functions

- int WriteUserMode (void *address, DWORD size, void *data)
- NTSTATUS OARKDRIVER_DispatchCreateClose (IN PDEVICE_OBJECT DeviceObject, IN PIRP Irp)
- NTSTATUS OARKDRIVER_DispatchDeviceControl (IN PDEVICE_OBJECT DeviceObject, IN PIRP Irp)
- VOID OARKDRIVER_DriverUnload (IN PDRIVER_OBJECT DriverObject)
- NTSTATUS DriverEntry (IN OUT PDRIVER_OBJECT DriverObject, IN PUNICODE_STRING RegistryPath)

Variables

- PDRIVER_OBJECT pdoGlobalDrvObj = 0

4.6.1 Function Documentation

4.6.1.1 NTSTATUS DriverEntry (IN OUT PDRIVER_OBJECT *DriverObject,* IN PUNICODE_STRING *RegistryPath*)

4.6.1.2 NTSTATUS OARKDRIVER_DispatchCreateClose (IN PDEVICE_OBJECT *DeviceObject,* IN PIRP *Irp*)

4.6.1.3 NTSTATUS OARKDRIVER_DispatchDeviceControl (IN PDEVICE_OBJECT *DeviceObject,* IN PIRP *Irp*)

4.6.1.4 VOID OARKDRIVER_DriverUnload (IN PDRIVER_OBJECT *DriverObject*)

4.6.1.5 int WriteUserMode (void * *address,* DWORD *size,* void * *data*)

4.6.2 Variable Documentation

4.6.2.1 PDRIVER_OBJECT pdoGlobalDrvObj = 0

Copyright (c) 2010 - <company name="" here>="">

Original filename: oark_driver.cpp Project : oark_driver Date of creation : 2010-11-12 Author(s) : <author name(s)>

Purpose :

Revisions: 0000 [2010-11-12] Initial revision.

4.7 oark_driver/oark_driver/oark_driver.h File Reference

```
#include "drvcommon.h"
#include "drvversion.h"
```

```
#include "common.h"
```

Defines

- #define FILE_DEVICE_OARKDRIVER 0x8000

Functions

- PRESET_UNICODE_STRING (usDeviceName, DEVICE_NAME)
- PRESET_UNICODE_STRING (usSymlinkName, SYMLINK_NAME)

4.7.1 Define Documentation

4.7.1.1 #define FILE_DEVICE_OARKDRIVER 0x8000

4.7.2 Function Documentation

4.7.2.1 PRESET_UNICODE_STRING (usDeviceName , DEVICE_NAME)

Copyright (c) 2010 - <company name="" here>="">

Original filename: oark_driver.h Project : oark_driver Date of creation : <see oark_driver.cpp> Author(s) : <see oark_driver.cpp>

Purpose : <see oark_driver.cpp>

Revisions: <see oark_driver.cpp>

4.7.2.2 PRESET_UNICODE_STRING (usSymlinkName , SYMLINK_NAME)

4.8 oark_usermode/oark_usermode/debug.c File Reference

```
#include "debug.h"
```

Functions

- STATUS_t EnableDebugPrivilege (void)

Variables

- debug = TRUE

4.8.1 Function Documentation

4.8.1.1 STATUS_t EnableDebugPrivilege (void)

4.8.2 Variable Documentation

4.8.2.1 debug = TRUE

4.9 oark_usermode/oark_usermode/debug.h File Reference

```
#include <windows.h>
#include <stdio.h>
#include "common.h"
```

Functions

- STATUS_t EnableDebugPrivilege (void)

Variables

- BOOL debug

4.9.1 Function Documentation

4.9.1.1 STATUS_t EnableDebugPrivilege (void)

4.9.2 Variable Documentation

4.9.2.1 BOOL debug

4.10 oark_usermode/oark_usermode/driverusr.c File Reference

```
#include "driverusr.h"
```

Functions

- void * IOCTLReadKernMem (HANDLE device, READ_KERN_MEM_t *read_kern_mem)
- BOOLEAN LoadDriver (HANDLE *device)
- int UnloadDriver (HANDLE *device)

4.10.1 Function Documentation

4.10.1.1 void* IOCTLReadKernMem (HANDLE *device,* READ_KERN_MEM_t * *read_kern_mem*)

4.10.1.2 BOOLEAN LoadDriver (HANDLE * *device*)

4.10.1.3 int UnloadDriver (HANDLE * *device*)

4.11 oark_usermode/oark_usermode/driverusr.h File Reference

```
#include <stdio.h>
#include <windows.h>
#include "resource.h"
#include "debug.h"
#include "common.h"
#include "others.h"
```

Functions

- void * IOCTLReadKernMem (HANDLE, READ_KERN_MEM_t *)
- BOOLEAN LoadDriver (HANDLE *)
- int UnloadDriver (HANDLE *)
- BOOLEAN GetFullTempPath (char **, char *)
- BOOLEAN DumpRSRC (char *, int, char *)

4.11.1 Function Documentation

4.11.1.1 BOOLEAN DumpRSRC (char * , int , char *)

4.11.1.2 BOOLEAN GetFullTempPath (char ** , char *)

4.11.1.3 void* IOCTLReadKernMem (HANDLE , READ_KERN_MEM_t *)

4.11.1.4 BOOLEAN LoadDriver (HANDLE *)

4.11.1.5 int UnloadDriver (HANDLE *)

4.12 oark_usermode/oark_usermode/idt.c File Reference

```
#include "idt.h"
```

Functions

- int idt (HANDLE device)

4.12.1 Function Documentation

4.12.1.1 int idt (HANDLE *device*)

4.13 oark_usermode/oark_usermode/idt.h File Reference

```
#include <windows.h>
#include <stdio.h>
#include "common.h"
#include "driverusr.h"
```

Data Structures

- struct _KIDTENTRY
- struct _KGDTENTRY
- struct _KPCR

Typedefs

- typedef struct _KIDTENTRY KIDTENTRY
- typedef struct _KIDTENTRY * PKIDTENTRY
- typedef struct _KGDTENTRY KGDTENTRY
- typedef struct _KGDTENTRY * PKGDTENTRY
- typedef struct _KPCR KPCR
- typedef struct _KPCR * PKPCR

Functions

- int idt (HANDLE)

4.13.1 Typedef Documentation

4.13.1.1 typedef struct _KGDTENTRY KGDTENTRY

4.13.1.2 typedef struct _KIDTENTRY KIDTENTRY

4.13.1.3 typedef struct _KPCR KPCR

4.13.1.4 typedef struct _KGDTENTRY * PKGDTENTRY

4.13.1.5 typedef struct _KIDTENTRY * PKIDTENTRY

4.13.1.6 typedef struct _KPCR * PKPCR

4.13.2 Function Documentation

4.13.2.1 int idt (HANDLE)

4.14 oark_usermode/oark_usermode/main.c File Reference

```
#include <stdio.h>
#include <windows.h>
#include "debug.h"
#include "common.h"
#include "driverusr.h"
#include "idt.h"
#include "others.h"
```

Functions

- int main (void)

4.14.1 Function Documentation

4.14.1.1 int main (void)

4.15 oark_usermode/oark_usermode/others.c File Reference

```
#include "others.h"
```

Functions

- STATUS_t LockInstance (DWORD *other_pid)
- BOOLEAN GetFullTempPath (char **out_full_temp_path, char *name)
- BOOLEAN DumpRSRC (char *full_temp_path, int resource_id, char *driver_name)

4.15.1 Function Documentation

4.15.1.1 BOOLEAN DumpRSRC (char * *full_temp_path,* int *resource_id,* char * *driver_name*)

4.15.1.2 BOOLEAN GetFullTempPath (char ** *out_full_temp_path,* char * *name*)

4.15.1.3 STATUS_t LockInstance (DWORD * *other_pid*)

4.16 oark_usermode/oark_usermode/others.h File Reference

```
#include <windows.h>
#include <tlhelp32.h>
#include "common.h"
#include "debug.h"
```

Defines

- #define __OTHERS_H__

Functions

- STATUS_t LockInstance (DWORD *)
- BOOLEAN DumpRSRC (char *, int, char *)
- BOOLEAN GetFullTempPath (char **, char *)

4.16.1 Define Documentation

4.16.1.1 #define __OTHERS_H__

4.16.2 Function Documentation

4.16.2.1 BOOLEAN DumpRSRC (char *, int , char *)

4.16.2.2 BOOLEAN GetFullTempPath (char **, char *)

4.16.2.3 STATUS_t LockInstance (DWORD *)

4.17 oark_usermode/oark_usermode/pebhooking.c File Reference

```
#include "pebhooking.h"
```

4.18 oark_usermode/oark_usermode/pebhooking.h File Reference

4.19 oark_usermode/oark_usermode/resource.h File Reference

Defines

- #define IDR_OARK_DRIVER 101
- #define IDI_ICON1 102

4.19.1 Define Documentation

4.19.1.1 #define IDI_ICON1 102

4.19.1.2 #define IDR_OARK_DRIVER 101

Index