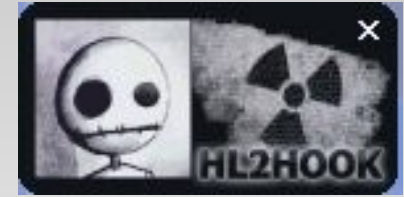


# HL2 Hook



- The Program
- The Disassembly
- Other Tools
- Playing Around
- Conclusion

# The Program Use Case

- Start the program
- Generates a widget showing it is ready
- Open CS:S
- HL2 Hook does its business and closes

# Disassembly, begin!

```
OllyDbg - miranda32.exe - [CPU - main thread, module miranda3]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
00401000 |$ 55 | PUSH EBP
00401001 | 50 | PUSH EAX
00401002 | 8BC4 | MOV EAX,ESP
00401004 | 83C0 04 | ADD EAX,4
00401007 | C700 00204600 | MOV DWORD PTR DS:[EAX],miranda3.00462000
0040100D | 58 | POP EAX
0040100E | C3 | RETN
0040100F | 90 | NOP
00401010 | C3 | RETN
00401011 | 50 | DB 50 CHAR 'J'
00401012 | CE | DB CE
00401013 | A3 | DB A3
00401014 | 50 | DB 50 CHAR 'P'
00401015 | 0A | DB 0A
00401016 | 06 | DB 06
00401017 | 62 | DB 62 CHAR 'b'
00401018 | B0 | DB B0
00401019 | CE | DB CE
0040101A | 38 | DB 38 CHAR '8'
0040101B | E5 | DB E5
0040101C | 1A | DB 1A
0040101D | 32 | DB 32 CHAR '2'
0040101E | 9A | DB 9A
0040101F | CF | DB CF
00401020 | 5A | DB 5A CHAR 'Z'
00401021 | C1 | DB C1
00401022 | 6F | DB 6F CHAR 'o'
00401023 | 84 | DB 84
00401024 | B5 | DB B5
00401025 | FE | DB FE
00401026 | 3E | DB 3E CHAR '>'
00401027 | CC | INT3
00401028 | 6A | DB 6A CHAR 'j'
00401029 | 08 | DB 08
0040102A | C5 | DB C5
0040102B | EB | DB EB
0040102C | 62 | DB 62 CHAR 'b'
0040102D | 33 | DB 33 CHAR '3'
0040102E | 77 | DB 77 CHAR 'w'
```

# Jump, Leaving Code Section

OllyDbg - miranda32.exe - [CPU - main thread, module miranda3]

File View Debug Plugins Options Window Help

← X ▶ || ↶ ↷ ↵ ↶ ↷ ↵ ↶ ↷ ↵ L E M T W H C / K B R ... S

00462000	55	PUSH EBP	
00462001	BD 00100600	MOV EBP,61000	We are here
00462006	60	PUSHAD	
00462007	68 180E0000	PUSH 0E18	
0046200C	68 1F204600	PUSH miranda3.0046201F	
00462011	E8 250E0000	CALL miranda3.00462E3B	
00462016	90	NOP	
00462017	90	NOP	
00462018	90	NOP	
00462019	90	NOP	
0046201A	90	NOP	
0046201B	90	NOP	
0046201C	90	NOP	
0046201D	90	NOP	
0046201E	90	NOP	
0046201F	8D85 3B104000	LEA EAX,DWORD PTR SS:[EBP+40103B]	
00462025	50	PUSH EAX	
00462026	33F6	XOR ESI,ESI	
00462028	64:FF36	PUSH DWORD PTR FS:[ESI]	
0046202B	64:8926	MOV DWORD PTR FS:[ESI],ESP	
0046202E	8D85 49104000	LEA EAX,DWORD PTR SS:[EBP+401049]	
00462034	50	PUSH EAX	
00462035	E8 FBFFFFFF	CALL miranda3.00462035	
0046203A	C3	RETN	
0046203B	8B4424 0C	MOV EAX,DWORD PTR SS:[ESP+C]	
0046203F	8380 B8000000	ADD DWORD PTR DS:[EAX+B8],5	
00462046	33C0	XOR EAX,EAX	
00462048	C3	RETN	
00462049	64:8F06	POP DWORD PTR FS:[ESI]	
0046204C	58	POP EAX	
0046204D	8B5C24 24	MOV EBX,DWORD PTR SS:[ESP+24]	
00462051	66:33DB	XOR BX,BX	
00462054	66:B9 405A	MOV CX,5A40	
00462058	66:330B	XOR CX,WORD PTR DS:[EBX]	
0046205B	74 08	JE SHORT miranda3.00462065	
0046205D	81EB 00000100	SUB EBX,10000	
00462063	EB EF	JMP SHORT miranda3.00462054	
00462065	66:81C1 5045	ADD CX,4550	UNICODE ":::~"
0046206A	8BC3	MOV EAX,EBX	

# Time to Rewrite

The screenshot shows the OllyDbg interface for miranda32.exe. The assembly window displays instructions from address 00462E3B to 00462E9F. Annotations with arrows point to specific instructions:

- Getting Data:** Points to `LODS DWORD PTR DS:[ESI]` at address 00462E88.
- "Decrypt":** Points to `DEC EBX` at address 00462E90.
- Write Data:** Points to `MOV EBX,EBX` at address 00462EDF.
- Jump back:** Points to `JNZ SHORT miranda3.00462E88` at address 00462E9F.

The registers window on the right shows the current state of the CPU registers, including EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDI, and EIP.



# The End, I Give Up

OllyDbg - miranda32.exe - [CPU - main thread, module miranda3]

File View Debug Plugins Options Window Help

LEMTW H C / K B R ... S

Address	Disassembly
0046201C	90 NOP
0046201D	90 NOP
0046201E	90 NOP
0046201F	8D85 3B104000 LEA EAX, DWORD PTR SS:[EBP+40103B]
00462020	59 PUSH EAX
00462021	33F6 XOR ESI, ESI
00462022	64:FF36 PUSH DWORD PTR FS:[ESI]
00462023	64:8926 MOV DWORD PTR FS:[ESI], ESP
00462024	8D85 49104000 LEA EAX, DWORD PTR SS:[EBP+401049]
00462025	59 PUSH EAX
00462026	E8 FBFFFFFF CALL miranda3.00462035
00462027	C3 RETN
00462028	8B4424 0C MOV EAX, DWORD PTR SS:[ESP+C]
00462029	8380 B0000000 0 ADD DWORD PTR DS:[EAX+B8], 5
0046202A	33C0 XOR EAX, EAX
0046202B	C3 RETN
0046202C	64:8F06 POP DWORD PTR FS:[ESI]
0046202D	59 POP EAX
0046202E	8B5C24 24 MOV EBX, DWORD PTR SS:[ESP+24]
0046202F	66:330B XOR BX, BX
00462030	66:B9 4D5A MOV CX, 5A4D
00462031	66:330B XOR CX, WORD PTR DS:[EBX]
00462032	75 E9 JE SHORT miranda3.00462065
00462033	81EB 00000100 SUB EBX, 10000
00462034	EB EF JMP SHORT miranda3.00462054
00462035	66:81C1 5045 ADD CX, 4550
00462036	8BC3 MOV EAX, EBX
00462037	0340 3C ADD EAX, DWORD PTR DS:[EAX+3C]
00462038	66:330B XOR CX, WORD PTR DS:[EAX]
00462039	75 E9 JNZ SHORT miranda3.0046205D
0046203A	8B40 50 MOV EAX, DWORD PTR DS:[EAX+50]
0046203B	3D 00300200 CMP EAX, 23000
0046203C	76 32 JBE SHORT miranda3.004620B0
0046203D	8DBD CD1C4000 LEA EDI, DWORD PTR SS:[EBP+401CCD]
0046203E	B9 25000000 MOV ECX, 25
0046203F	57 PUSH EDI
00462040	51 PUSH ECX
00462041	8B3F MOV EDI, DWORD PTR DS:[EDI]
00462042	E8 AA020000 CALL miranda3.0046233C
00462043	59 POP ECX
00462044	5F POP EDI
00462045	AB STOS DWORD PTR ES:[EDI]
00462046	E2 F2 LOOPD SHORT miranda3.00462089
00462047	F785 811D4000 0 TEST DWORD PTR SS:[EBP+401D81], 1
00462048	74 29 JE SHORT miranda3.004620CC
00462049	53 PUSH EBX
0046204A	E8 E2020000 CALL miranda3.0046238B
0046204B	5B POP EBX
0046204C	8BB5 F51C4000 MOV ESI, DWORD PTR SS:[EBP+401CF5]
0046204D	8DBD 87144000 LEA EDI, DWORD PTR SS:[EBP+401487]
0046204E	E8 3C090000 CALL miranda3.004629F7
0046204F	8BB5 ED1C4000 MOV ESI, DWORD PTR SS:[EBP+401CED]
00462050	8DBD C8144000 LEA EDI, DWORD PTR SS:[EBP+4014CA]
00462051	E8 2B090000 CALL miranda3.004629F7
00462052	6A 00 PUSH 0
00462053	FF95 F91C4000 CALL DWORD PTR SS:[EBP+401CF9]
00462054	8BD8 MOV EBX, EAX
00462055	8BF0 MOV ESI, EAX
00462056	8BD8 MOV ECX, DWORD PTR SS:[EBP+401E33]
00462057	0376 3C ADD ESI, DWORD PTR DS:[ESI+3C]
00462058	56 PUSH ESI
00462059	0FB776 14 MOVZX ESI, WORD PTR DS:[ESI+14]
0046205A	83C6 18 ADD ESI, 18
0046205B	013424 ADD DWORD PTR SS:[ESP], ESI
0046205C	5E POP ESI
0046205D	817E 1C 292D3B00 CMP DWORD PTR DS:[ESI+1C], 3B2D29
0046205E	75 70 JNZ SHORT miranda3.00462166
0046205F	60 PUSHAD
00462060	8B7E 0C MOV EDI, DWORD PTR DS:[ESI+C]

Infinite Call Stack Overflow

Unicode ":::::"

Registers (FPU)

EAX 00001000  
ECX 368E0665  
EDX 000073DA  
EBX 118B8EC0  
ESP 0012FFA0  
EBP 00061000  
ESI 000021EF  
EDI 0000167E

EIP 0046201C miranda3.0046201C

C 0 ES 0023 32bit 0(FFFFFFFF)  
F 1 CS 001B 32bit 0(FFFFFFFF)  
A 1 SS 0023 32bit 0(FFFFFFFF)  
Z 0 DS 0023 32bit 0(FFFFFFFF)  
S 0 FS 003B 32bit 7FFDF000(FFF)  
T 0 GS 0000 NULL

D 0  
O 0 LastErrr ERROR\_SUCCESS (00000000)

EFL 00000216 (NO, NB, NE, A, NS, PE, GE, G)

ST0 empty -UNORM BDEC 01050104 00000000  
ST1 empty 0.0  
ST2 empty 0.0  
ST3 empty 0.0  
ST4 empty 0.0  
ST5 empty 0.0  
ST6 empty 0.0  
ST7 empty 0.0

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0  
FCW 027F Prec NEAR, 53 Mask 1 1 1 1 1 1

Breakpoint at miranda3.0046201C

Paused

start 4 Windows Explorer OllyDbg - miranda32... 97% 7:55 AM

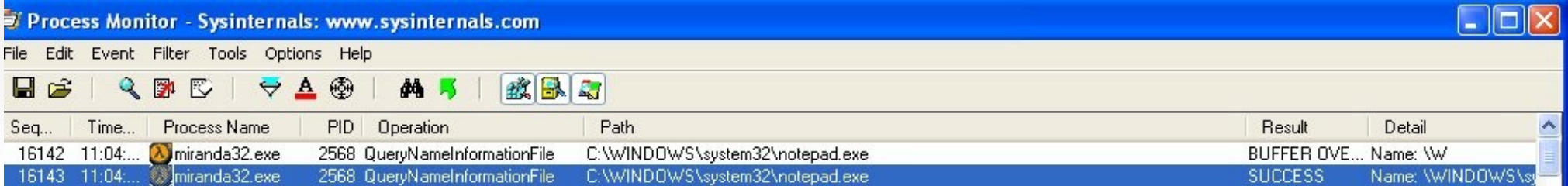
# Process Monitor

The screenshot shows the Process Monitor application window with a list of events. The window title is "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations and monitoring. The main area is a table with columns for Sequence Number, Time, Process Name, PID, Operation, and Path. The events listed are for the process "miranda32.exe" with PID 3064, showing various registry and file operations. The status bar at the bottom indicates "Showing 1,491 of 554,813 events (0.26%)".

Seq...	Time...	Process Name	PID	Operation	Path
254260	10:40:...	miranda32.exe	3064	RegCloseKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters
254261	10:40:...	miranda32.exe	3064	RegOpenKey	HKLM\System\CurrentControlSet\Services\Winsock2\Parameters
254262	10:40:...	miranda32.exe	3064	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Ws2_32NumHandleBuckets
254263	10:40:...	miranda32.exe	3064	RegCloseKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters
254264	10:40:...	miranda32.exe	3064	ReadFile	C:\Hack\_pub.13.0.3\miranda32.exe
254274	10:40:...	miranda32.exe	3064	CreateFile	C:\Hack\_pub.13.0.3
254275	10:40:...	miranda32.exe	3064	QueryDirectory	C:\Hack\_pub.13.0.3\aspr_keys.ini
254276	10:40:...	miranda32.exe	3064	CloseFile	C:\Hack\_pub.13.0.3
254278	10:40:...	miranda32.exe	3064	CreateFile	C:\WINDOWS\system32\ntdll.dll
254282	10:40:...	miranda32.exe	3064	QueryStandardInfo...	C:\WINDOWS\system32\ntdll.dll
254283	10:40:...	miranda32.exe	3064	QuerySizeInformati...	C:\WINDOWS\system32\ntdll.dll
254284	10:40:...	miranda32.exe	3064	CreateFile	C:
254997	10:40:...	miranda32.exe	3064	WriteFile	C:\Documents and Settings\cs492\Local Settings\Temporary Internet Files\Content.IE5\index.dat
255001	10:40:...	miranda32.exe	3064	WriteFile	C:\Documents and Settings\cs492\Local Settings\Temporary Internet Files\Content.IE5\index.dat
255002	10:40:...	miranda32.exe	3064	WriteFile	C:\Documents and Settings\cs492\Local Settings\Temporary Internet Files\Content.IE5\index.dat
255005	10:40:...	miranda32.exe	3064	WriteFile	C:\Documents and Settings\cs492\Local Settings\History\History.IE5\index.dat
255010	10:40:...	miranda32.exe	3064	WriteFile	C:\Documents and Settings\cs492\Cookies\index.dat
257801	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
257828	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
257837	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
257862	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
257865	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
258020	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
258086	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
258089	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
258144	10:40:...	miranda32.exe	3064	WriteFile	C:\\$Directory
258241	10:40:...	miranda32.exe	3064	FileSystemControl	C:
258249	10:40:...	miranda32.exe	3064	FileSystemControl	C:\WINDOWS\system32\ntdll.dll

# Detecting HL2

- Checks the name/path of all starting programs .exe

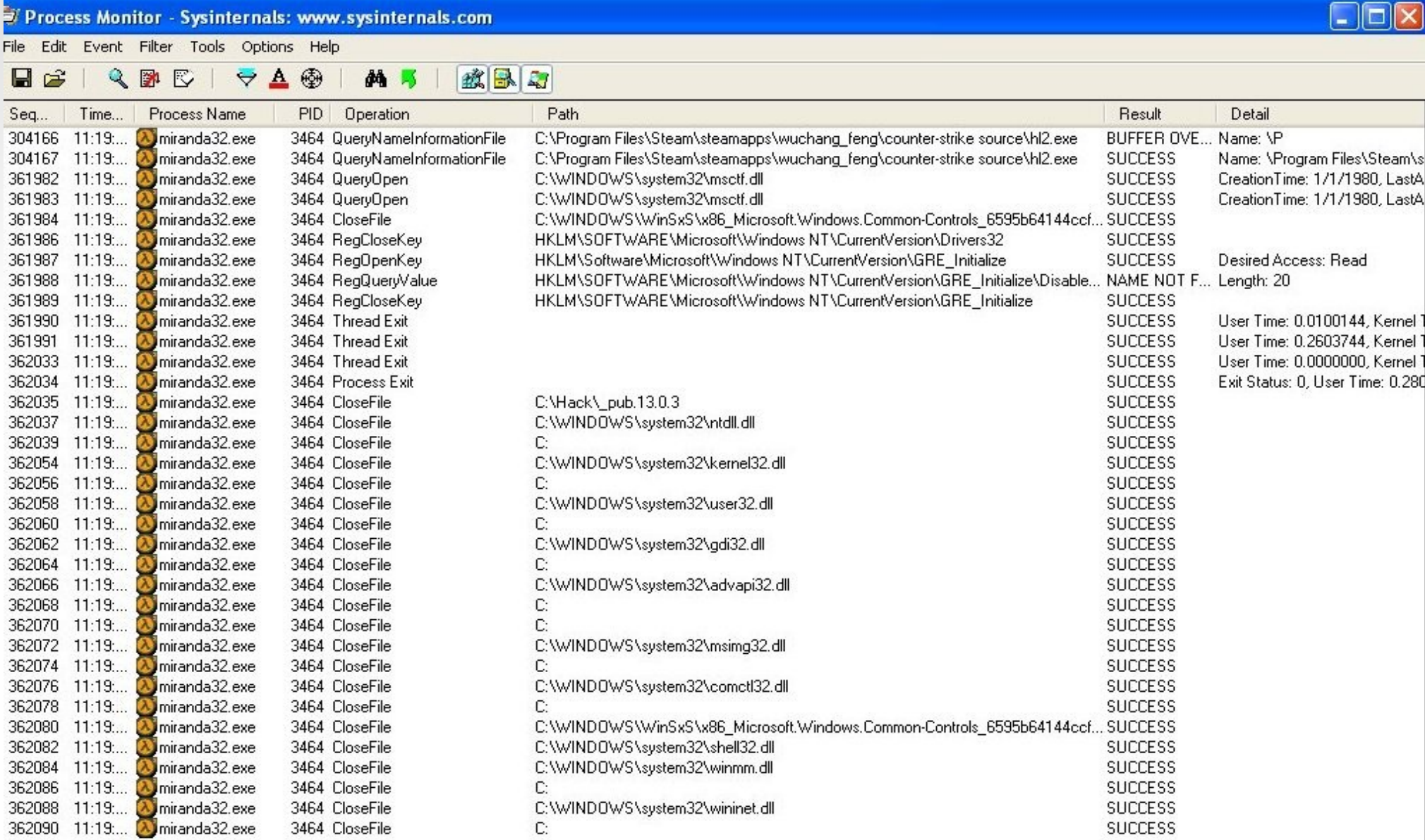


The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Event", "Filter", "Tools", "Options", and "Help". The toolbar contains various icons for file operations, search, and system functions. The main display area is a table with the following columns: "Seq...", "Time...", "Process Name", "PID", "Operation", "Path", "Result", and "Detail". Two rows of data are visible, both for the process "miranda32.exe" with PID 2568, performing the operation "QueryNameInformationFile" on the path "C:\WINDOWS\system32\notepad.exe". The first row shows a "BUFFER OVE..." result with detail "Name: \W...", and the second row shows a "SUCCESS" result with detail "Name: \WINDOWS\st...".

Seq...	Time...	Process Name	PID	Operation	Path	Result	Detail
16142	11:04:...	miranda32.exe	2568	QueryNameInformationFile	C:\WINDOWS\system32\notepad.exe	BUFFER OVE...	Name: \W/
16143	11:04:...	miranda32.exe	2568	QueryNameInformationFile	C:\WINDOWS\system32\notepad.exe	SUCCESS	Name: \WINDOWS\st



# Found it

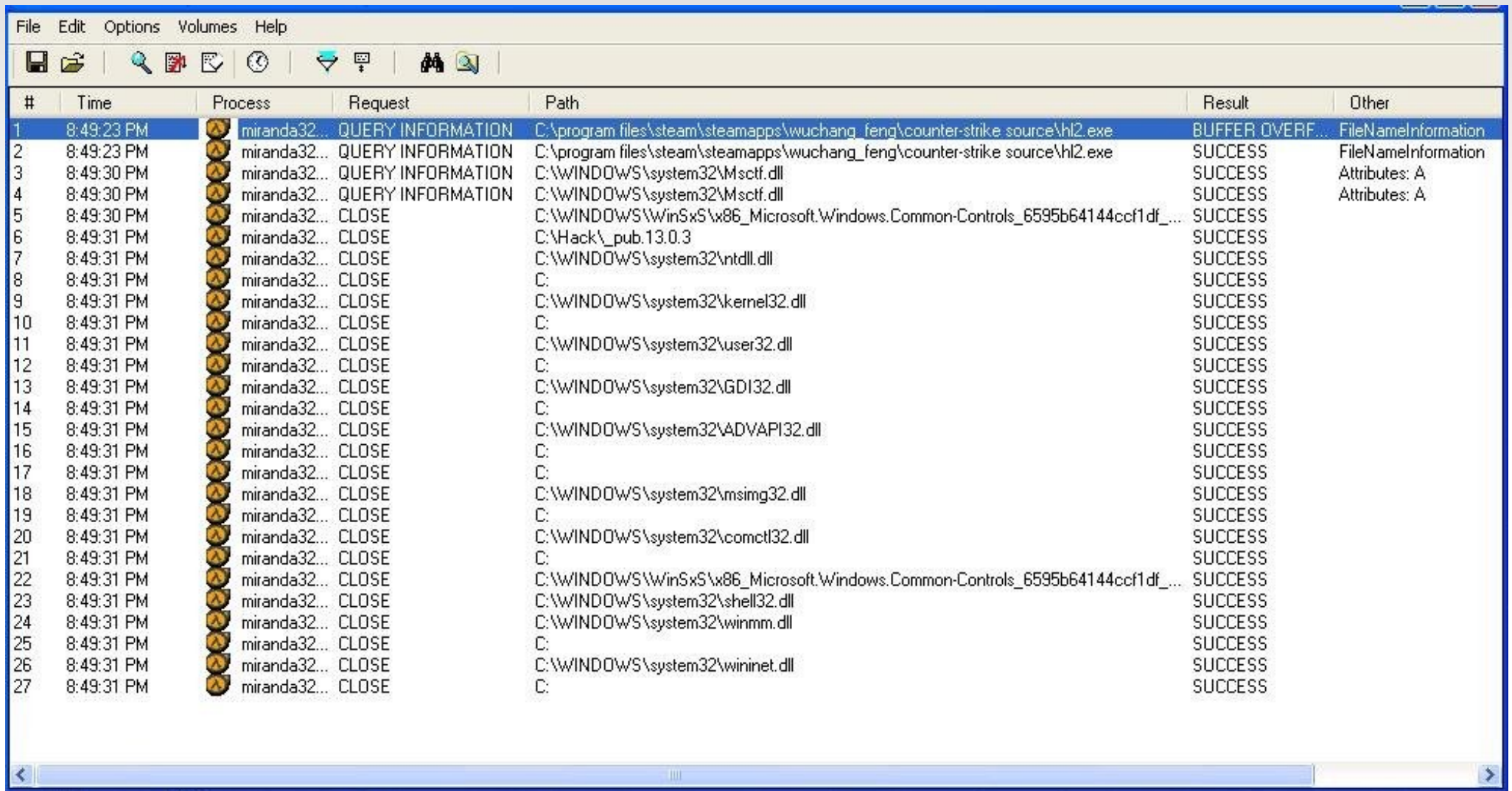


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

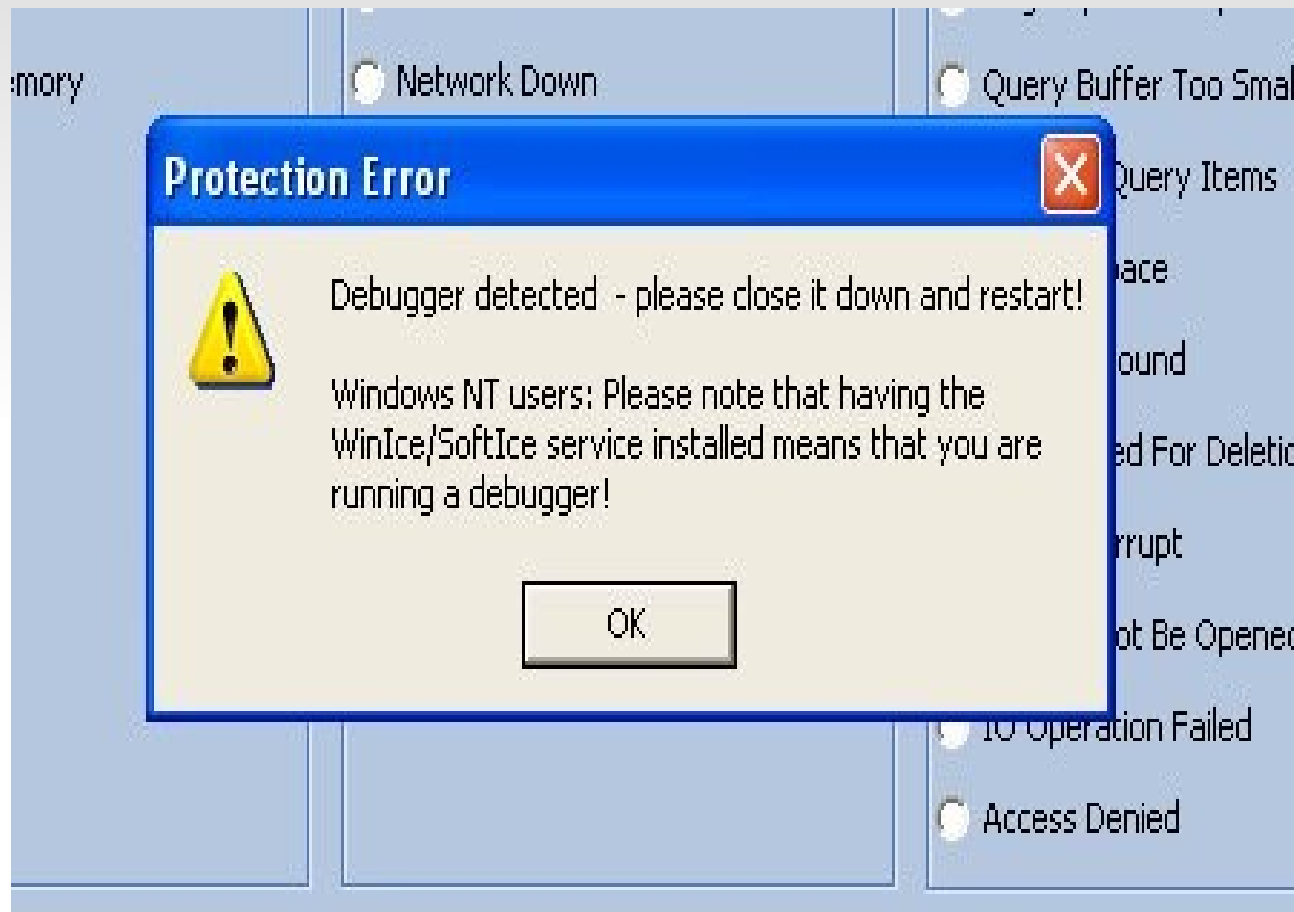
Seq...	Time...	Process Name	PID	Operation	Path	Result	Detail
304166	11:19:...	miranda32.exe	3464	QueryNameInformationFile	C:\Program Files\Steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	BUFFER OVE...	Name: \P
304167	11:19:...	miranda32.exe	3464	QueryNameInformationFile	C:\Program Files\Steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	SUCCESS	Name: \Program Files\Steam\s
361982	11:19:...	miranda32.exe	3464	QueryOpen	C:\WINDOWS\system32\msctf.dll	SUCCESS	CreationTime: 1/1/1980, LastA
361983	11:19:...	miranda32.exe	3464	QueryOpen	C:\WINDOWS\system32\msctf.dll	SUCCESS	CreationTime: 1/1/1980, LastA
361984	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf...	SUCCESS	
361986	11:19:...	miranda32.exe	3464	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32	SUCCESS	
361987	11:19:...	miranda32.exe	3464	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
361988	11:19:...	miranda32.exe	3464	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\Disable...	NAME NOT F...	Length: 20
361989	11:19:...	miranda32.exe	3464	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
361990	11:19:...	miranda32.exe	3464	Thread Exit		SUCCESS	User Time: 0.0100144, Kernel T
361991	11:19:...	miranda32.exe	3464	Thread Exit		SUCCESS	User Time: 0.2603744, Kernel T
362033	11:19:...	miranda32.exe	3464	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel T
362034	11:19:...	miranda32.exe	3464	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.280
362035	11:19:...	miranda32.exe	3464	CloseFile	C:\Hack\_pub.13.0.3	SUCCESS	
362037	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
362039	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362054	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
362056	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362058	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\user32.dll	SUCCESS	
362060	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362062	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\gdi32.dll	SUCCESS	
362064	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362066	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
362068	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362070	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362072	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\msimg32.dll	SUCCESS	
362074	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362076	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS	
362078	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362080	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf...	SUCCESS	
362082	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	
362084	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\winmm.dll	SUCCESS	
362086	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362088	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\wininet.dll	SUCCESS	
362090	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	

# Filemon/Regmon



#	Time	Process	Request	Path	Result	Other
1	8:49:23 PM	miranda32...	QUERY INFORMATION	C:\program files\steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	BUFFER OVERF...	FileNameInformation
2	8:49:23 PM	miranda32...	QUERY INFORMATION	C:\program files\steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	SUCCESS	FileNameInformation
3	8:49:30 PM	miranda32...	QUERY INFORMATION	C:\WINDOWS\system32\Mscf.dll	SUCCESS	Attributes: A
4	8:49:30 PM	miranda32...	QUERY INFORMATION	C:\WINDOWS\system32\Mscf.dll	SUCCESS	Attributes: A
5	8:49:30 PM	miranda32...	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_...	SUCCESS	
6	8:49:31 PM	miranda32...	CLOSE	C:\Hack\_pub.13.0.3	SUCCESS	
7	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
8	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
9	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
10	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
11	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\user32.dll	SUCCESS	
12	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
13	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\GDI32.dll	SUCCESS	
14	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
15	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\ADVAPI32.dll	SUCCESS	
16	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
17	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
18	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\msimg32.dll	SUCCESS	
19	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
20	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\comctl32.dll	SUCCESS	
21	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
22	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_...	SUCCESS	
23	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\shell32.dll	SUCCESS	
24	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\winmm.dll	SUCCESS	
25	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
26	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\wininet.dll	SUCCESS	
27	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	

# Holodeck





# Standard MS C Library

hl2h - Holodeck Enterprise Edition

File Session Application Log Tools View Help

Welcome to Holodeck **miranda32.exe Log - 3432(All Threads)** **Faults - 3432(All Threads)**

TimeStamp	Thread	Category	Dll	Function	Return Value	Error Code	Exception
06/10/2007 14:11:48:963	3512	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL	ERROR_SUCCESS	
⊕ 06/10/2007 14:11:48:963	3512	MEMORY	kernel32.dll	LocalAlloc	1715592	ERROR_SUCCESS	
⊕ 06/10/2007 14:11:48:963	3512	REGISTRY	advapi32.dll	RegOpenKeyExA	0	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	REGISTRY	advapi32.dll	RegQueryValueExA	2	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	REGISTRY	advapi32.dll	RegQueryValueExA	2	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	REGISTRY	advapi32.dll	RegQueryValueExA	2	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	REGISTRY	advapi32.dll	RegCloseKey	0	ERROR_SUCCESS	
⊕ 06/10/2007 14:11:48:973	3512	MEMORY	kernel32.dll	LocalAlloc	1723352	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1723400	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL	ERROR_SUCCESS	
⊕ 06/10/2007 14:11:48:973	3512	MEMORY	kernel32.dll	LocalAlloc	1653112	ERROR_SUCCESS	
⊕ 06/10/2007 14:11:48:973	3512	MEMORY	kernel32.dll	LocalFree	NULL	ERROR_SUCCESS	
⊕ 06/10/2007 14:11:48:973	3512	MEMORY	kernel32.dll	LocalAlloc	1724536	ERROR_SUCCESS	
⊕ 06/10/2007 14:11:48:973	3512	MEMORY	kernel32.dll	LocalAlloc	1653112	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL	ERROR_SUCCESS	

C:\Hack\\_pub.13.0.3\miranda32.exe - Process 3432

Terminated Entries: 5159 Visible: 5159

limits



# Windows Socket API

h12h - Holodeck Enterprise Edition

File Session Application Log Tools View Help

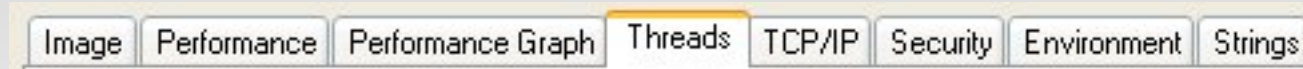
Welcome to Holodeck miranda32.exe Log - 3432(All Threads) Faults - 3432(All Threads)

TimeStamp	Thread	Category	Dll	Function	Return Value	Error Code	Exception
06/10/2007 14:12:09:443	3512	PROCESS	kernel32.dll	DeleteCriticalSection	NULL	ERROR_SUCCESS	
06/10/2007 14:12:09:443	3512	MEMORY	kernel32.dll	HeapFree	True	ERROR_SUCCESS	
06/10/2007 14:11:48:883	3512	DANGEROUS	msvcrt40.dll	wcscpy	1240096	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1723400	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1724728	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1726120	ERROR_SUCCESS	
06/10/2007 14:11:48:973	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1242456	ERROR_SUCCESS	
06/10/2007 14:12:09:192	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1239540	ERROR_SUCCESS	
06/10/2007 14:12:09:222	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1240720	ERROR_SUCCESS	
06/10/2007 14:12:09:242	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1243792	ERROR_SUCCESS	
06/10/2007 14:12:09:252	3512	DANGEROUS	msvcrt40.dll	wcsncpy	1243792	ERROR_SUCCESS	
06/10/2007 14:11:46:910	3512	NETWORK	ws2_32.dll	WSAStartup	0	ERROR_SUCCESS	
06/10/2007 14:11:46:...	3512	DANGEROUS	kernel32.dll	lstrcpYA	1244540	ERROR_FILE_NOT_FOUND	
06/10/2007 14:11:46:...	3512	DANGEROUS	kernel32.dll	lstrcpYA	1244797	ERROR_FILE_NOT_FOUND	
06/10/2007 14:11:46:...	3512	MEMORY	kernel32.dll	GetProcAddress	1907101736	ERROR_FILE_NOT_FOUND	
06/10/2007 14:11:46:...	3512	MEMORY	kernel32.dll	GetProcAddress	1907047936	ERROR_FILE_NOT_FOUND	
06/10/2007 14:11:46:...	3512	MEMORY	kernel32.dll	GetProcAddress	1907070521	ERROR_FILE_NOT_FOUND	
06/10/2007 14:11:46:...	3512	MEMORY	kernel32.dll	GetProcAddress	1907048554	ERROR_FILE_NOT_FOUND	

C:\Hack\\_pub.13.0.3\miranda32.exe - Process 3432 Terminated Entries: 5159 Visible: 5159

Limits

# Process Explorer



- Another Sysinternals program
- The threads
  - Doesn't appear to create a thread in the game or game launcher
- Nothing useful in strings

# Stack During Load

miranda32.exe: 3968 Properties

Image Performance Performance Graph **Threads** TCP/IP Security Environment Strings

CPU	CSwitch Delta	Start Address
4		miranda32.exe+0x206ef
206		miranda32.exe+0x1000 ADVAPI32.dll!RegDeleteKeyW+0xfd

Did it even start?

This section of the file used to be encrypted

Thread ID: 3988  
Start Time: 9:22:27 AM  
State: Wait:UserRe  
Kernel Time: 0:00:00.010  
User Time: 0:00:00.010  
Context Switches: 1,244  
Base Priority: 15  
Dynamic Priority: 15

**Stack for thread 3988**

0	ntdll.dll!KiFastSystemCallRet
1	kernel32.dll!WaitForSingleObject+0x12
2	miranda32.exe+0x21fe8
3	miranda32.exe+0x209f4
4	kernel32.dll!GetModuleFileNameA+0x1b4

Copy OK

# Playing Around

- Post initial load
  - No obvious debugger detection but program will exit stepping through or resuming the process.
  - runs kernel32, user32, ntdll, and other OS modules.

CPU - thread 00000EC4, module miranda3

Address	Hex dump	Disassembler
00423083	56	PUSH ESI
00423084	8BF0	MOV ESI, EAX
00423086	83C8 FF	OR EAX, FFFFFFFF
00423089	85F6	TEST ESI, ESI
0042308B	74 39	JE SHORT miranda3.004230C6
0042308D	BA FF000000	MOV EDX, 0FF
00423092	57	PUSH EDI
00423093	66:8B0E	MOV CX, WORD PTR DS:[ESI]
00423096	66:85C9	TEST CX, CX
00423099	74 2A	JE SHORT miranda3.004230C5
0042309B	23CA	AND ECX, EDX
0042309D	807C24 0C 00	CMP BYTE PTR DS:[ESI], 0
004230A2	74 0D	JE SHORT miranda3.004230C4
004230A4	83F9 61	CMP ECX, 61
004230A7	7C 08	JL SHORT miranda3.004230C4
004230A9	83F9 7A	CMP ECX, 7A
004230AC	7F 03	JG SHORT miranda3.004230C4
004230AE	83E9 20	SUB ECX, 20
004230B1	8BF8	MOV EDI, EAX
004230B3	23FA	AND EDI, ECX
004230B5	33F9	XOR EDI, ECX
004230B7	C1E8 08	SHR EAX, 8
004230BA	3304BD 80454200	XOR EAX, 80454200
004230C1	46	INC ESI
004230C2	46	INC ESI
004230C3	75 CE	JNZ SHORT miranda3.004230C6
004230C5	5F	POP EDI
004230C6	F7D0	NOT EAX
004230C8	5E	POP ESI
004230C9	C3	RETN
004230CA	83C8 FF	OR EAX, FFFFFFFF
004230CD	85D2	TEST EDX, EDX
004230CF	74 1F	JE SHORT miranda3.004230C6

Jump is taken  
00423093=miranda3.00423093

Address Hex dump Disassembler  
00425000 0000 ADD BYTE

Context menu options:  
Backup  
Copy  
Binary  
Assemble Space  
Label :  
Comment ;  
Breakpoint  
Run trace  
Follow Enter  
Go to  
Thread  
Follow in Dump  
Search for  
Find references to

Thread submenu:  
Main  
000008F0  
000009D8  
00000EC4



# Final

- Stealth
  - Likely not much
  - Named after common application
  - Encryption
- "Code section" decrypts itself if no debugger present
  - Attach debugger after program starts and view that section
  - Cannot get program to step through and generate/run it yet
  - Still "holes" in decrypted code