



Programa: Karuro Master.
Objetivo: Verlo Funcional.
Herramientas: OllyDBG, impresora para crear pdf.
Limitación: 120 minutos y Loader Inertia Software.
Página de descarga: <http://www.kakuro.com/>
Cracker: Apuromafo **Fecha creacion** 6/6/2008 **Fecha publicacion:** Agosto 2010

Contenido

Introducción:	2
¿Como se juega karuro?	2
Instalandolo	3
ERROR File Tampering "karuro Master.exe "	3
Referencias.....	4
Motivo.....	4
Idea 1	5
Pasamos el error:.....	7
Verdadero origen:	8
GENERIC.EXE	8
Referencias.....	8
Cambio para volverlo full	9
Jugando:	10
Proyección:	12
Despedida:.....	12
Anexo 1 "Record extraordinario casi sin jugarlo"	12

Introducción:

Muchos cariños a mi novia , que si no hubiera sido por ella, jamás hubiera conocido este juego

A 2 años libero este escrito, se me había olvidado compartirlo .
En aquel tiempo chateaba con marciano mientras se despedia le comente la hazaña,

```
marcianito: nos vemos mafo
yo: okis
vere si escribo sobre un
juego
se llama kakuro master
marcianito: ah dale, cuando lo
tengas mandalo a la lista
yo: sip
xD
```

Creo que es mejor Presentar estas historias y que no queden como recuerdo, esta historia es del año 2008, saludos cordiales, esperando que lo miren de forma educacional.

marcianito está desconectado/a. Los mensajes que envíes se entregarán cuando marcianito se conecte.

Quando termine de escribir, marciano se fue, no alcance a avisarle

¿Como se juega karuro?

Fuente <http://usuarios.lycos.es/sudoku/noticias-sudoku.htm>

Unas reglas muy fáciles.

Jugar al Kakuro no exige ser un genio de las matemáticas. Las reglas son muy simples. El objetivo de este juego de lógica consiste en colocar números del 1 al 9 en columnas compuestas de dos a nueve celdas vacías, que se sitúan horizontal y verticalmente a lo largo de una cuadrícula. La suma de cada columna de cifras debe igualar el número clave que aparece en las celdas oscurecidas, divididas en dos por líneas diagonales. Estos números clave se sitúan bien arriba (para los problemas o columnas verticales), bien a la izquierda (para los horizontales). No se puede usar un número más de una vez en la misma columna, de tal manera que si la cifra clave es el 4 y tenemos una columna con dos celdas, los números requeridos serán 1 y 3, nunca 2 y 2.

Por lo tanto, un buen regate para sortear la desesperación y encarar la victoria consiste en recordar que hay ciertas combinaciones que se repiten siempre. Por ejemplo, si el número clave es 16 y tiene solo dos celdas, no se puede usar 8 y 8 porque contraviene las reglas. Por lo tanto, la única respuesta es 7 y 9. Lo mismo con la cifra 11 y una columna con cuatro celdas. La única manera posible de salir del embrollo reside en utilizar los números 1, 2, 3 y 5.

Con esta ayuda y la paciencia de un santo, todo el mundo podrá vencer a este terrible contrincante.

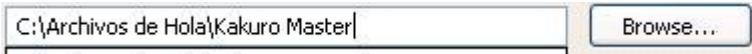
Ahora que se saben las reglas, suerte.

Instalandolo

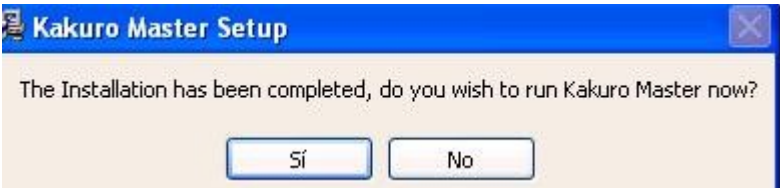
Comienzo con instalador tipo NSIS



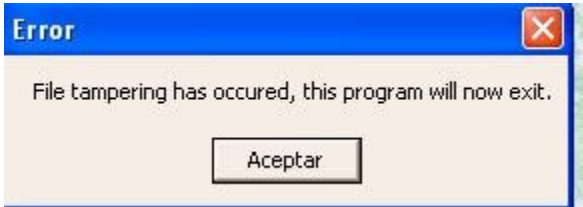
Coloco el nombre de la ruta



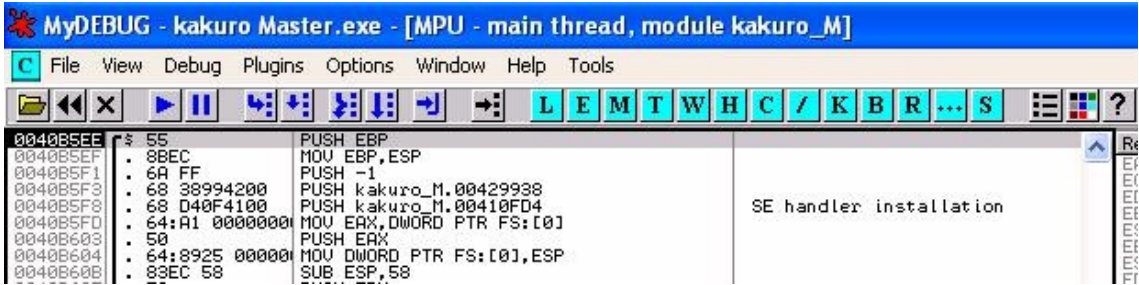
Y al terminar me pregunta si quiero jugar
Pero me muestra el siguiente error, y con esto comienza mi historia



ERROR File Tampering "karuro Master.exe "



Quiero jugar, Depuramos para investigar, El programa esta sin empacar:



Referencias

```
ASCII "%s/html/start.htm"
ASCII "%s/html/end.htm"
ASCII "mailto"
ASCII "Error"
ASCII "File tampering has occured, this program will now exit."
ASCII "Error"
ASCII "A demo error has happened, this program will now exit."
ASCII "Buy"
ASCII "Buy this Game"
ASCII "You will now be taken to our online store, this will open in a new browser window."
ASCII "http://www.inertiasoftware.com/onlinestore.php?game=%s"
ASCII "www.inertiasoftware.com"
ASCII "c:\program files\internet explorer\iexplore.exe"
ASCII "paypal"
ASCII "Paypal Page"
ASCII "You will now be taken to a paypal page, this will open in a new browser window."
ASCII "http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside"
ASCII "www.inertiasoftware.com"
ASCII "c:\program files\internet explorer\iexplore.exe"
ASCII "support"
ASCII "Buy this Game"
ASCII "You will now be taken to our support page, this will open in a new browser window."
ASCII "http://www.inertiasoftware.com/support.php"
ASCII "www.inertiasoftware.com"
ASCII "c:\program files\internet explorer\iexplore.exe"
ASCII "inertia"
ASCII "Buy this Game"
ASCII "You will now be taken to inertiasoftware.com, this will open in a new browser window."
ASCII "http://www.inertiasoftware.com"
ASCII "www.inertiasoftware.com"
ASCII "c:\program files\internet explorer\iexplore.exe"
ASCII "try"
ASCII "generic.exe"
ASCII "open"
ASCII "exit"
ASCII "<!--timeleft-->"
ASCII "%s/html/temp"
ASCII "<!--timeleft--><FONT COLOR='FF0000'>Your trial period has expired<FONT>"
ASCII "<!--timeleft--><FONT COLOR='FF0000'>You have %d Minutes remaining<FONT>"
ASCII "<!--timeleft-->You have %d Minutes remaining"
ASCII "%s/html/temp"
ASCII "%s/html/start.htm"
ASCII "%c"
```

Entro a la primera rutina y coloco analizar,

```
00401F2F 90 NOP
00401F30 81EC 00020000 SUB ESP,200
00401F36 33C9 XOR EAX,EAX
00401F38 8D5424 00 LEA EDI,DWORD PTR SS:[ESP]
00401F3C 53 PUSH EBX
00401F3D 8B09 MOV EBX,ECX
00401F3F 56 PUSH ESI
00401F40 57 PUSH EDI
00401F41 8B7B 5C MOV EDI,DWORD PTR DS:[EBX+5C]
00401F44 83C9 FF OR ECX,FFFFFFFF
00401F47 C643 64 00 MOV BYTE PTR DS:[EBX+64],0
00401F4B F2AE REPNE SCAS BYTE PTR ES:[EDI]
00401F4D F7D1 NOT ECX
00401F4F 2BF9 SUB EDI,ECX
00401F51 8BC1 MOV EAX,ECX
00401F53 8BF7 MOV ESI,EDI
00401F55 8BFA MOV EDI,EDX
00401F57 C1E9 02 SHR ECX,2
00401F5A F3A6 REP MOVS DWORD PTR ES:[EDI],DWORD PTR D
00401F5C 8BC8 MOV ECX,EAX
00401F5E 83E1 03 AND ECX,3
00401F61 F3A4 REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:
00401F63 8D4C24 0C LEA ECX,DWORD PTR SS:[ESP+C]
00401F67 51 PUSH ECX
00401F68 83C4 04 ADD ESP,4
00401F6D 83F8 02 CMP EAX,2
00401F70 75 25 JNZ SHORT kakuro_M.00401F9A
00401F75 6A 00 PUSH 0
00401F77 68 84054300 PUSH kakuro_M.00430584
00401F7C 68 4C054300 PUSH kakuro_M.0043054C
00401F81 8BCB MOV ECX,EBX
00401F83 E8 30B00100 CALL kakuro_M.004107B8
00401F88 6A 00 PUSH 0
00401F8A FF15 44744200 CALL DWORD PTR DS:[&USER32.PostQuitMes
00401F90 5F POP EDI
00401F91 5E POP ESI
00401F92 5D POP EDI
00401F93 81C4 00020000 ADD ESP,200
00401F94 73 RETN
ASCII "Error"
ASCII "File tampering has occured, this program will now exit."
ExitCode = 0
PostQuitMessage
```

Me posiciono al comienzo, para ver quien lo llama.

00401FB2 | . 6A 00 | PUSH

Local call from 00401CB2

Copy pane to clipboard

Go to CALL from 00401CB2

Address	Hex	dump
00401CB2 . 6A 00 PUSH		

Y es claro que aparece un mensaje que no veo, no veo el start.

```
00401C90 . C/4424 18 0000 MOV DWORD PTR SS:[ESP+18],0
00401C98 . E8 63F3FFFF CALL kakuro_M.00401000
00401C9D . 50 PUSH EAX
00401C9E . 8D4C24 0C LEA ECX,DWORD PTR SS:[ESP+C]
00401CA2 . 68 F8044300 PUSH kakuro_M.004304F8
00401CA7 . 51 PUSH ECX
ASCII "%s/html/start.htm"
00401CA8 . E8 EC7C0100 CALL kakuro_M.00419999
00401CAD . 83C4 0C ADD ESP,0C
00401CB0 . 8BCE MOV ECX,ESI
00401CB2 . E8 79020000 CALL kakuro_M.00401F30
00401CB7 . 8A46 64 MOV AL,BYTE PTR DS:[ESI+64]
00401CBA . 84C0 TEST AL,AL
00401CBC . 75 09 JNZ SHORT kakuro_M.00401CC7
00401CBE . A0 204A4300 MOV AL,BYTE PTR DS:[434A20]
00401CC3 . 84C0 TEST AL,AL
00401CC5 . 74 18 JE SHORT kakuro_M.00401CDF
00401CC7 . E8 34F3FFFF CALL kakuro_M.00401000
00401CCC . 50 PUSH EAX
00401CCD . 8D5424 0C LEA EDX,DWORD PTR SS:[ESP+C]
00401CD1 . 68 E8044300 PUSH kakuro_M.004304E8
00401CD6 . 52 PUSH EDX
ASCII "%s/html/end.htm"
```

Motivo

Todo esto ocurre porque uso firefox como navegador.
Y el programa debería tener Internet explorer Pero bueno.

50	PUSH EAX	
804C24 0C	LEA ECX,DWORD PTR SS:[ESP+C]	
68 F8044300	PUSH kakuro_M.004304F8	ASCII "%s/html/start.htm"
51	PUSH ECX	
E8 EC7C0100	CALL kakuro_M.00419999	
83C4 0C	ADD ESP,0C	
8BCE	MOV ECX,ESI	
E8 79020000	CALL kakuro_M.00401F30	
8A46 64	MOV AL,BYTE PTR DS:[ESI+64]	
84C0	TEST AL,AL	
75 09	JNZ SHORT kakuro_M.00401CC7	
A0 204A4300	MOV AL,BYTE PTR DS:[434A20]	
84C0	TEST AL,AL	
74 18	JE SHORT kakuro_M.00401CDF	
E8 34F3FFFF	CALL kakuro_M.00401000	
50	PUSH EAX	
8D5424 0C	LEA EDX,DWORD PTR SS:[ESP+C]	
68 E8044300	PUSH kakuro_M.004304E8	ASCII "%s/html/end.htm"
52	PUSH EDX	
E8 BD7C0100	CALL kakuro_M.00419999	
83C4 0C	ADD ESP,0C	
804C24 08	LEA ECX,DWORD PTR SS:[ESP+8]	
E8 080B0000	CALL kakuro_M.004027F0	

Idea 1

Comenzamos a hacer los cambios suponiendo que es la ruta

```
j address
I "C:\Archivos de Hola\Kakuro Master\files\html\start.htm"
RN to kakuro_M.0041EBC8 from kakuro_M.0041EBA2
```

porque estaba con los slach al revés

La ruta era esta



Teniamos:

0	TEST AL,AL	
09	JNZ SHORT kakuro_M.00401CC7	
204A4300	MOV AL,BYTE PTR DS:[434A20]	
0	TEST AL,AL	
18	JE SHORT kakuro_M.00401CDF	
34F3FFFF	CALL kakuro_M.00401000	
	PUSH EAX	
424 0C	LEA EDX,DWORD PTR SS:[ESP+C]	
E8044300	PUSH kakuro_M.004304E8	ASCII "%s/html/end.htm"
	PUSH EDX	
BD7C0100	CALL kakuro_M.00419999	
4 0C	ADD ESP,0C	

Y AL tiene el manejo de la situación

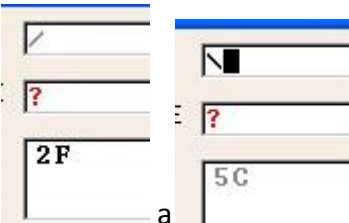
00401CBE	75 09	JNZ SHORT kakuro_M.00401CC7	
00401CC3	A0 204A4300	MOV AL,BYTE PTR DS:[434A20]	
00401CC5	84C0	TEST AL,AL	
00401CC7	74 18	JE SHORT kakuro_M.00401CDF	
00401CCC	E8 34F3FFFF	CALL kakuro_M.00401000	
00401CCD	50	PUSH EAX	
00401CD0	8D5424 0C	LEA EDX,DWORD PTR SS:[ESP+C]	
00401CD1	68 E8044300	PUSH kakuro_M.004304E8	ASCII "%s/html/end.htm"
00401CD6	52	PUSH EDX	
00401CD7	E8 BD7C0100	CALL kakuro_M.00419999	
00401CDC	83C4 0C	ADD ESP,0C	
00401CDF	804C24 08	LEA ECX,DWORD PTR SS:[ESP+8]	
00401CE3	E8 080B0000	CALL kakuro_M.004027F0	
00401CE8	51	PUSH ECX	
00401CE9	8BCC	MOV ECX,ESP	
00401CEB	896424 10	MOV DWORD PTR SS:[ESP+10],ESP	
00401CEF	50	PUSH EAX	
00401CF0	E8 E19D0100	CALL kakuro_M.0041BAD6	
00401CF5	8BCE	MOV ECX,ESI	
00401CF7	E8 04060000	CALL kakuro_M.004023D0	
00401CFC	8D4424 08	MOV EAX,DWORD PTR SS:[ESP+8]	
00401D00	6A 00	PUSH 0	
00401D02	6A 00	PUSH 0	
00401D04	6A 00	PUSH 0	
00401D06	6A 00	PUSH 0	
00401D08	50	PUSH EAX	
00401D09	8D4E 68	LEA ECX,DWORD PTR DS:[ESI+68]	
00401D0C	E8 8F0B0000	CALL kakuro_M.004028A0	

DS:[00434A20]=00
AL=00

Así que modifco

004304E0	09 4C 4C 4C 4C 4C 4B 00	.LLLLLK.
004304E8	25 73 5C 68 74 6D 6C 5C	%s\html\
004304F0	65 6E 64 2E 68 74 6D 00	end.htm.
004304F8	25 73 5C 68 74 6D 6C 5C	%s\html\
00430500	73 74 61 72 74 2E 68 74	start.ht
00430508	6D 00 00 00 6D 61 69 6C	m...mail
00430510	74 6F 00 00 41 20 64 65	to..A de
00430518	6D 6F 20 65 72 72 6F 72	no error
00430520	20 68 61 73 20 68 61 70	has hap

Desde



a

Quedando fixed

Quedando fixado

```

004304D8 . 50          PUSH EAX
004304D9 . E8 E19D0100 CALL kakuro_H
004304DA . 8BCE        MOV ECX, ESI
004304DB . E8 D4060000 CALL kakuro_H
004304DC . 8B4424 08   MOV EAX, DWORD
004304DD . 6A 00      PUSH 0
004304DE . 6A 00      PUSH 0
004304DF . 6A 00      PUSH 0
004304E0 . 50         PUSH EAX
004304E1 . 8D4E 68    LEA ECX, DWORD
004304E2 . E8 8F0B0000 CALL kakuro_H
004304E3 . 8D4C24 08  LEA ECX, DWORD
004304E4 . C74424 18 FF MOV DWORD PTR
004304E5 = kakuro_H.004304E8 (ASCII "%s\n")

```

Address	Hex dump	ASCII
004304D8	61 6D 00 00 FF FF FF FF	am...
004304E0	09 4C 4C 4C 4C 4C 48 00	.LLLLL
004304E8	25 73 5C 68 74 6D 6C 5C	%s\htm
004304F0	65 6E 64 2E 68 74 6D 00	end.ht
004304F8	25 73 5C 68 74 6D 6C 5C	%s\html
00430500	73 74 61 72 74 2E 68 74	start.ht
00430508	6D 00 00 00 6D 61 69 6C	m...mail
00430510	74 6F 00 00 41 20 64 65	to...A de
00430518	6D 6F 20 65 72 72 6F 72	m...error

Error

File tampering has occurred, this program will now exit.

Aceptar

kakuro Master_fixed.exe
Demo launcher
Inertia Soft LTD

Pasamos el error:

Como la rutina se ve que no es muy grande,no tengo mas más remedio que parcharlo

00401F2F	90	NOP
00401F30	B8 01000000	MOV EAX,1
00401F35	C3	RETN
00401F36	33C0	XOR EAX,EAX
00401F38	8D5424 00	LEA EDX,DWORD PTR SS:[ESP]
00401F3C	53	PUSH EBX
00401F3D	8BD9	MOV EBX,ECX
00401F3F	56	PUSH ESI
00401F40	57	PUSH EDI

Y el resultado esta a la vista



Pero corre el final, pero no tengo algun boton para jugar, solo de pagar o quitar el juego, menuda solucion. Analizo denuevo y veo que el valor de al, es importante y lo cambio a uno.

00401CA8	E8 EC7C0100	CALL kakuro_M.00419999	
00401CAD	83C4 0C	ADD ESP,0C	
00401CB0	8BCE	MOV ECX,ESI	
00401CB5	B0 01	MOV AL,1	
00401CB4	90	NOP	
00401CB5	90	NOP	
00401CB6	90	NOP	
00401CB7	8A46 64	MOV AL,BYTE PTR DS:[ESI+64]	
00401CBA	84C0	TEST AL,AL	
00401CBC	75 09	JNE SHORT kakuro_M.00401CC7	
00401CBE	A0 204A4300	MOV AL,BYTE PTR DS:[434A20]	
00401CC3	84C0	TEST AL,AL	
00401CC5	74 18	JE SHORT kakuro_M.00401CDF	
00401CC7	E8 34F3FFFF	CALL kakuro_M.00401000	
00401CCC	50	PUSH EAX	
00401CCD	8D5424 0C	LEA EDX,DWORD PTR SS:[ESP+C]	
00401CD1	B8 F0443000	PUSH kakuro_M.004304F8	ASCII "%s\html\start.htm"
00401CD6	52	PUSH EDX	
00401CD7	E8 BD7C0100	CALL kakuro_M.00419999	
00401CDB	83C4 0C	ADD ESP,0C	
00401CDF	8D4C24 08	LEA ECX,DWORD PTR SS:[ESP+8]	
00401CE3	E8 080B0000	CALL kakuro_M.004027F0	

Parchado denuevo para que el final sea el comienzo.



Muy bien, ahora deberia poder jugar



Pero aparece al continúe trial, lo pulso.y

Sospecho un poco. Miro que aparece en el navegador:

Verdadero origen:

```
il/start.htm#try
```

la palabra: “try”

La referencia try en karuro master.exe

00402298	PUSH	kakuro_M.0043058C	ASCII	"c:\program files\ir
004022F9	PUSH	kakuro_M.0043081C	ASCII	"try"
00402314	PUSH	kakuro_M.00430810	ASCII	"generic.exe"
0040232F	PUSH	kakuro_M.00430808	ASCII	"open"
00402385	PUSH	kakuro_M.00430820	ASCII	"exit"
00402434	PUSH	kakuro_M.00430838	ASCII	"<!--timeleft-->"

Luego dice una palabra "generic.exe"

Pues en la ruta hay un programa.

Pruebo abriéndolo y dice



Aqui nace realmente la referencia de entenderlo todo,

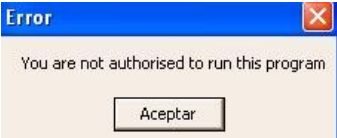
El programa principal envia un argumento a generic.exe y por eso se puede ejecutar,

Y miro ahora con mas detalle lo que dice



"Demo Launcher," por ende es solo un lanzador de otra app.

GENERIC.EXE



Ahora comenzamos a depurar para vencer a

Referencias

401085	PUSH	generic.0047A08C	ASCII	"initialising inertia engine - vws
401085	PUSH	generic.0047A080	ASCII	"config.cfg"
401299	MOV	EBX, generic.0047A194	ASCII	"kakuro"
4012D1	PUSH	generic.0047A18C	ASCII	"Error"
4012D6	PUSH	generic.0047A160	ASCII	"You are not authorised to run this program"
401307	PUSH	generic.0047A18C	ASCII	"Error"
40130C	PUSH	generic.0047A128	ASCII	"A demo error has heppened, this program will now exit."
401321	PUSH	generic.0047A18C	ASCII	"Error"
401326	PUSH	generic.0047A0F4	ASCII	"Your demo has expired, this program will now exit."
40133B	PUSH	generic.0047A18C	ASCII	"Error"
401340	PUSH	generic.0047A08C	ASCII	"File tampering has occured, this program will now exit."
401455	MOV	DWORD PTR SS:[ESP+30], generic.0047A194	ASCII	"KakuroWindow"
4014A2	PUSH	generic.0047A160	ASCII	"v_width"

También sale el tampering.y bueno .expired Llegando a

00401290	53	PUSH	EBX	
00401291	56	PUSH	ESI	
00401292	57	PUSH	EDI	
00401293	8B7C24 10	MOV	EDI, DWORD PTR SS:[ESP+10]	
00401297	8BF7	MOV	ESI, EDI	
00401299	8B 94A14700	MOV	EBX, generic.0047A194	ASCII "kakuro"
0040129E	> 8A10	MOV	DL, BYTE PTR DS:[EBX]	
004012A0	8A1E	MOV	BL, BYTE PTR DS:[ESI]	
004012A2	8AC9	MOV	CL, DL	
004012A4	8AD3	CMP	DL, BL	
004012A6	75 1E	JNZ	SHORT generic.004012C6	
004012A8	84C9	TEST	CL, CL	
004012AA	74 16	JE	SHORT generic.004012C2	
004012AC	8A50 01	MOV	DL, BYTE PTR DS:[EBX+1]	
004012AF	8A5E 01	MOV	BL, BYTE PTR DS:[ESI+1]	
004012B2	8AC9	MOV	CL, DL	
004012B4	8AD3	CMP	DL, BL	
004012B6	75 0E	JNZ	SHORT generic.004012C6	
004012B8	83C0 02	ADD	EBX, 2	
004012BB	83C6 02	ADD	ESI, 2	
004012BE	84C9	TEST	CL, CL	
004012C0	75 DC	JNZ	SHORT generic.0040129E	
004012C2	33C0	XOR	EBX, EBX	
004012C4	EB 05	JMP	SHORT generic.004012CB	
004012C6	1BC0	SBB	EBX, EBX	
004012C8	83D8 FF	SBB	EBX, -1	
004012CB	85C0	TEST	EBX, EBX	
004012CD	74 1A	JE	SHORT generic.004012E9	
004012CF	6A 00	PUSH	0	
004012D1	68 8CA14700	PUSH	generic.0047A18C	
004012D6	68 60A14700	PUSH	generic.0047A160	
004012D8	6A 00	PUSH	0	
004012D0	FF15 10A24600	CALL	DWORD PTR DS:[I<&USER32.MessageBoxA	Style = MB_OK!MB_APPLMODAL Title = "Error" Text = "You are not authorised to run this program" hOwner = NULL MessageBoxA
004012E3	5F	POP	EDI	
004012E4	5E	POP	ESI	
004012E7	5D	POP	EBX	

Llamado del call:

0040101B	. A3 DC9A4900	MOV DWORD PTR DS:[488ADC],EAX	
00401020	. E3 DB830000	CALL generic.00401900	
00401025	. FF15 4CA24600	CALL DWORD PTR DS:[<&WINMM.timeGetTime>]	WINMM.timeGetTime
00401028	. 50	PUSH EAX	
0040102C	. E8 438F0500	CALL generic.00459F74	
00401031	. 68 B4A04700	PUSH generic.0047A0B4	ASCII "log.txt"
00401036	. E8 45090000	CALL generic.00401980	
0040103B	. 83C4 08	ADD ESP,8	
0040103E	. 68 B0A04700	PUSH generic.0047A0B0	ASCII "1.0"
00401043	. 68 8CA04700	PUSH generic.0047A08C	ASCII "Initialising Inertia Engine - v%s"
00401048	. 6A 00	PUSH 0	
0040104A	. E8 91090000	CALL generic.004019E0	
0040104F	. 8B4C24 50	MOV ECX,DWORD PTR SS:[ESP+50]	
00401053	. 51	PUSH ECX	
00401054	. E8 37020000	CALL generic.00401290	
00401059	. 83C4 10	ADD ESP,10	
0040105C	. 84C0	TEST AL,AL	
0040105E	. 75 08	JNZ SHORT generic.00401068	
00401060	. 33C0	XOR EAX,EAX	
00401062	. 83C4 38	ADD ESP,38	
00401065	. C2 1000	RETN 10	
00401068	. E8 43010000	CALL generic.004011B0	
0040106D	. 85C0	TEST EAX,EAX	
0040106F	. 75 09	JNZ SHORT generic.0040107A	
00401071	. 83C8 FF	OR EAX,FFFFFFFF	
00401074	. 83C4 38	ADD ESP,38	
00401077	. C2 1000	RETN 10	
0040107A	. E8 319A0000	CALL generic.0040AAB0	
0040107F	. 8B15 048A4800	MOV EDI,DWORD PTR DS:[488AD4]	
00401085	. 68 80A04700	PUSH generic.0047A080	
0040108A	. 8B4A 10	MOV ECX,DWORD PTR DS:[EDI+10]	Arg1 = 0047A080 ASCII "config.cfg"
0040108D	. E8 3E8E0000	CALL generic.00409ED0	generic.00409ED0
00401092	. E8 A9030000	CALL generic.00401440	
00401097	. A1 D88A4800	MOV EAX,DWORD PTR DS:[488AD8]	
0040109C	. 8B00 D08A4800	MOV ECX,DWORD PTR DS:[488AD0]	
004010A2	. 5A	PUSH EAX	

Cambio para volverlo full

Anulo el cal

l haciendolo valer al, 1 parchando en el call o mas estetico: al comienzo de su rutina:

140104F	. 8B4C24 50	MOV ECX,DWORD PTR SS:[ESP+50].	
1401053	. 51	PUSH ECX	
1401054	B0 01	MOV AL,1	
1401056	90	NOP	
1401057	90	NOP	
1401058	90	NOP	
1401059	. 83C4 10	ADD ESP,10	
140105C	. 84C0	TEST AL,AL	
140105E	. 75 08	JNZ SHORT generic.00401068	
00401290	33C0	XOR EAX,EAX	
00401292	B0 01	MOV AL,1	
00401294	C3	RETN	
00401295	90	NOP	
00401296	90	NOP	
00401297	. 8BF7	MOV ESI,EDI	
00401299	. B8 94A14700	MOV EAX,generic.0047A194	ASCII "kakuro"
0040129E	. 8A10	MOV DL,BYTE PTR DS:[EAX]	
004012A0	. 8A1E	MOV BL,BYTE PTR DS:[ESI]	

generic_fix.exe

Guardar

Y guardo el cambio

Y terminó comenzando y sin limitación de tiempo,

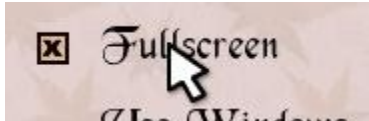


solo había que revisar este generic.exe y asi ver la pantalla principal.



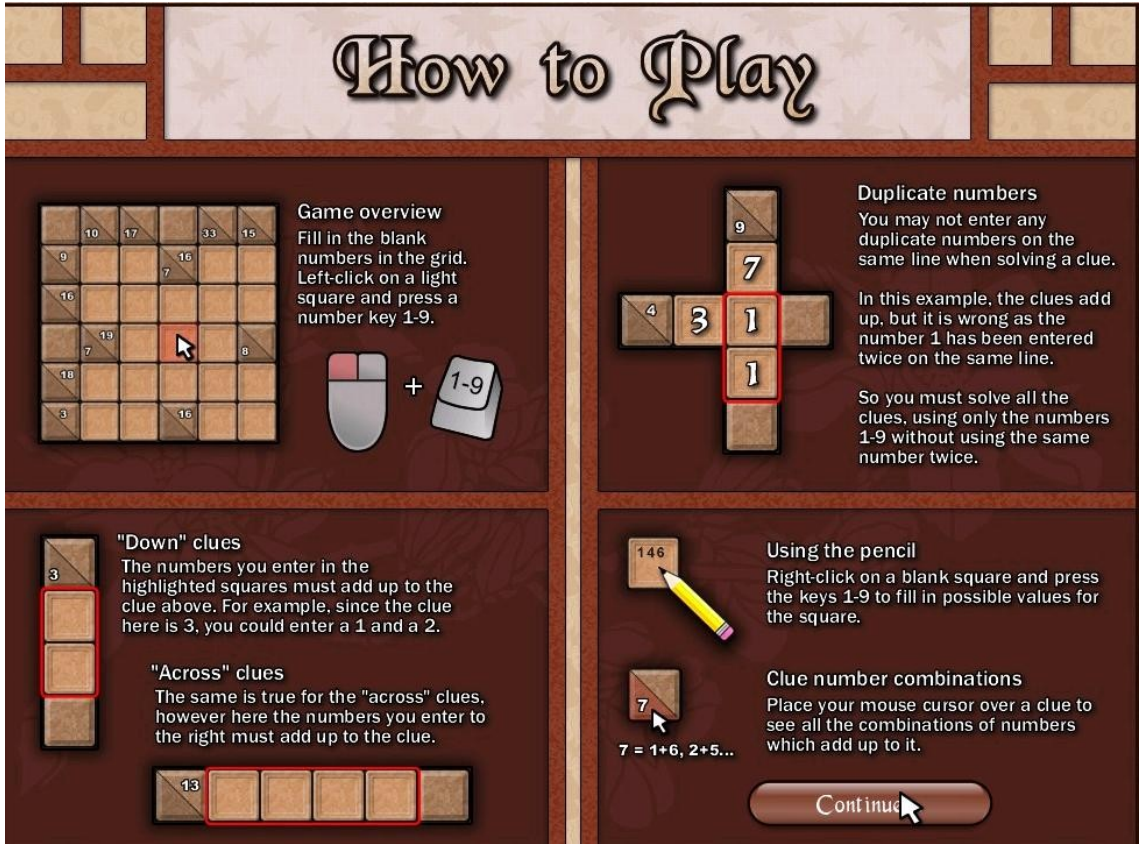
Jugando:


si pulsamos hint o solve, no entramos en el ranking Ahora en OPCIONES, cambio el




Para quienes no sepan jugar, también dice como jugar pero en ingles Mas o menos seria algo como :

El clic derecho ingresa el número definitivo Y el click izquierdo Puedes escribir las opciones posibles No deben existir números duplicados para obtener en suma, Y además tendrás en el numero que debes obtener, en la parte inferior, la clave de los valores posibles.




Al colocar play vemos:  si coloco el mouse en el numero veo la ayuda abajo

 Dice que 4 en 2 celdas, es igual a UNO mas TRES el DOS mas DOS no esta en las reglas, pues, que no puede ser sumado el mismo numero



Sigamos: coloco las 2 opciones con el mouse: Así que coloco 1 y 3 en las opciones Pero como es 3 abajo.



No puede ser igual pues la suma total debe ser tres, y no mayor.  aqui muestra que es 3 sobre 2 celdas es UNO mas DOS

Y mis opciones son 1 y 3, por lo tanto la opción a elegir es el numero 1 y asi se escribe el numero definitivo



Pues sumados debe dar 3 en las 2 celdas. Con ello puedo seguir completando.

Con el 1 resuelto, pues completo el 4 que comencé







12 over 2 squares = 3+9, 4+8, 5+7


luego el doce:

El 12 es 3+9, igual existen mas opciones, pero es la única con el numero 3





Y así avanzo y avanzo ,Colocando las opciones posibles



es = 1+3

Por ejemplo este 4 podía 1 2 4, y como la suma debe ser
pues aquí es 1 el valor que debo ingresar





para ver: Y de a poco se va completando

Y en 8 minutos aproximadamente termine, con las fotos y este escrito

Congratulations!

You have completed this kakuro puzzle in 08:26. You have earned a place on the scoreboard!

Cracklatinos

Enter

Ranking

1	Cracklatinos	3094
2	Anon	0

Proyección:

El loader ejecuta el programa principal, y lo derrotamos para ejecutar un juego , espero les haya gustado la historia.
También de la pagina principal hay otras aplicaciones y ayudas, todas pueden caer de la misma forma que fue presentado en este escrito, todas accediendo como loader buscando las referencias, parchando con mov al,1 al nivel de algún call.

Despedida:

Saludos Cordiales, Apuromafo
Dedicado a los integrantes de la Lista Crackslatinos
Y un saludo a la distancia a marciano quien algún día esperaba este escrito

Desde Chile, Apuromafo

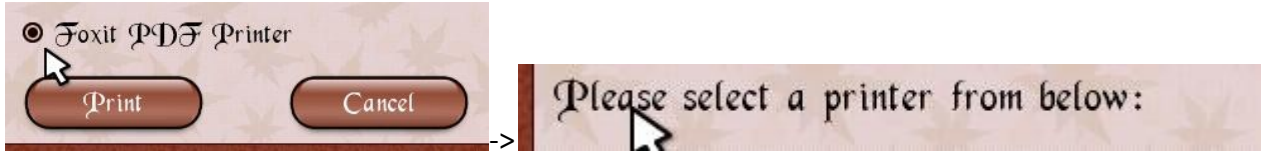
Anexo 1 "Record extraordinario casi sin jugarlo"

La idea era sorprender en el ranking, lo unico que necesitas es una impresora o para ahorrar hojas, una impresora tipo pdf, en este caso usare Foxit pdf printer

Vamos con el juego: Pulso play en la forma fácil



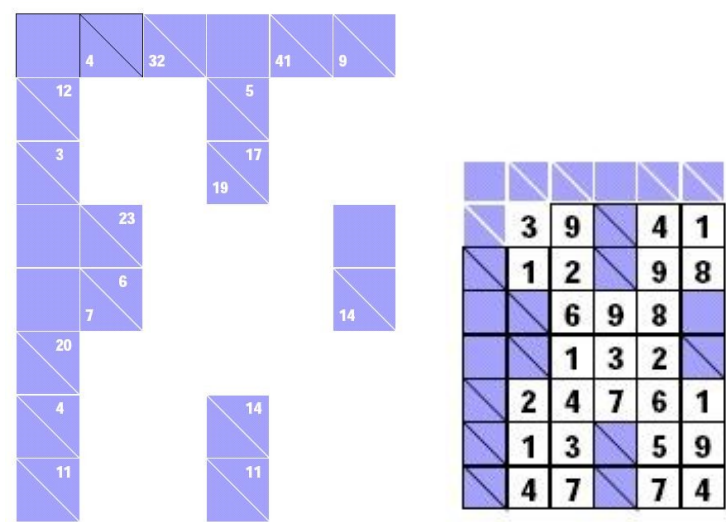
Ahora pulsa Pause: Pulsa el boton de Imprimir(print) , en este caso usare foxit pdf printer:



Y la parte importante de imprimir



Y tendrás esta imagen: Asi te dará la solución y ahora colocas "Resume"(continuar) y vas colocando los datos que están en el pdf.



Ahora si o si accederás al Ranking, normalmente si presionas solve, o hint, pues no entras en el ranking, y con esto, pues entras si o si, pues tienes la solución directamente sin presionar ayuda, pues puedes colocar el valor correcto que ahora esta en un impreso.