A Study on the Categorization of Webshell

Jae Chun, Lee(jclee@kisa.or.kr)
Agenda

• Part1 - Introduce Webshell

• Part2 - Advantage and disadvantage of WebShell Profiling

• Part3 – Criteria Categorization of WebShell
Hacking Trend

[Reference: John Pescatore, Security Analyst, Gartner Group]
What is Webshell?

• Backdoor program which is used for web hacking most commonly

• The first attack tool of hacker

• General, Easy, Convenience
What is Webshell?

- Backdoor program which is used for web hacking most commonly
- The first attack tool of hacker
- General, Easy, Convenience

- So, Webshell is important Indicator Of Compromise.
Review: The Pyramid of Pain (1/3)

This simple diagram shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them.

<From mandiant: The Pyramid of Pain>
Hashes are, by far, the highest confidence indicators.

Unfortunately, they are extremely susceptible to change (even accidentally).

Hashes are probably the least useful type of indicators.
TTPs are the expression of the attacker's training.

Retraining is probably the hardest thing you can do once, let alone continually.

This becomes so expensive that they have to question their commitment to attacking you. Win!
Webshell position
(in The Pyramid of Pain)

**Tools:** Software used by the adversary to accomplish their mission. Mostly this will be things they bring with them, rather than software or commands that may already be installed on the computer. This would include utilities designed to create malicious documents for spearphishing, backdoors used to establish C2 or password crackers or other host-based utilities they may want to use post-compromise.
Why webshell profiling is difficult?

- Text format
  - Easy to transform

- Open-Source program
  - Many attacker used
How can use webshell for profiling?

Attacker use similar variable name, comment, etc
-> it is a important fingerprint
How can use webshell for profiling?(2/2)

Attacker not use original Open-Source webshell. They use webshell changed which is similar the method of source code encoding, analysis disturbance, detection evasion, concealment method.
(Ex) WSO Webshell (1/2)

- WSO webshell
  - Login password: OOO
  - Normal url connection: error page
  - Related incidents: OO homepage
  - Regular expression substitution
(Ex) WSO Webshell (2/2)

• WSO webshell

- Login password: OOO
  By the fingerprint
- Normal url connection: error page
  By concealment method
- Related incidents: OO homepage
  By incidents
- Regular expression substitution
  By detection evasion
How to classify webshell

- By the language
- By function
- By the length of webshell source code
- By the method of source code encoding
- By detection evasion
- By analysis disturbance
- By file name
- By concealment method
- By the fingerprint and transformation of webshell
Classification by language

- PHP
- ASP
- ASPX
- JSP
- Perl
Classification by function

- System command execution
- Dynamic code injection
- File manipulation and download
- File upload
- DB-related functions
- Login
- Remote file include
- Back-connecting
- Sending Mail
- Brute force
- Forced moves URL
- Remote file download
- Etc.
(CF) Classification by function

- System command execution

<table>
<thead>
<tr>
<th>Function</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>shell_exec</td>
<td>unserialize</td>
</tr>
<tr>
<td>paththru</td>
<td>ssh2_exec</td>
</tr>
<tr>
<td>open</td>
<td>ssh1_exec</td>
</tr>
<tr>
<td>proc_lpopen</td>
<td>preg_replace</td>
</tr>
<tr>
<td>system</td>
<td>preg_replace</td>
</tr>
</tbody>
</table>

- Dynamic code injection

<table>
<thead>
<tr>
<th>Function</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>builtin_val, php_eval</td>
<td>call</td>
</tr>
<tr>
<td>create_function</td>
<td>unserialize</td>
</tr>
</tbody>
</table>
Classification by length

- Single line Webshell
- Html Injected single line Webshell
- Image file injected single line Webshell
- Small webshell
- Program type Webshell
By the method of source code encoding

- Base64
- Gzipinflat
- vbscript encoding
- Strtr
- Zend encoding
By detection evasion

- Cut the string
- Hex string display
- Magic Number insertion
- Regular expression substitution
(CF) By detection evasion

• Cut the string

```
<%set os=server.createobject("wsc"+"ri"+"pt.sh"+"ell")
```

Detection pattern: wscript.shell
By analysis disturbance

• Debug code removed
• Variable and function names randomization
By file name

- Use a semicolon
- Insert intermediate extension
By concealment method

- Display error page
- Parameters required
- Login feature
(EX) By concealment method

- Display error page / Login feature

Not Found

The requested URL was not found on this server.

Apache Server at 172.16.30.131 Port 80

Normal url access

If you are login
By the fingerprint and transformation of webshell

| file name            | Admin | C99 | phpspy | HP20 | Spidey | O6 | Webshell | Shelled | SmartShell | asp_shell | dback | privvy | Sim Attacker | doc | d0sya | r57 | ASPI | Spyd | md53 | 2 | JSP | FileBrowser | JspShell | JspFile | JspSpy | JspFile | Angel | Crystal | IShell | DSShell | Fatalshell |
|----------------------|-------|-----|--------|------|--------|----|----------|---------|------------|-----------|-------|--------|-------------|-----|-------|-----|------|------|------|---|----|-----------|---------|---------|--------|---------|-------|--------|--------|---------|---------|----------|
| ass.php.html.php.inc.php.txt |       |     |        |      |        |    |          |         |            |           |       |        |             |     |       |     |      |      |      |   |    |          |         |         |         |         |       |        |        |         |         |          |
| index.html           |       |     |        |      |        |    |          |         |            |           |       |        |             |     |       |     |      |      |      |   |    |          |         |         |         |         |       |        |        |         |         |          |
| index.php.txt        |       |     |        |      |        |    |          |         |            |           |       |        |             |     |       |     |      |      |      |   |    |          |         |         |         |         |       |        |        |         |         |          |
| m.php.gif            |       |     |        |      |        |    |          |         |            |           |       |        |             |     |       |     |      |      |      |   |    |          |         |         |         |         |       |        |        |         |         |          |
| newfile.php          |       |     |        |      |        |    |          |         |            |           |       |        |             |     |       |     |      |      |      |   |    |          |         |         |         |         |       |        |        |         |         |          |
Conclusion

• Criteria Categorization of WebShell

• In my case, make a DB from list of WebShell and find a hacker profile from DB
Thanks you

jcle@kisa.or.kr (Jae Chun, Lee)