27th ANNUAL
# FIRST CONFERENCE BERLIN
14 - 19 JUNE 2015

# UNIFIED SECURITY:
## IMPROVING THE FUTURE

27th ANNUAL FIRST CONFERENCE BERLIN 14-19 JUNE 2015

# A Study on the Categorization of Webshell

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

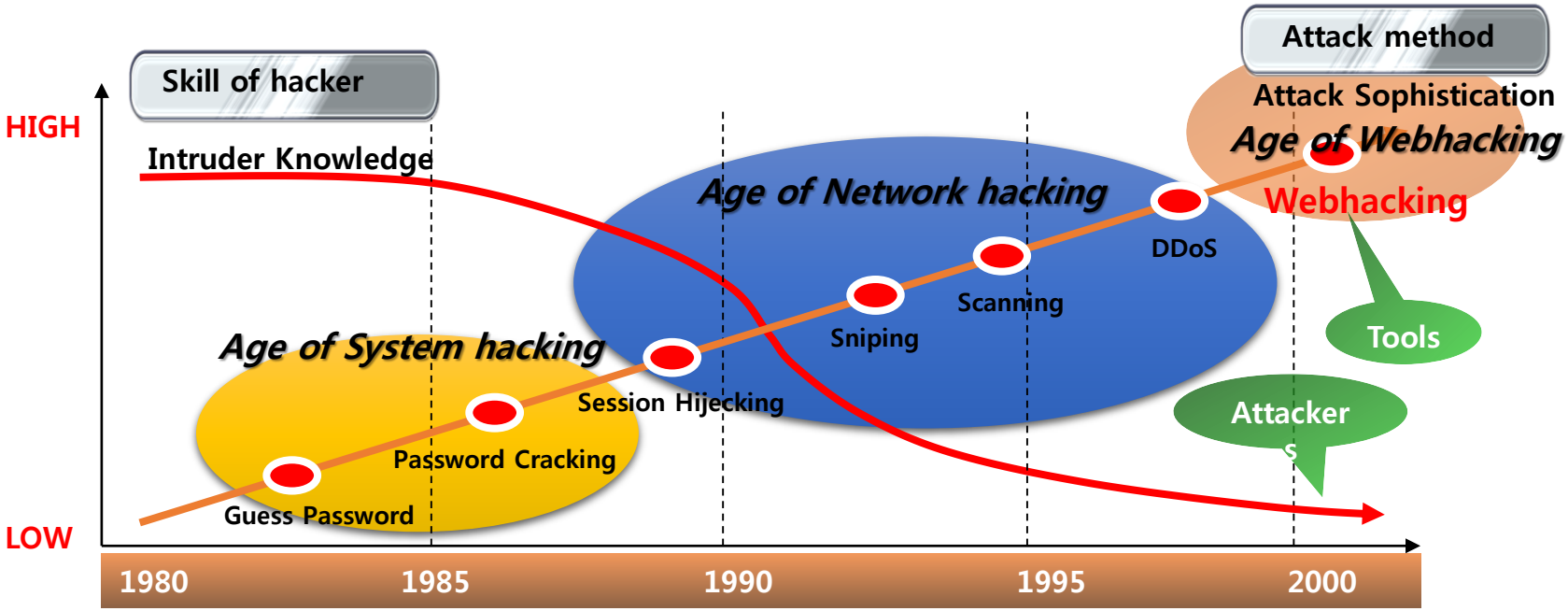
KISA KOREA INTERNET & SECURITY AGENCY

KrCERT/CC 인터넷 침해 대응 센터

# 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]

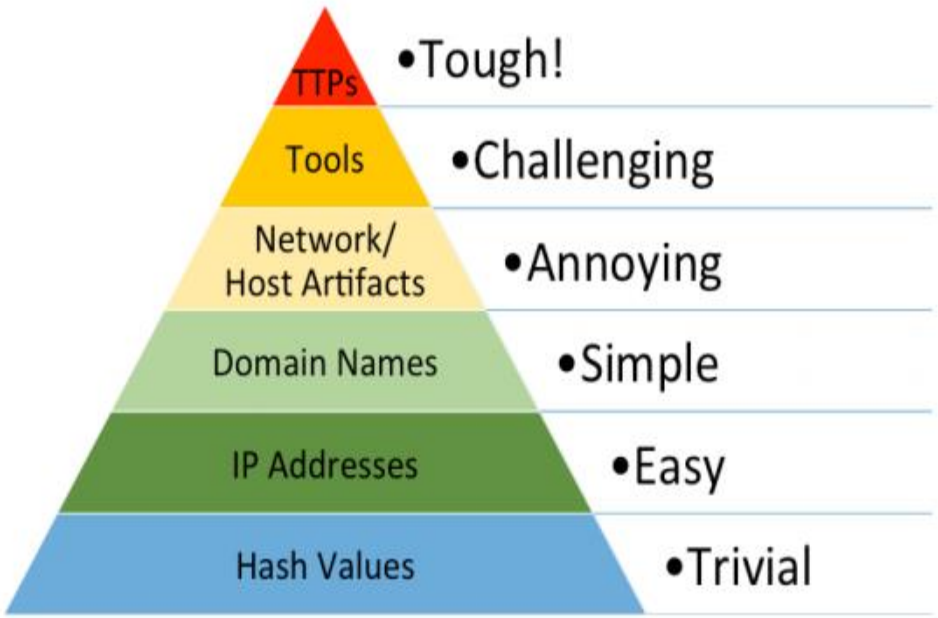
# What is Webshell?

- 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

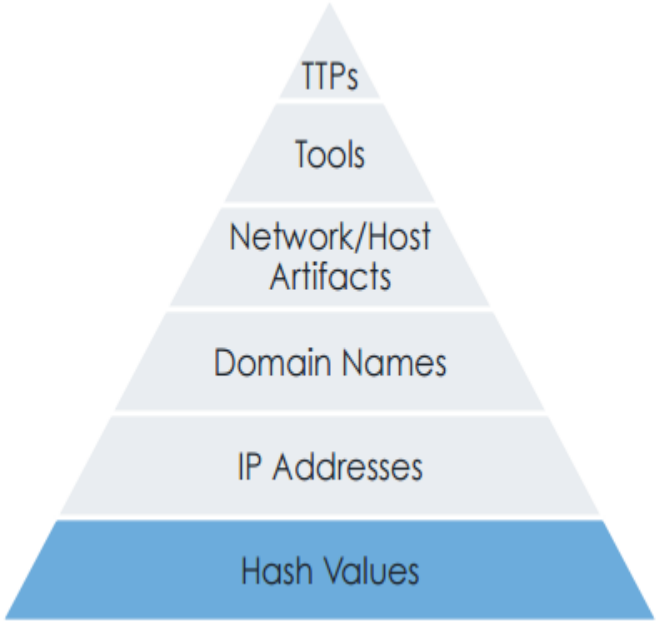
<From mandiant : The Pyramid of Pain>

# Review : The Pyramid of Pain(2/3)

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.

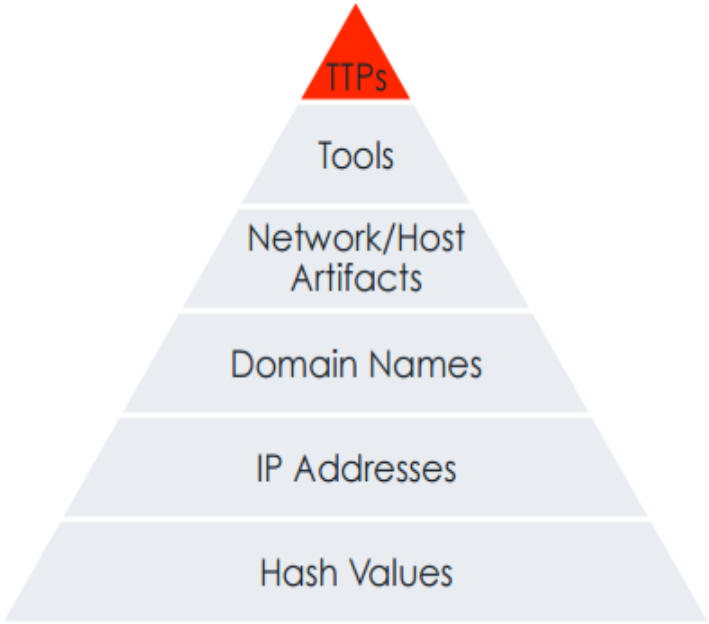


# Review : The Pyramid of Pain(3/3)

TTPs are the expression of the attacker's training.

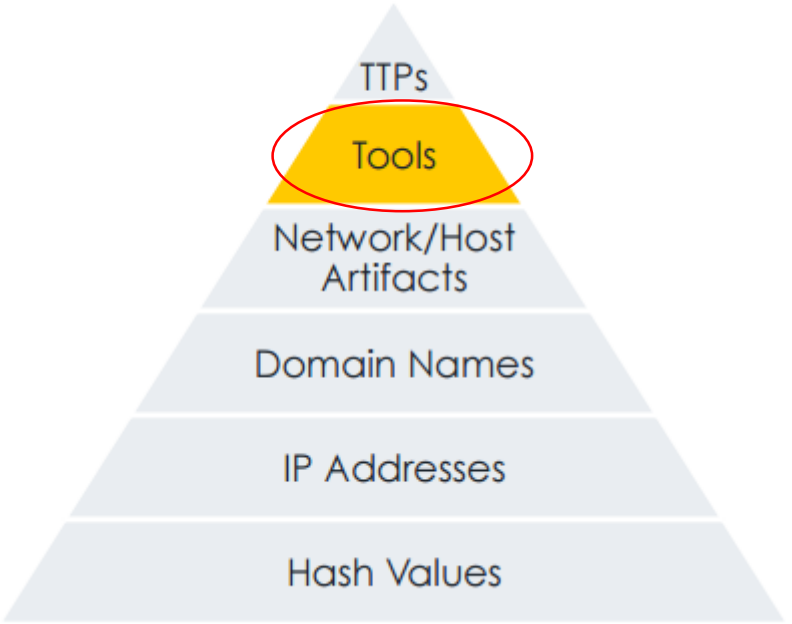
Retraining is probably the hardest thing you can do once, let alone continually.

This becomes so expensive that they have to question their commitment to attacking you. Win!

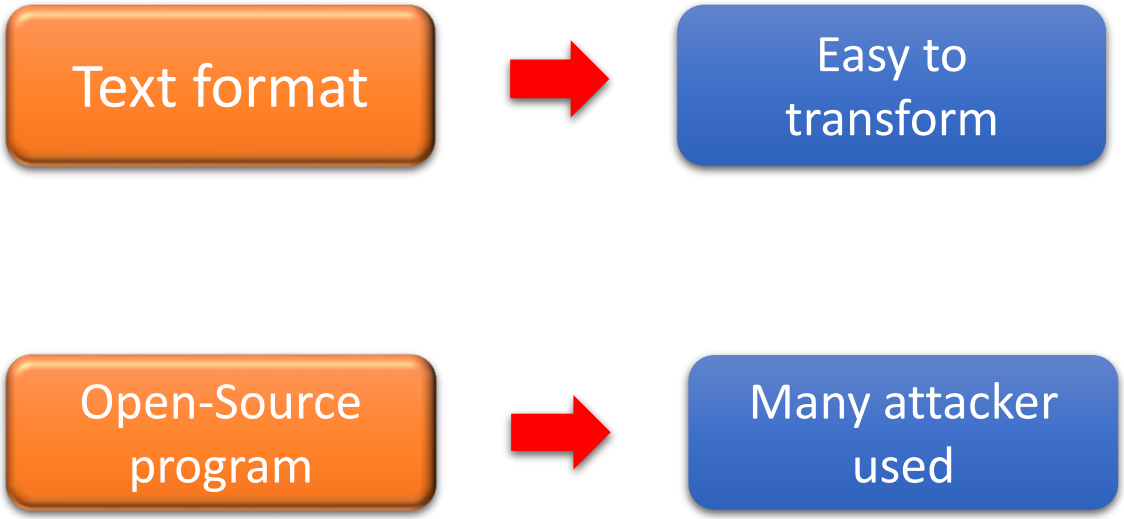


# Webshell position
## (in The Pyramid of Pain)

**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?



# How can use webshell for profiling?(1/2)

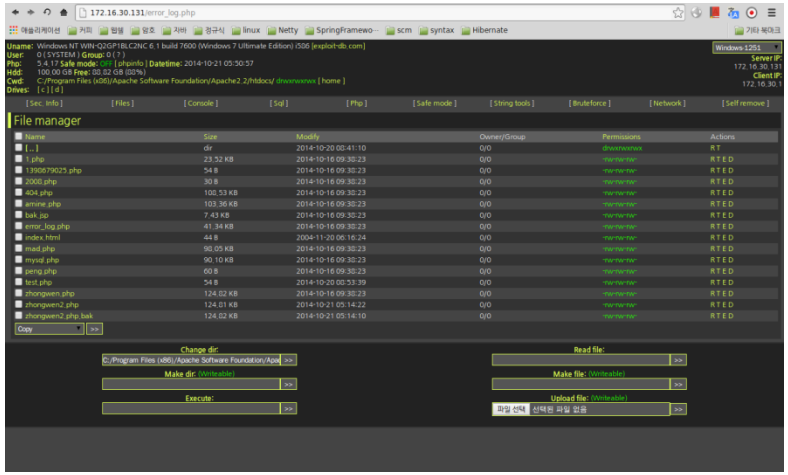

Attacker use similar variable name, comment, etc
-> it is a **important fingerprint**

# 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

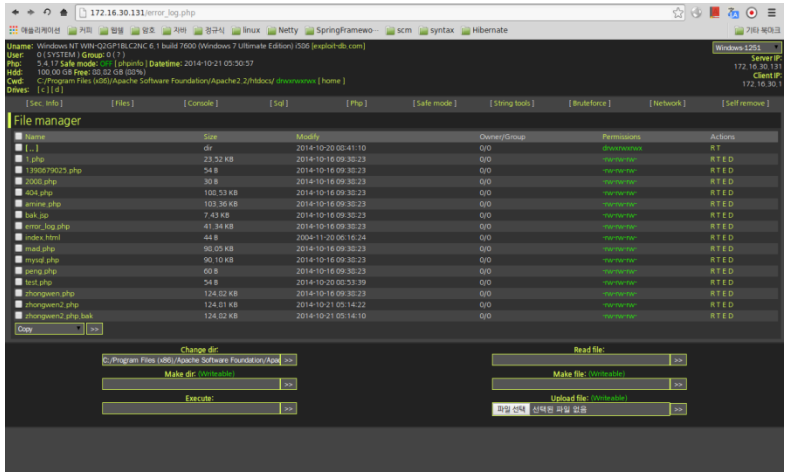
- Nomarl url connection :
  error page

- Related incidents : OO homepage

- Regular expression substitution

# (Ex) WSO Webshell(2/2)

- WSO webshell




- Login password: OOO — By the fingerprint / By function
- Nomarl 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

| | |
|---|---|
| shell_exec | unserialize |
| paththru | ssh2_exec |
| open | ssh1_exec |
| proc_lpopen | preg_replace |
| system | preg_replace |

- Dynamic code injection

| | |
|---|---|
| builtin_val, php_eval | call |
| create_function | unserialize |

<example in php>

# 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
- Gzipinflate
- 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

detection pattern : wscript.shell

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

# By analysis disturbance

- Debug code removed
- Variable and function names randomization

# By file name

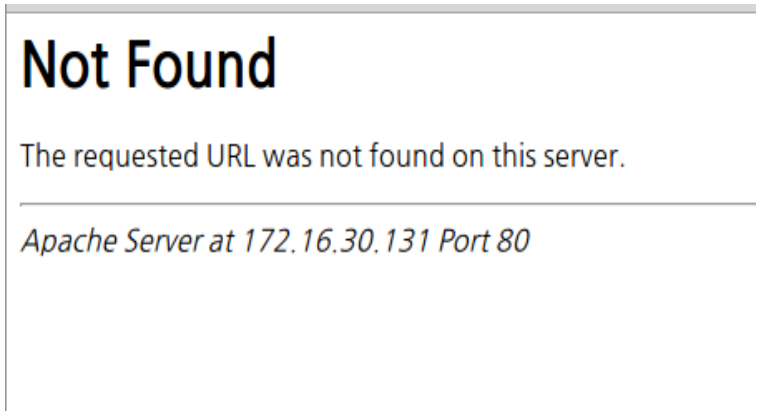
- Use a semicolon
- Insert intermediate extension

# By concealment method

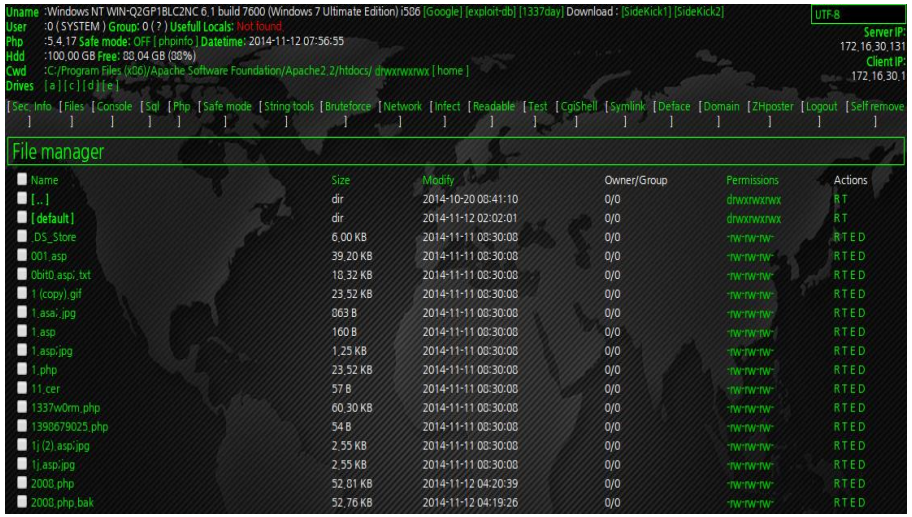
- Display error page
- Parameters required
- Login feature

# (EX) By concealment method

- Display error page / Login feature




Normal url access




If you are login

KrCERT/CC

# By the fingerprint and transformation of webshell

| file name | Adminer | C99 | phpspy | HP2006 | Spider PHP Shell | WSO 404 Shell | Dark blade | Web-Based Window | Smart Shell | asp.backdoor.peiya.. | ASPX Spy | YeMeNi Sh3ll | SimAttacker | dmc | 1337 wOrm | dosya | r57 | ASP!Spyder | md5 32 | JSP File browser | jfolder | JspWebshell | JSP_KIT | Jshell | Jsp File Manager | Jspspy | 4ngel | CrystalShell | DSShell | FaTaLSheLL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ass.phtml.php.inc.php.txt | | | | | O | | | | | | | | | | | | | | | | | | | | | | | | | |
| index.html | | | | | O | | | | | | | | | | | | | | | | | | | | | | | | | |
| index.php.txt | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| m.php.gif | | | | | O | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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

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