個案分析-來自手機簡訊的惡意程式攻擊 分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/09

前言

智慧型手機已經是目前市場主流的手持設備,可說是小型移動式電腦。該設備幾乎都能透過 WiFi 或 3G 等方式上網,然而與一般電腦不同的是,大多的使用者都不會在手機裡安裝防毒軟 體,一旦被駭客入侵可能就會造成個人資料外洩。

主要原因是因為使用者還是將智慧型手機當作是一般的手機,沒有電腦的觀念。

事件說明

- 一、 事件經過:
 - 1. 某網友在國內知名 BBS 站[PTT]的反詐騙版[Bunco]發文,表示自己疑似收到詐騙的 SMS 簡訊。
 - 由截圖發現該簡訊會以『XXX 被偷拍的是你麼』為主旨(XXX 是該用戶姓名),並附上 一個 URL 作為連結。



圖 1、PTT 內文和簡訊內容

 發信來源的門號為簡訊代轉發的公司,主要提供「手機版簡訊平台」服務讓使用者不會 透露自已發送的門號,很適合做為駭客使用。



4. 此簡訊提供網址 IP [199.101.117.21] 的國別為 US 美國 LA。

5. 實地將該網址"http://199.101.117.21/index.php"點入,透過Firefox 的瀏覽器監看工具可以 看到其行為,是下載一個 Android 所用的程式安裝檔,其檔名為『images.apk』。

請求 URL: http://199.101.117.21/ はままかた、CPT	Created by using <u>HTTPNetworkSniffer</u>			
研水方法:001 狀態代碼: ● 200 0K	Host Name	199.101.117.21		
	Method	GET		
	Path	/		
△ 回應榴頭 (0.444 KB)	User Agent	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)		
Cache-Control: "must-revalidate, post-check=0, pre-check=0"	Response Code	200		
Connection: "Keep-Alive"	Response String	OK		
Content-Description: "File Transfer"	Content Type	application/octet-stream		
Content-Disposition: "attachment; filename=images.apk"	Referer			
Content-Length: "250836"	Content Encoding			
Content-Transfer-Encoding: "binary"	Transfer Encoding			
Content-Type: "application/octet-stream"	Server	Apache/2.2.9 (APMServ) PHP/5.2.6		
Date: "Tue, 13 Aug 2013 03:45:45 GMT"	Content Length	250836		
Expires: "0"	Connection	Keep-Alive		
Keep-Alive: "timeout=5, max=100"	Cache Control	must-revalidate, post-check=0, pre-check=0		
Pragma: "public"	Location			
Server: "Apache/2.2.9 (APMServ) PHP/5.2.6"	Server Time	2013/8/12 上午 09:06:08		
X-Powered-By: "PHP/5.2.6"	Expiration Time			
△ 請求椔頭 (0.301 KB)	Last Modified Time			
Host: "199.101.117.21"	Cookie			
User-Agent: "Mozilla/5.0 (Windows NT 6.2; WO0) Gecko/20100101 Firefox/23.0"	Client Address	140		
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"	Server Address	199.101.117.21:80		
Accept-Language: "zh-tw,zh;q=0.8,en-us;q=0.5,en;q=0.3"	Request Time	00:00:00.000		
Accept-Encoding: "gzip, deflate"	Response Time	11 ms		
Connection: "keep-alive"	URL	http://199.101.117.21/		

圖 2、HTTP 的 Header 動作為 File Transfer。

- 6. 先將該 APK 檔用線上 Virustotal 檢測,惡意程式的檢出比例為 2/45,確實為一個後門程式。
- 二、 惡意程式的測試過程:
 - 1. 使用虛擬機器 VirtualBox 配合 Genymotion 的智慧型裝置模擬器,創建一個 Andorid 4.2.2 的手機平台。

∞ oO Genymotion	Genymotion	_ _ ×	型號 Galaxy S4 HTC One Xperia Z - 4.2.2 - with Google Apps - API 17 - 1080x1920
IIII ► Menu Play	+ Add	? Help	Android 版本 4.2.2
Your virtual devices Galaxy S4 HTC One Xperia Z - 4.2.2 - with Google Apps - API 17 - 1080x1920		1920 🔯 💼	核心版本 3.4.0-qemu+ dan@ubunt#8 Fri Nov 23 15 08:48 CET 2012
Not authenticated to Genymotion Cloud			版本號碼 vbox86p-userdebug 4.2.2 JDO39E eng.buildbot.20130717.143040 test-keys

- 2. 使用 Wireshark 側錄該設備的網路流量。
- 3. 使用實體 IP 並安裝該『images.apk』,安裝時的軟體名稱為"Sys Config",且圖示為 iPhone 的設定樣式。
- 4. 該程式"Sys Config"要求的隱私及存取權限有:
 - (1). 讀取手機狀態和識別碼。
 - (2).SMS 簡訊的發送、讀取、編輯。
 - (3).設備的概略位置。
 - (4).修改和删除 SD 卡的內容。
 - (5). 完整網路的存取及狀態。
 - (6). 啟動時自動執行。
 - (7). 測試能否存取受保護的儲存裝置。

•• Genymotion - Galaxy S4 H	HTC One Xperia Z - 4.2.2 - with Google Apps - API 17	- 1080x1920 (1024x768 – 🗖 🗙	○ Genymotion - Galaxy S4 H	TC One Xperia Z - 4.2.2 - with Google Apps - API 17 - 10	080x1920 (1024x768 🗕 🗖 🗙
		🗢 🗎 4:36			🐨 🗎 4:37
您所直询的網頁不存在或 × -	_		松所直约的胡贾不存在或 。 × -		
\leftarrow \rightarrow C \blacksquare http://199	9 Sys Config	☆ 🔍 🖬 🎽	\leftarrow \rightarrow C \blacksquare http://199	Sys Config	☆ 🔍 🖬 ⁹
你听奇物的網百不存在可	您要安装這個應用程式嗎?應用程式將取得以下權限:		你所查询的網百不存在可	您要安裝這個應用程式嗎?應用程式將取得以下權限:	
此相互位址: http://199.101.117.21		_	此網頁位址: http://199.101.117.21	1945 0990 1001 ● 這可能需要付算 總權節詞 (SMS ₩ MMS)	
建摄您嘗試以下動作:	. 請取手機狀態和識別碼	4+	建調您審試以下動作:	績取態的簡訊 (SMS 或 MMS)	4 +
 ・	接收總訊 (SMS) (用) まいの 前日		 ·	♥ 概略位置(以続路為基準)	
 The Google Hitters of the state of 	● 遠可能需要付費 編編總訊 (SMS 既 MMS)	O	• 12 OUGHE HIRRING CONTRACT	↓ 修改或删除 SD 卡的內容	Ø
	講取您的简訊 (SMS 或 MMS)			裝置存取權	, in the second s
	概略位置(以蝦鹉為基準)			完整網路存取權	
	↓ 修改或删除 SD 卡的內容			查看 WiFi 連線 演看網路連線	
装置存取權		\		▲	6
	完整规路存取模 资源 WiFi 通信	æ		➡ 测缸能否存取受保護的儲存装置	æ
	取消 下一夕			102月 安装	
		Q			Q

安裝完成後會該程式無法點入,會一直出現「很抱歉,Sys Config 已停止」的訊息,此時其實已經在背景執行網路行為,重開機後依然會出現該訊息,自動背景執行。



- 6. 觀察側錄的網路流量封包:
 - (1).透過封包分析發現該程式會一直向 IP: 216.244.79.37 的 port 80 傳送資料,使用的方 式為 HTTP POST。因為測試主機並無登入任何帳號和密碼,從網路行為上來看應該 是會竊取個資。
 - (2).下圖得知該程式會將左下紅框的資料 POST 至 Server 端的

/index.php/Backdoor/task_query 下,而 Server 端成功接收後回覆 HTTP/1.1 200 OK。



(3).IP [216.244.79.37] 位於美國的西雅圖,實際開啟該網站為一個 Web 的登入畫面,並 且顯示是簡體中文,該主機可能是被大陸駭客用來當作跳板。



(4).網域名稱為"member.updatalook.com"的正解為 IP [216.244.79.37], 然而並無反解。

. here is the nslookup result for member.updatalook.com from serv	$er 8.8.8.8, \dots$ here is the historkup result for 210.244.79.37 from server 8.8.8.6, querytype=P r	ζ.
DNS server handling your query: 8.8.8.8 DNS server's address: 8.8.8.8#53	DNS server handling your query: 8.8.8.8	
Non-authoritative answer:	DNS server's address: 8.8.8.8#53	
Name: member.updatalook.com Address: 216.244.79.37	<pre>** server can't find 37.79.244.216.in-addr.arpa.: NXDOMAIN</pre>	

7. 觀察側錄的網路流量封包

	tcp6	0	1 ::ffff:140.x.x.147:55724 ::ffff:216.244.79.37:80 CLOSE_WAIT
300	tcp6	0	0 ::ffff:140.x.x.147:47972 ::ffff:216.244.79.37:80 TIME_WAIT
	tcp6	0	0 ::ffff:140.x.x.147:36675 ::ffff:216.244.79.37:80 TIME_WAIT
	tcp6	0	0 ::ffff:140.x.x.147:60116 ::ffff:216.244.79.37:80 TIME_WAIT
	tcp6	0	1 ::ffff:140.x.x.147:46847 ::ffff:74.217.75.7:443 CLOSE_WAIT
	tcp6	0	0 ::ffff:140.x.x.147:48030 ::ffff:216.244.79.37:80 ESTABLISHED
	tcp6	0	0 ::ffff:140.x.x.147:49093 ::ffff:216.244.79.37:80 TIME_WAIT
	tcp6	0	0 ::ffff:140.x.x.147:39076 ::ffff:216.244.79.37:80 ESTABLISHED

(1).透過設備終端機指令 netstat 記錄到當時手機資料正在被傳輸給駭客。

(2). Process State : PS

USER	PID	PPID	VSIZE	RSS	WCHAN	PC	NAME
u0_a62	1374	127	498764	21396 ffffffff	b753ea07	S	au.com.phil.minepro

8. 解決方式

- (1).使用內建的應用程式管理將該程式移除「Sys Config」。
- (2). 更改內存的密碼,如 Google 和 Facebook 等。
- (3). 備份個人資料至外部或雲端,通訊錄可以用 Gmail 自動同步備份。
- (4).若擔心惡意程式移除不乾淨,建議設備還原至原廠設定。

建議措施

- 1. 盡量不要安裝來路不明的軟體,除非能確定它的功能作用。
- 2. 安裝軟體時看注意軟體會存取的權限,避免較高權限被使用。
- 3. 當軟體安裝完後無法開啟或有錯誤時,先關閉網路並盡速移除。
- 4. 安裝不明檔案前先透過 Virustotal 進行線上掃毒,或安裝手機的防毒軟體。
- 網路上很多論壇會提供號稱是某某破解版的 APK 供人下載,未來很有可能會被駭客 用來植入後門的一個途徑,務必小心避免個資外洩。

