個案分析-

E 大學中繼站個資事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/05

一. 事件簡介

1. 今年二月底接獲通知E大學有主機疑似感染成為C&C或中繼站，協同ICST前往側錄主機流量及資安鑑識。
2. 這台感染主機特性是，持續傳送及接收大量網路流量，導致網路頻寬壅塞，故判斷可能成為C&C主機或中繼站。
3. E大學的感染主機IP是140.X.X.55，是使用Linux的作業系統，且為系所研究室的伺服器。

二. 事件檢測

1. 透過側錄主機網路流量封包以觀察其網路行為，藉此判定是否為C&C主機或中繼站。
2. 收集主機內的相關系統紀錄，藉此判定有異常的執行程序。
3. 該系統被植入後門的網站伺服器套件Nginx，故連接埠80(http)和443(https)是被開啟的。故能被用來接收殭屍電腦的資料，再中繼給C&C主機。
   (1). 連接埠22(ssh)是開啟的，此主機root的管理權限被設定能夠遠端ssh登入，且沒有設定連線來源端網段限制，可能因此遭受駭客破解登入。
   (2). 從Crontab檔案得知，例行程序會透過指令「killall

nginx」定期清除 nginx 紀錄。

(3). 檢查發現除了 Nginx 之外，sshd 的服務紀錄也都被導入 dev/null，且 history 的指令紀錄也被自動清除，為駭客避免留下登入的線索。

4. 觀察封包可知有許多網域名稱對應到感染主機 IP，研判駭客使用多對一的「Fast-Flux」的動態 DNS 轉換技術。這些動態網域都是用來掩飾中繼站 IP 所用，部分特定名稱會有特定用途，如傳送病毒檔案或個金融資。

Fast-Flux 動態網域名稱		
網域名稱	解析出的 IP	方式
rangetozthpick.com	140.X.X.55	HTTP
defensesuncomp.at	140.X.X.55	HTTP
enthusiastsma.com	140.X.X.55	HTTP
littwronthath.net	140.X.X.55	HTTP
www.littwronthath.net	140.X.X.55	HTTP
nss1.primebeauty.net	140.X.X.55	HTTP
gefodidnsands.com	140.X.X.55	HTTP
saysthnetwork.com	140.X.X.55	HTTP (金融個資)
www.primebeauty.net	140.X.X.55	HTTP
mailcow.net	140.X.X.55	HTTP
reonetedugred.com	140.X.X.55	HTTP (圖片 JPG)
primebeauty.net	140.X.X.55	HTTP
hresellerspasta.com	140.X.X.55	HTTP (惡意程式 exe)
qqd52ayf1uz.com	140.X.X.55	HTTP
pronautmaster.net	140.X.X.55	HTTP (圖片 JPG)
dsaoe5pr95.net	140.X.X.55	HTTP
thnetworkcabl.net	140.X.X.55	HTTP (圖片 JPG)
ectedsaysitha.com	140.X.X.55	HTTP (圖片 JPG)

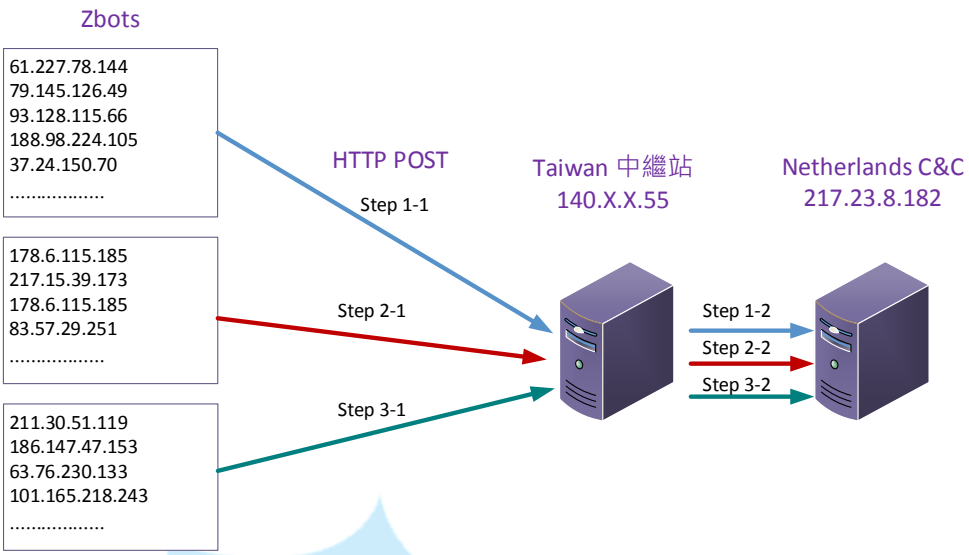
wujieliulan.com	140.X.X.55	HTTP
mkjnl.net	140.X.X.55	HTTP
test.com	140.X.X.55	HTTP
www.pronautmaster.net	140.X.X.55	HTTP (圖片 JPG)
共 22 個	多網域對一 IP	皆使用 port 80

5. 從封包紀錄得知，大量的網路流量會連至 217.23.8.182，此台可能為上層的 C&C 伺服器，用來接收底層殭屍電腦中繼上來的資料。

   (1). C&C 的 IP 位址 217.23.8.182 位於紐西蘭，反解析出的網域名稱為「customer.worldstream.nl」。

   (2). 瀏覽器測試該網站，網站運作中卻顯示為空白畫面，應該為駭客用來收集資料所用。

6. 連至中繼站的底層殭屍電腦至少有 3000 個相異 IP，全部來自國外等 62 個國家，且排名前三個分別是“德國、西班牙、南非”。



Step 1-1 : POST **pronautmaster.net/hez/xsea.php** from zbot to 140.X.X.55
Step 1-2 : POST **pronautmaster.net/hez/xsea.php** from 140.X.X.55 to 217.23.8.182

Step 2-1 : POST **littwronthath.net/het/sdgf.php** from zbot to 140.X.X.55
Step 2-2 : POST **littwronthath.net/het/sdgf.php** from 140.X.X.55 to 217.23.8.182

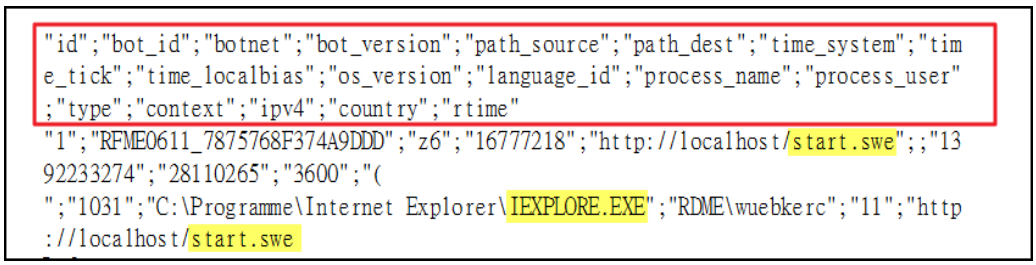
Step 3-1 : POST **rangetozthpick.com/** from zbot to 140.X.X.55
Step 3-2 : POST **rangetozthpick.com/** from 140.X.X.55 to 217.23.8.182

7. 觀察其中一個中繼行為其網域名稱是「saysthnetwork.com」，由底層主機 88.130.24.178 透過中繼站 140.X.X.55 向上層 C&C 主機 217.23.8.182 要求資料，我們發現都會使用一組帳號密碼作為認證，封包中的帳密透過 Base64 編碼方式加密，密文字串「YWRtaW5fNDVqZ2hmOkFRNkdVQmNS」經過解密後為「admin_45jghf:AQ6GUBcR」，也就是帳號密碼分別為，『admin_45jghf』和『AQ6GUBcR』。

(1). 此例底層主機向中繼站做「POST /phpmyadmin//export.php」後，中繼站立刻也會向 C&C 217.23.8.182 做相同的 POST 路徑動作。

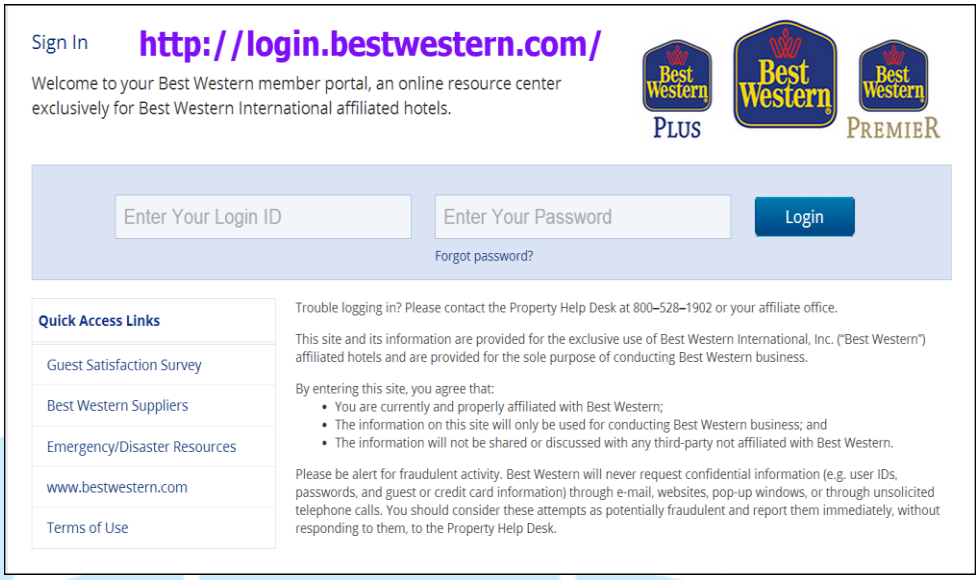
(2). 待 C&C 主機收到中繼站的 POST Request 後，從回覆的訊息中發現許多機密性資訊，例如「"id";"bot_id";"botnet";"bot_version";"path_source";"path_dest";"time_system";"time_tick";"time_localbias";"os_version";"language_id";"process_name";"process_user";"type";"context";"ipv4";"country";"rtime"」的殭屍主機欄位資訊。

a. 其中 process_name 主要是由一隻名叫 start.swe 的程式所執行。



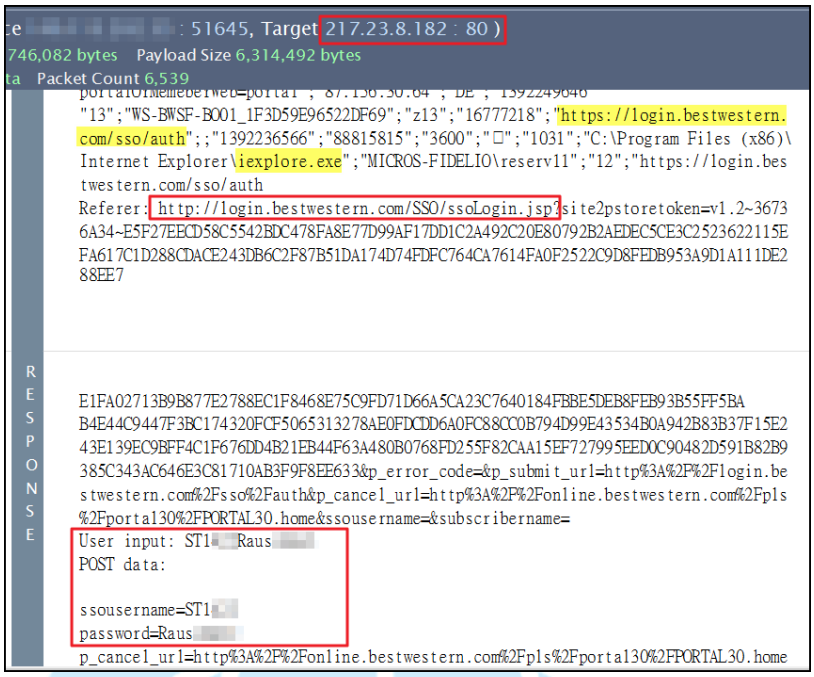
b. 該程式會回傳一些使用者 IP 位址及特定網站的登入帳號

及密碼，而封包中出現 Windows IE 瀏覽器的執行路徑，研判受害者因為 IE 的漏洞而遭竊個資。此特定網站為線上 Hotel 住宿訂房網站。



c. 由以上資訊研判底層主機 88.130.24.178 可能為駭客向 C&C 主機索取資料用，利用中繼站當作跳板存取 C&C 而非直接登入，可藏匿於大量殭屍主機之中不易被察覺。

使用者 IP	網域	帳號	密碼	網站
195.125.241.27	DE	SF_***	Raus*****	http://login.bestwestern.com/
195.125.241.27	DE	ST1***	Raus*****	http://login.bestwestern.com/
87.156.30.64	DE	ST1***	Raus*****	http://login.bestwestern.com/



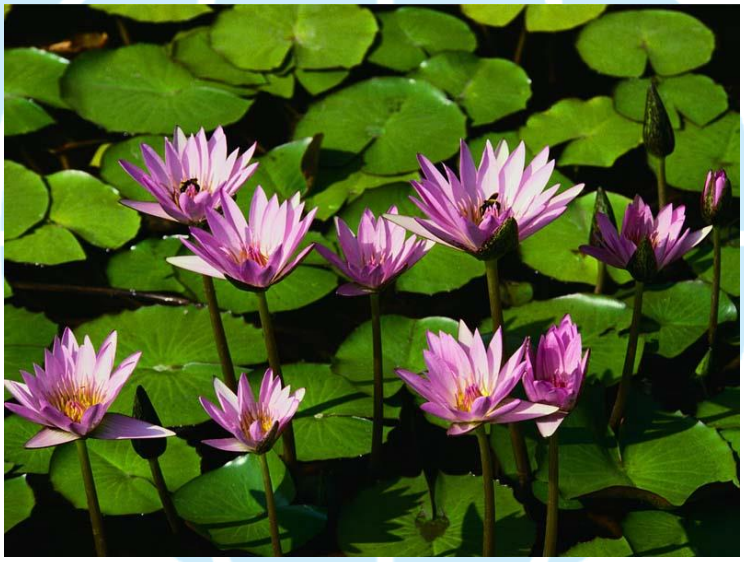
8. 網路封包中得知中繼站主機負責轉送大量的 JPG 檔案，主要由三張不同的圖片構成。經過比對發現此圖在趨勢科技新聞有報導過可能內藏有金融資訊等個資，透過特殊的資訊隱藏術（Steganography）將金融資訊隱藏在其中。參考新聞連結:

http://www.ithome.com.tw/news/85690

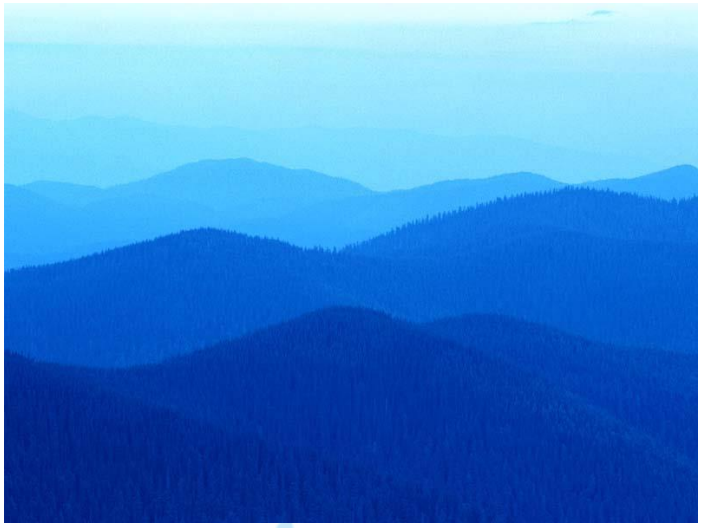
(1). 在此我們透過工具將收集到的部分封包還原成圖檔做解析，尚未發現有相關的隱藏資訊或方式，研判只做為殭屍電腦感染後做報到或暗號使用，或許每張圖對駭客來說有特殊的意義。因為封包中會記錄原始發送主機 IP，以便透過中繼站之後還能讓 C&C 主機能夠得知來源端主機 IP。

(2). 第一張風景圖為新聞顯示同一張的夕陽風景圖。

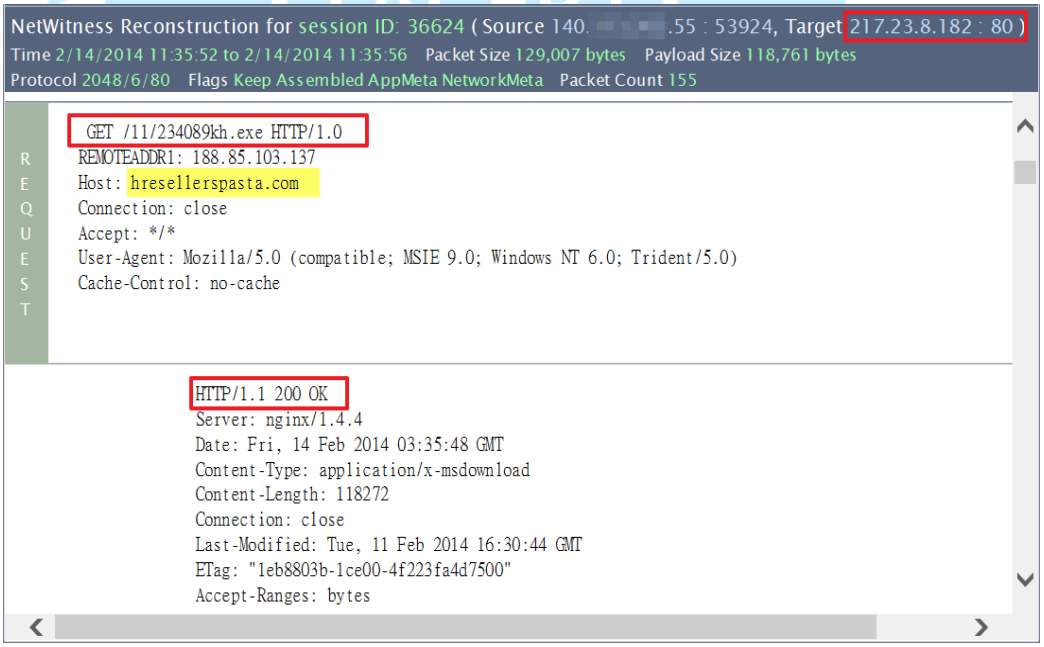
(3). 第二張圖為植物蓮花圖。



(4). 第三張圖為山林的風景圖。



9. 此中繼站也會向 C&C 接收一些惡意程式執行檔，目前有紀錄到的檔案為「234089kh.exe」和「kia.exe」這兩種檔案，且都是透過特定網域名稱「hresellerspasta.com」做傳輸用途，這兩種檔案使用掃毒軟體檢測確定為惡意程式。



10. 從封包發現有網站登入的資料，經分析還原發現內藏有惡意程式 cmd.php.exe 執行檔，主要是由下層 zbot 德國主機 80.188.76.27 傳至 140.X.X.55 後再中繼至上層 C&C 主機

217.23.8.182。

(1). 將惡意程式「cmd.php.exe」透過 Virustotal 掃描後有 11/51 的檢出比例，判別為 zbot 木馬程式，原始名稱為 Satloud.exe，目的使感染主機成為殭屍電腦。

Authenticode signature block	
Copyright	Copyright © 2012 Gigamon Corporation. All rights reserved.
Publisher	Gigamon
Product	Callconsider Gigamon Im
Original name	Satloud.exe
Internal name	Satloud.exe
File version	5.0.351.844
Description	Callconsider

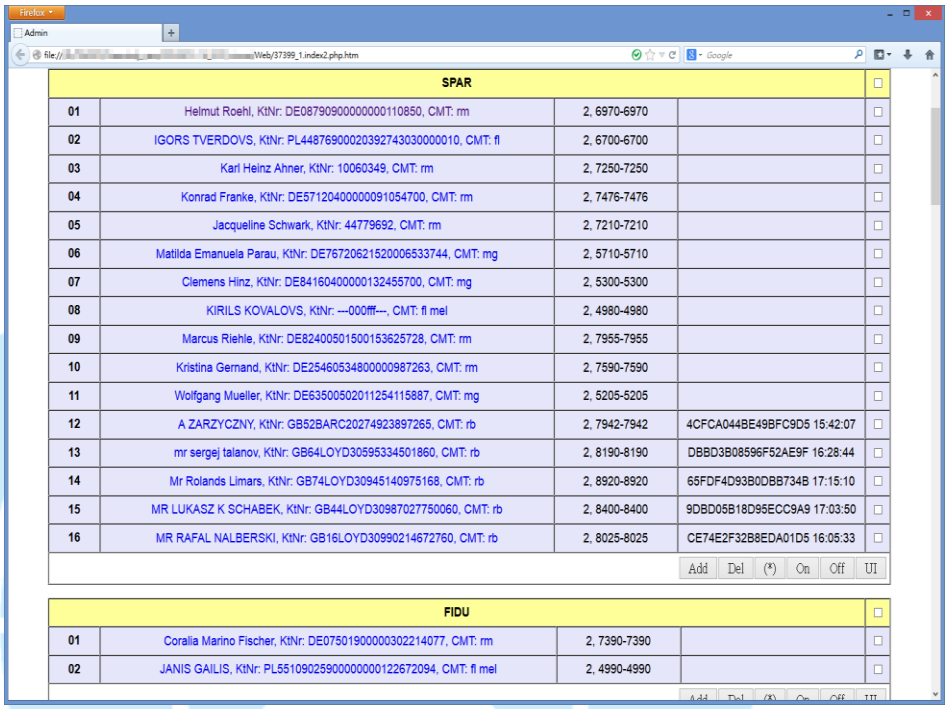
(2). 還原出來的程式除了惡意程式之外，還有 htm 網頁檔。其中內容記錄許多收集來的德國各線上銀行的帳戶 ID、密碼、網址及金額等個人資訊，研判許多人的金融帳號密碼可能已被駭客竊取。

(3). 另有檔案紀錄受害者手機 SMS 的發送資訊，包含各 IP、銀行網址、帳號密碼及下載的惡意 APK 網址。該網址透過 Virustotal 檢測出的比例卻只有 1/53，非常的低。

a. 封包還原後的檔名為「index2.php.htm」，其中前面有 SPAR 和 FIDU 這兩個欄位，內容似乎記載了特殊訊息和連結，但我們無法判斷是什麼意思。另外有個 Success 72h

的欄位就較為明顯易懂，記錄了網路銀行連結、帳戶名稱、密碼及金額等資訊，並且都是以明文方式記錄。

b. 這些網路銀行的所記錄到的都是德國的銀行，若為真的個人資訊，表示已經相當多人的個資被竊取。



SPAR				
01	Helmut Roehl, KtNr: DE08790900000000110850, CMT: rm	2, 6970-6970		
02	IGORS TVERDOVS, KtNr: PL44876900020392743030000010, CMT: fl	2, 6700-6700		
03	Karl Heinz Ahner, KtNr: 10060349, CMT: rm	2, 7250-7250		
04	Konrad Franke, KtNr: DE57120400000091054700, CMT: rm	2, 7476-7476		
05	Jacqueline Schwark, KtNr: 44779692, CMT: rm	2, 7210-7210		
06	Matilda Emanuela Parau, KtNr: DE76720621520006533744, CMT: mg	2, 5710-5710		
07	Clemens Hinz, KtNr: DE84160400000132455700, CMT: mg	2, 5300-5300		
08	KIRILS KOVALOVS, KtNr: ---000fff---, CMT: fl mel	2, 4980-4980		
09	Marcus Riehle, KtNr: DE82400501500153625728, CMT: rm	2, 7955-7955		
10	Kristina Gernand, KtNr: DE25460534800000987263, CMT: rm	2, 7590-7590		
11	Wolfgang Mueller, KtNr: DE63500502011254115887, CMT: mg	2, 5205-5205		
12	A ZARZYCZNY, KtNr: GB52BARC20274923897265, CMT: rb	2, 7942-7942	4CFCA044BE49BFC9D5 15:42:07	
13	mr sergej talanov, KtNr: GB64LOYD30595334501860, CMT: rb	2, 8190-8190	DBBD3B08596F52AE9F 16:28:44	
14	Mr Rolands Limars, KtNr: GB74LOYD30945140975168, CMT: rb	2, 8920-8920	65FDF4D93B0DBB734B 17:15:10	
15	MR LUKASZ K SCHABEK, KtNr: GB44LOYD30987027750060, CMT: rb	2, 8400-8400	9DBD05B18D95ECC9A9 17:03:50	
16	MR RAFAL NALBERSKI, KtNr: GB16LOYD30990214672760, CMT: rb	2, 8025-8025	CE74E2F32B8EDA01D5 16:05:33	
			Add Del (*) On Off UI	

FIDU				
01	Coralia Marino Fischer, KtNr: DE07501900000302214077, CMT: rm	2, 7390-7390		
02	JANIS GAILIS, KtNr: PL55109025900000000122672094, CMT: fl mel	2, 4990-4990		

Success 72 h

11/02/2014 08:50:26 GMT	SPAR	A111000111 5BFACBA8598458B2F5
	89.187.202.72	IEXPLORE 10.0.9200.16750
USERHOST:	banking.sparkasse-leipzig.de	
USERACC:	114070 Mehnert	
USERPASS:		
AVBALANS:	1140701173 : $13809.92;	
DROP DATA:	ARTIS ZAKIS; POLUPLPR; PL87876900020202362330000010; 6810,00; OLK109927823	
ExINF:	1140701173 |21m|-68904467| SEPA	
COMMENT:	fl	

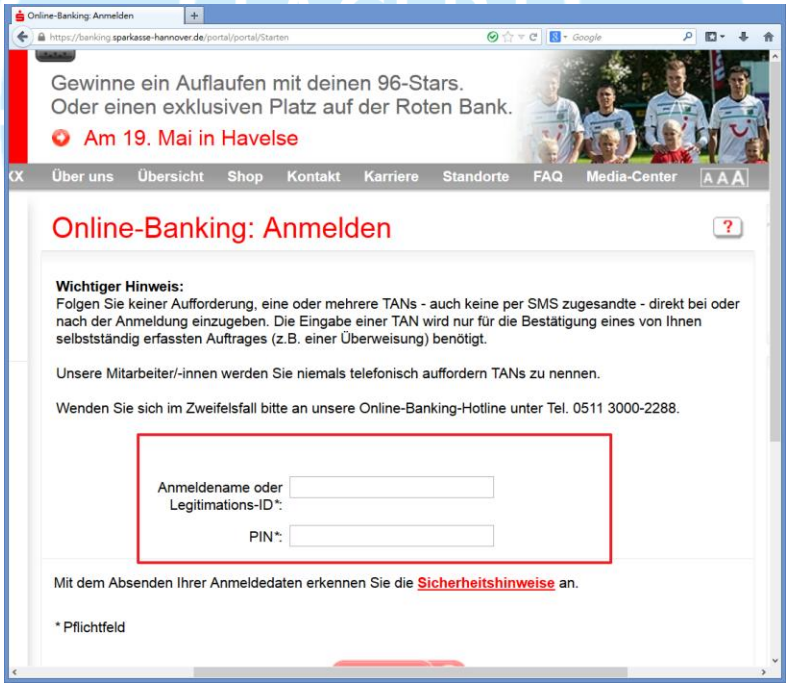
11/02/2014 16:44:17 GMT	SPAR	A111000111 7CAE0111641A5C0BEB
	80.137.160.147	firefox 26.0.0.0
USERHOST:	bankingportal.sparkasse-aachen.de	
USERACC:	673900217991 Mazumder	
USERPASS:		
AVBALANS:	48164305 : $2786.58;	
DROP DATA:	Chris Weber; BOFSDEF1XXX; DE90502205000000949768; 1700,00; L463042B9XAA	
ExINF:	48164305 |4m|-571286749| SEPA	
COMMENT:	MOc se	

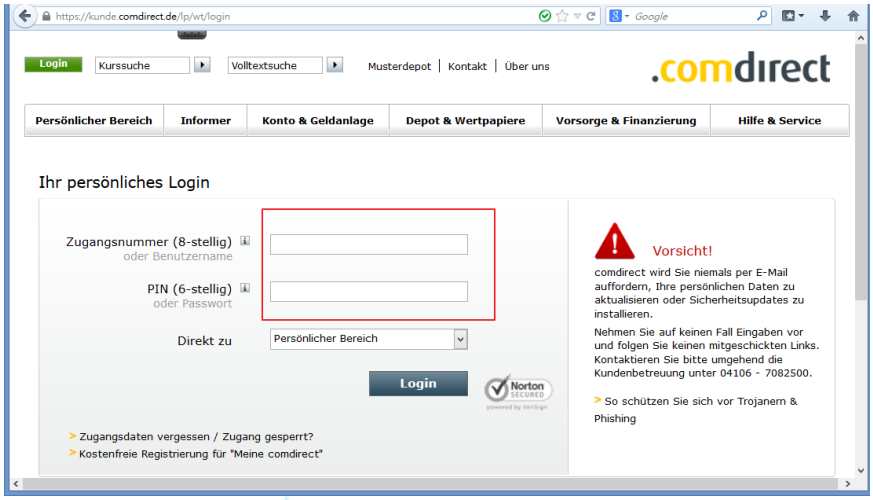
11/02/2014 18:59:28 GMT	SPAR	A111000111 C9C37C3E89040C62AB
	78.49.135.104	firefox 3.0.4.0
USERHOST:	banking.sparkasse-hannover.de	
USERACC:	114096 ml;rg Gaebke	
USERPASS:	80	
AVBALANS:	1140960350 : $20008.12; 1905157061 : $56.51;	
DROP DATA:	Matthias Isermann; 60050101; 7853042081; 5670,00; 2/2014 U.03	
ExINF:	1140960350 |3h43m|1903092700| SEPA	
COMMENT:	dn	

11/02/2014 19:50:56 GMT	SPAR	A111000111 98286823882946BBA7
	94.218.180.80	iexplore 8.0.6001.18702
USERHOST:	bankingportal.sparkasse-rhein-neckar-nord.de	
USERACC:	767584032197 Betancourt	
USERPASS:	EB	
AVBALANS:	34011664 : $5667.34;	
DROP DATA:	ERNST KIETAIBL; HYVEDEMMXXX; DE30700202700044918846; 5180,00; Abrechn. PO409788125	
ExINF:	34011664 |2h38m|627426486| SEPA	
COMMENT:	mg	

c. 實際檢查網址確實是銀行的登入頁面，然而我們並無實地使用以上的帳號密碼做登入測試。

已紀錄的網路銀行網址	國家
https://banking.postbank.de/rai/login	德國
https://bankingportal.kskbitburg-pruem.de	德國
https://bankingportal.sskbo.de	德國
https://banking.lzo.com	德國
https://bankingportal.spk-bbg.de	德國
https://bankingportal.sparkasse-dieburg.de	德國
https://kunde.comdirect.de/lp/wt/login	德國
https://banking.berliner-sparkasse.de	德國



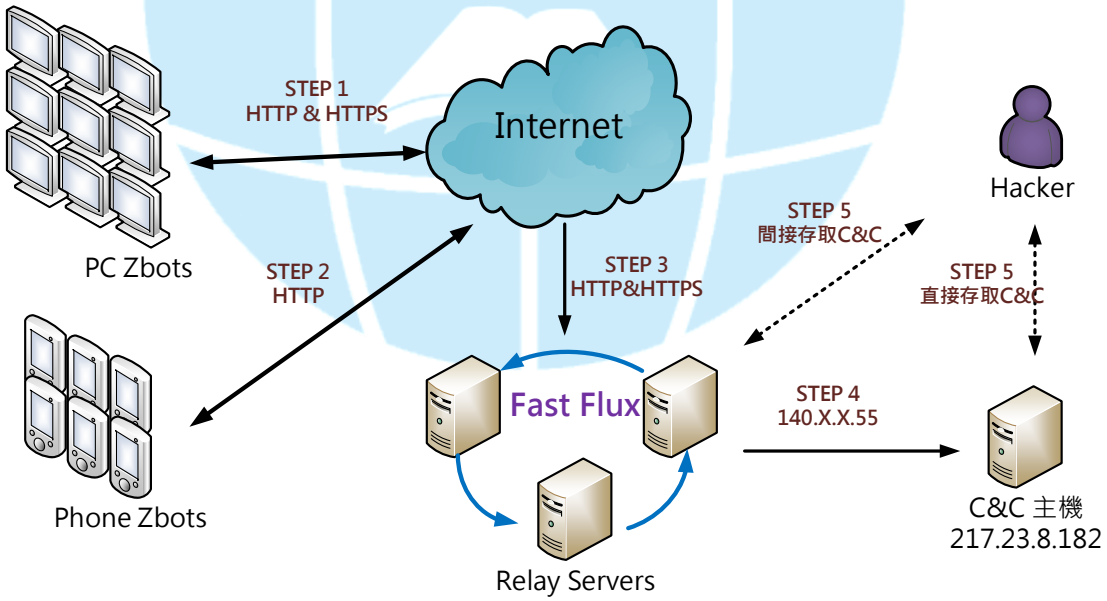


d. 封包還原後檔名為「sms.php.htm」，下圖可得知內容放有手機登入銀行的帳號密碼明文等資訊。例如手機的 GPS 經緯度及 IP，能讓駭客取得該手機登入的位置。使用的瀏覽器資訊，例如 Firefox。這些手機應該都是遭受特定惡意程式感染，故欄位中存有惡意 APK 的下載連結，但這些 APK 存放的位置為亂數產生的暫存檔，故我們要測試下載路徑不存在，研判可能安裝了其他軟體於背景下載執行。另外有個欄位標註為 SMS Send: Yes or No，研判應該為感染後能夠在控制 SMS 的發送感染給其他人。

13/02/2014 10:09:21 GMT	Not Set	A111000111 8696230EA42FF77B3A
2	95.91.232.120	firefox 26.0.0.0
Host:	https://banking.postbank.de/rai/login	
login:	24689	
password:	21	
Available:	4.764,92; 1.713,11;	
TelNr:	491608982541	
Sms Send:	Yes/1	
App load:	No	
Link:	http://appsmartsecurity.net/04bc4a949b7d /SmartSecurityApp1_2.apk	
Code:	**********	
Status:	Enabled Ok	

13/02/2014 11:56:31 GMT	android	A111000111 95860FD3259F31EEAA
3	84.118.158.238	firefox 27.0.0.0
Host:	https://banking.postbank.de/rai/login	
login:	6438	
password:	SX	
Available:	475,70; 670,00; 216,84;	
TelNr:	491773519590	
Sms Send:	Yes/2	
App load:	Yes	
Link:	http://appsmartsecurity.net/eb59b25bb7bf /SmartSecurityApp1_2.apk	
Code:	1824049950	
Status:	Enabled Ok	

三. 網路架構示意圖



STEP 1：電腦感染成為殭屍主機Zbots，並向中繼站透過HTTP或HTTPS方式傳送資料。
STEP 2：手機平板感染成為殭屍主機Zbots，也向中繼站透過HTTP方式傳送資料。
STEP 3：大量Zbots透過Fast Flux動態網域名稱解析連到中繼站主機群。
STEP 4：C&C主機接受來自中繼站140.X.X.55及其他中繼站的中繼資料。
STEP 5：駭客可能直接或間接向C&C主機存取偷竊來的資料。

四. 結論

1. 此主機遭受駭客植入後門程式，並安裝有問題的 Nginx Web Server 套件，主要開啟 Port 80 和 443 來中繼資料。
2. 此主機感染為中繼站而非 C&C，主要接收來自底層殭屍電腦的資料，並中繼至上層的 C&C 控制命令主機，至少為三階層式的網路架構。
3. 底層的殭屍電腦除了常見的桌上型電腦外，目前看起來還有來自智慧型手機(Smart phone)或平板(pad)的設備。
4. 駭客利用了動態網域變更的 Fast Flux 技術，進行多對多的網域名稱解析，使得網域名稱存活時間不長且真實 IP 不易被查到。
5. 駭客可能利用特殊的資訊隱藏術，將可用資訊藏匿於圖形檔之中大量傳送及接收。
6. 有觀察到此主機駭客所傳遞的網路銀行個資，表示國外確實有大量的使用者金融個資外洩，有此推論遭受感染的電腦或手機資料都可能遭竊。

五. 建議措施

1. 管理者的密碼複雜度要加強，並且避免最高權限帳號能夠透過

遠端登入。

2. 限制遠端來源端的登入網段 IP，並加強防火牆規則並時常更新修補作業系統漏洞。
3. 時常透過指令 netstat 方式查看是否有可疑通訊埠被開啟或連線，當有大量網路流量產生時可能就是主機已遭受感染。
4. 檢查 CPU 或記憶體使用率是否一直很高，可能為惡意程式所為。