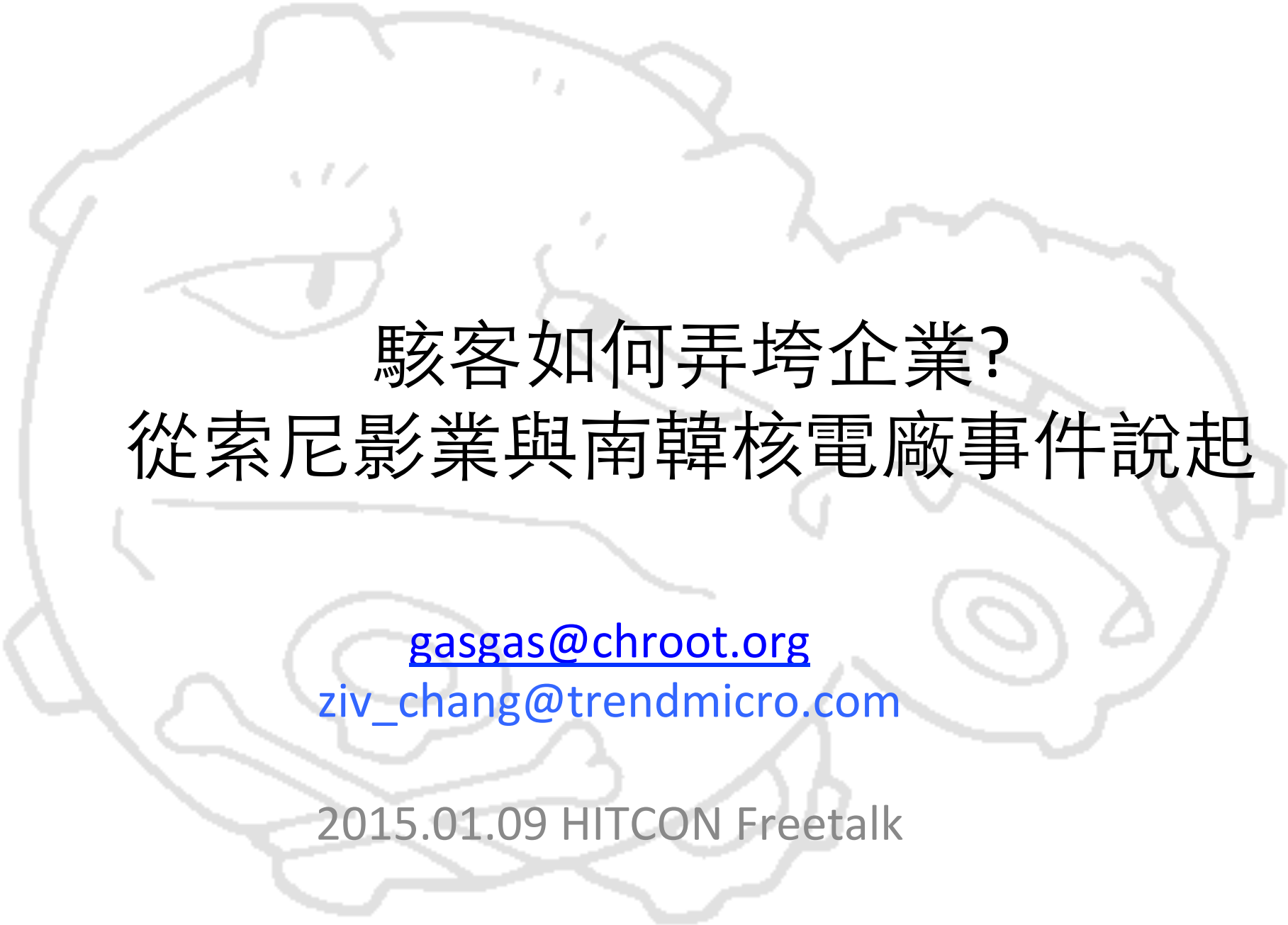


駭客如何弄垮企業?
從索尼影業與南韓核電廠事件說起

gasgas@chroot.org
ziv_chang@trendmicro.com

2015.01.09 HITCON Freetalk

索尼影業被害事件

- iThome 2014 12 05 報導
- 索尼影業（Sony Pictures）在上周一（11/24）遭到駭客入侵，導致內部網路及電腦全數停擺，除影片及員工資料外流，並傳出內部電腦資料全數遭刪除。介入調查的FBI隨後緊急警告美國業者應留意一款可執行毀滅性網路攻擊的惡意程式，資安業者對該惡意程式研究發現，駭客在正式展開攻擊的48小時前才編譯執行程式，顯示在攻擊之前就已掌握目標對象的所有網路及鎖定的目標機器。

- 包括趨勢科技、賽門鐵克、卡巴斯基實驗室，與Blue Coat等資安業者都分析了FBI所提及的Destover惡意程式，發現該惡意程式專門鎖定Sony Pictures，熟悉其內部電腦架構。除了記錄Sony內部主機名稱與IP位址的關係，還含有許多可進入共享網路的使用者名稱與密碼。當滲透到Sony網路之後，惡意程式就會開始運作，包括刪除使用者的檔案，刪除近端或遠端磁碟的檔案還有用來開機的主啟動磁區（MBR）。此外，Destover中還有一個BMP桌布檔的「Hacked By #GOP」畫面與Sony被駭時所出現的電腦畫面一致。

資料來源:http://www.ithome.com.tw/news/92853

Sony Pictures事件編年史(1)

2014.11.24

Sony Pictures 傳出被駭, GOP（Guardians Of Peace） 宣稱是他們作的

I am the head of GOP.
I appreciate you for calling us.
The data will soon get there.
You can find what we do on the following link.

2014.12.01

FBI介入調查, 並懷疑是北韓做的

GOP釋出26.4GB的資料, 包含4864個資料夾與33880個檔案
15232個在職員工的SSN外洩

Sony Pictures事件編年史(2)

2014.12.03

北韓外交官出面否認

- GOP釋出第二批被偷資料, 33.7MB的壓縮檔案
- 包含了500組帳密, 主機資訊, 內部IP
- 伺服器的憑證資料
- 121組FTP帳密
- 公司對外使用的各種服務帳號, 包括YouTube,novell, mediataxi, inflight, fidelity, spiDR, SPIRIT, sony style family center, FEDEX, Connect, SPTI, Acron TASS, SPE Courier, Concur, SPC Press, AIM, HR Connect, AMEX

Sony Picture事件編年史(3)

2014.12.09	北韓朝鮮通信表示駭客行為是正義的, 並否認北韓參與
2014.12.17	Sony Pictures 宣布取消 “The Interview” 公映
2014.12.19	FBI開記者會證實北韓是幕後主使者
2014.12.23	北韓對外網路斷光光
2014.12.24	Sony Pictures 宣布恢復 “The Interview” 公映
2015.01.02	美國對北韓進行新一輪的經濟制裁

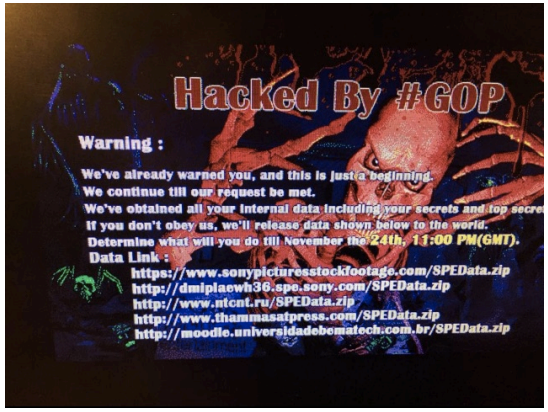
攻擊SPE的惡意軟體
（FBI/US-CERT公佈的資訊)

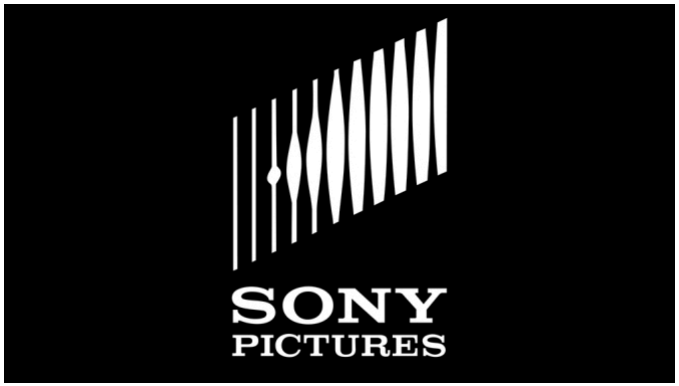
種類	數量	說明
SMB 蠕蟲	2種	透過網芳猜測密碼並植入惡意程式
監聽工具	未知	監聽網路, 監聽鍵盤, 監聽瀏覽器
輕量型後門	13種	單純回報與接收命令
代理工具	10種	內部網路連接使用
硬碟破壞工具	未知	破壞硬碟開機區域(MBR)
毀滅&清除工具	2種	刪除惡意程式並清除記錄
Destover	6種	徹底銷毀硬碟資訊, 復原無效

惡意程式中繼站
（FBI/US-CERT公佈的資訊)

IP	國家	Port Number
203.131.222.102	泰國	8080
217.96.33.164	波蘭	8080
88.53.215.64	義大利	8080
200.87.126.116	玻利維亞	8080
58.185.154.99	新加坡	8080
212.31.102.100	塞浦路斯	8080
208.105.226.235	美國	80

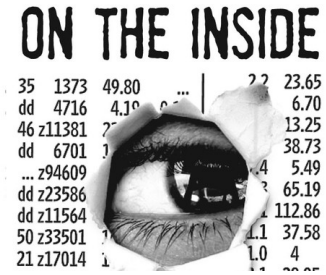
誰做的

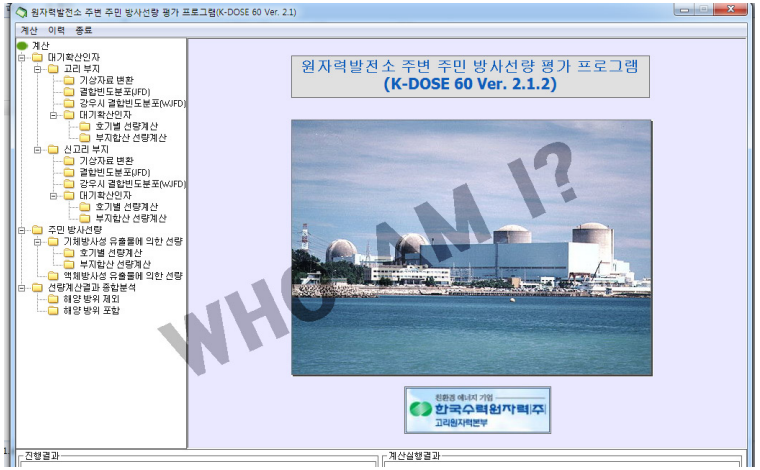

Hacked By #GOP
Warning :
We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip


SONY
PICTURES


Hacked By Whois Team
::: Who is 'Whois' ? :::
r3cycl3r@whois.com
!!! WARNING !!!
Hi !!!
We have an Interest in Hacking.
This is the Beginning of Our Movement.
User Acounts and All Data are in Our Hands.
Unfortunately, We have deleted Your Data.
We'll be back Soon.
See You Again


WANTED
KIM JONGUN
A.K.A. NUKE NUKE Mickey Lover


ON THE INSIDE
35 1373 49.80
dd 4716
46 z11381
dd 6701
... z94609
dd z23586
dd z11564
50 z33501
21 z17014
23.65
6.70
13.25
38.73
5.49
65.19
112.86
37.58
4


원자력발전소 주변 주민 방사선량 평가 프로그램(K-DOSE 60 Ver. 2.1)
원자력발전소 주변 주민 방사선량 평가 프로그램
(K-DOSE 60 Ver. 2.1.2)
WHO AM I?

跟FBI持不同看法

Christopher M Davis
@DavisSec

Follow

As a guy that works with the FBI on cyber crime fairly often, I still can't help but feel like they got this wrong. NK lacks this ability.

1:28 AM - 20 Dec 2014

Both Stammberger and Norse CEO made appearances on national news programs over the holiday weekend to disclose the investigation's conclusions. Video clips of the interviews can be found here:

時間: 2014.11.21-22
資料大小: 200+ GB
複製花費時間: 5 小時

換算大概 88M bit/s ➔➔➔
USB 2.0 的速度

網路加碼爆料(http://sony.attributed.to/)
稱北韓真的有涉案

IP Indicators

IP Address	Country Geolocation	Description
203.131.222.102	Thailand	Malware C2
217.96.33.165		Malware C2
88.53.215.64	Italy	Malware C2
200.87.126.116		
58.185.154.99	Singapore	Malware C2
212.31.102.100	Cypress	
208.105.226.235	United States	Malware C2
125.183.249.218	North Korea	Communicating with 217.96.33.165
203.132.168.221	North Korea	
203.149.124.98	North Korea	Communicating with 58.185.154.99
150.107.68.133	North Korea	
58.181.42.23	North Korea	Logged into pastebin using the "GuardiansOfPeace" login id.

POWERCOM，首爾, 南韓

DreamcityMedia，京畿道平澤市，南韓

VITSSEN, 京畿道安養市, 南韓

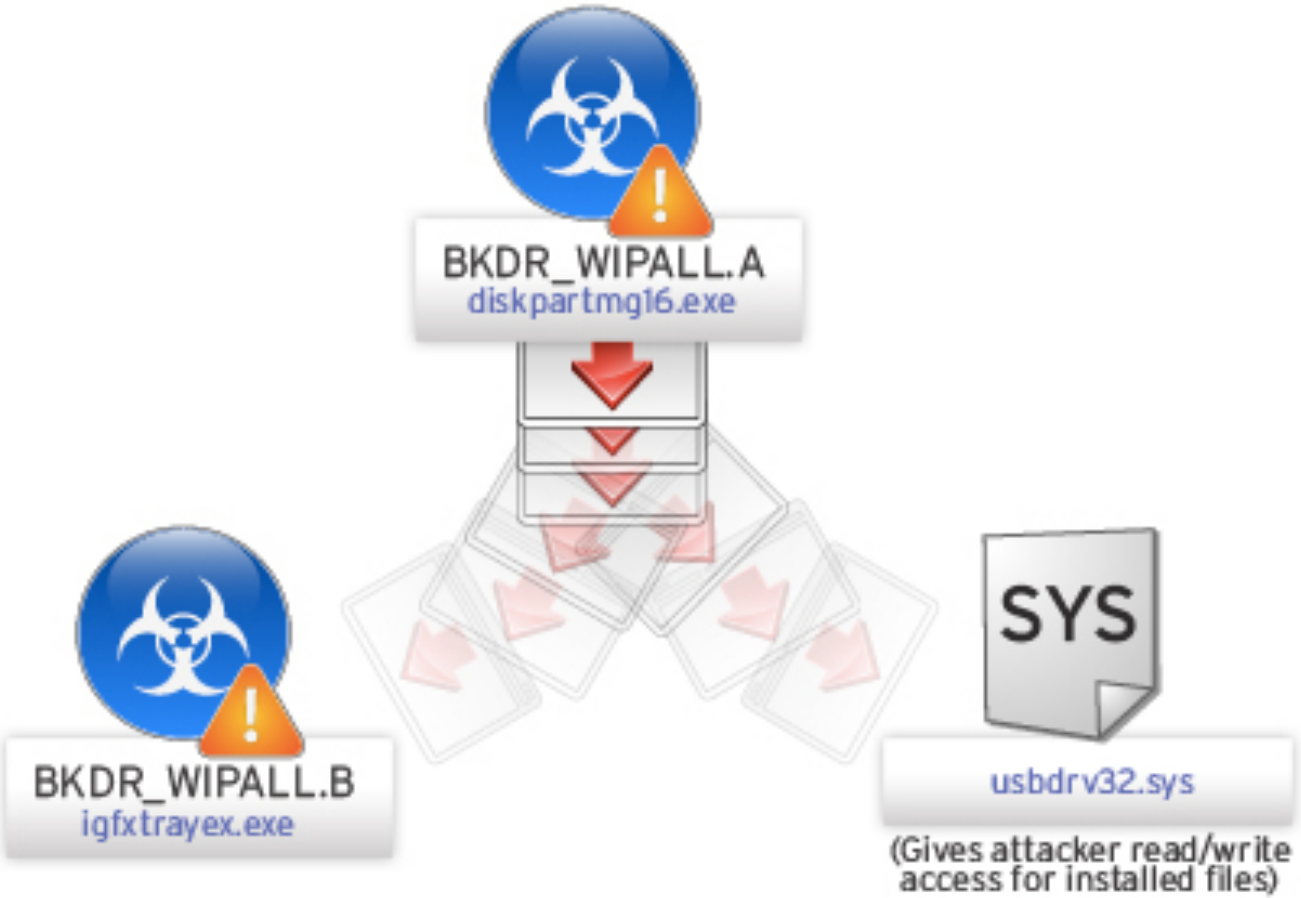
HOSTWAY, 江原道春川市, 南韓

VAAN，首爾, 南韓

個人觀點

- 行為大張旗鼓
  - 又勒索金錢, 又公佈資料, 怎看都不像國家級網軍會做的事情
- 技術層次不同
  - 2013/03/20 駭客有能力單一程式抹殺硬碟
  - 本次居然需要第三方驅動程式才能進行
- 程式碼分析沒有找到關聯性
  - 填入硬碟的字串 → 沒有關聯性
  - 相似的程式碼片段 → 沒有找到相似的

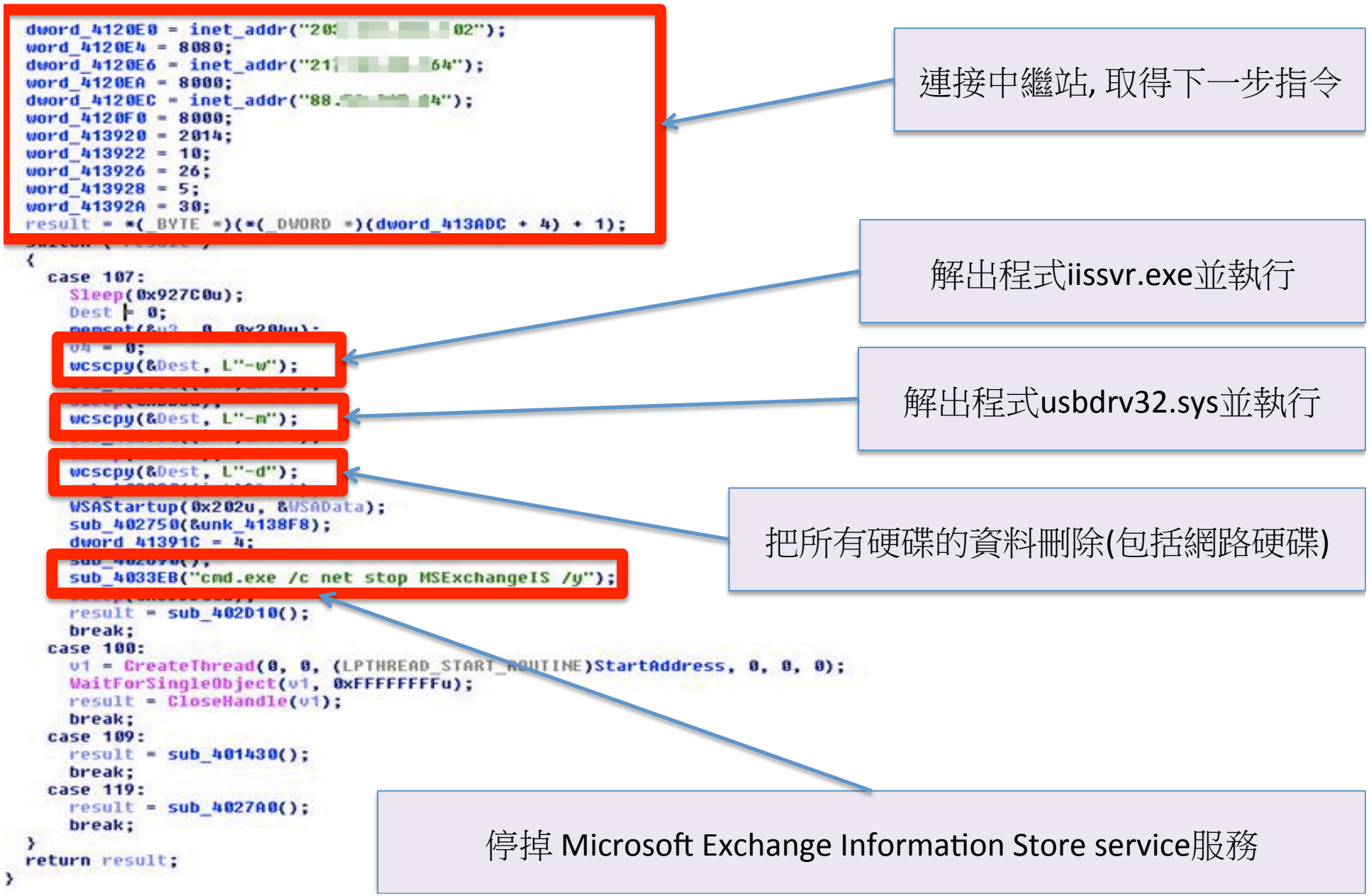
惡意行為分析 Part I



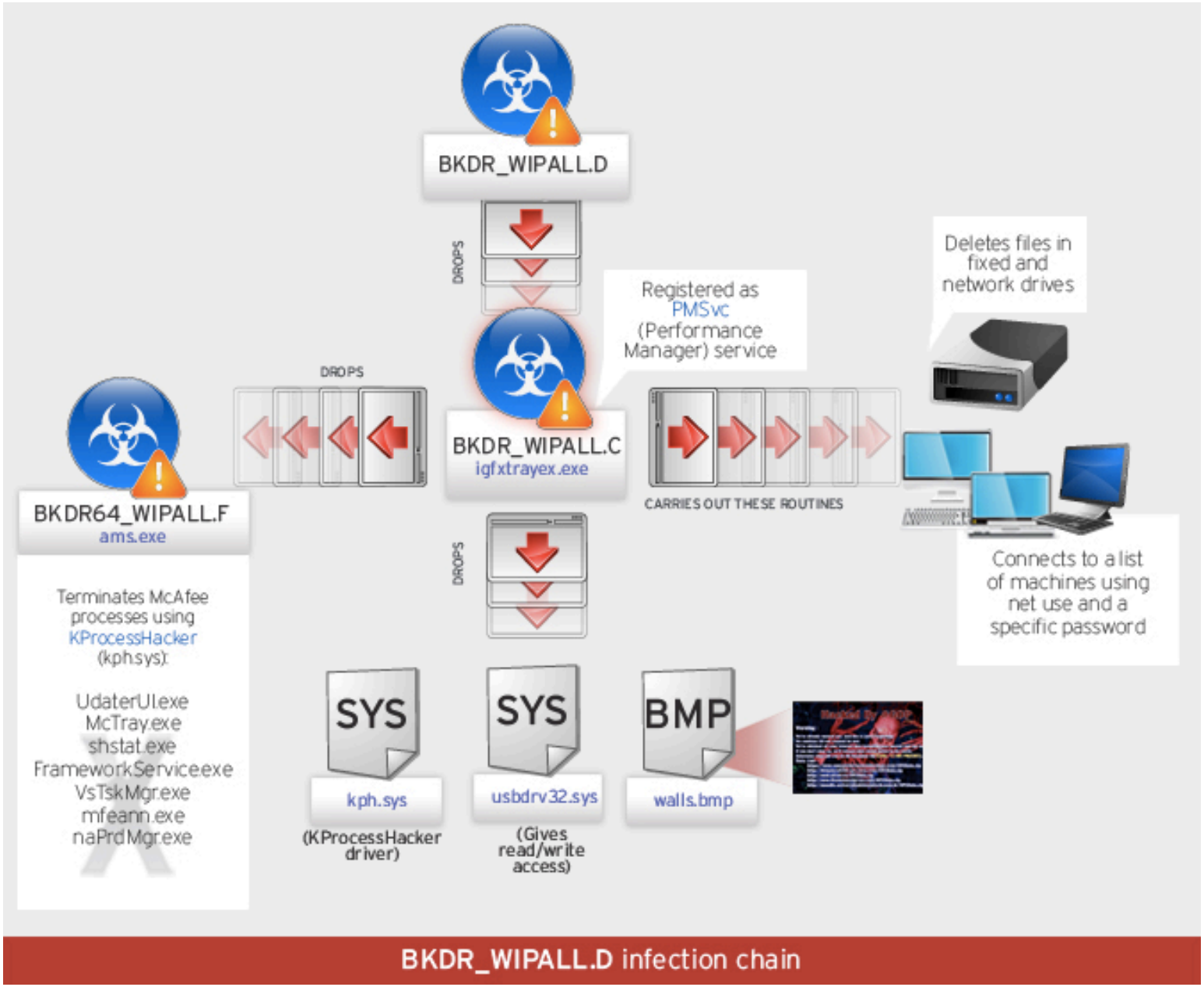
WIPALL infection chain

diskpartmg16.exe(BKDR_WIPALL.A)

igfxtrayex.exe(BKDR_WIPALL.B)



惡意行為分析 Part II



BKDR_WIPALL.D infection chain

BKDR64_WIPALL.F

- 安裝KProcessHacker 驅動程式
- 把下列McAfee程式停掉

  - *mcshield.exe*
  - *UdaterUI.exe*

```
mov     rcx, cs:qword_14000AF60
lea     rax, [rsp+68h+var_18]
xor     r8d, r8d
xor     edx, edx
mov     [rsp+68h+var_48], rax
call    cs:qword_14000AF58 ; ZwDeviceIoControlFile
add     rsp, 68h
retn
```


Confidential | Copyright 2014 TrendMicro Inc.

南韓核電廠事件

南韓核電廠遭駭，攻擊IP源自中國

- 負責南韓23個核電廠的**南韓水力與核電公社（Korea Hydro and Nuclear Power，KHNP）**在上周傳出遭到駭客入侵，南韓追查來源之後發現，攻擊IP位於中國。然而外電報導指出，南韓懷疑幕後黑手其實是北韓，因此已請求中國政府協助調查。

- 駭客自稱為「反核子反應爐集團主席」，並陸續公布南韓核電廠的平面圖、操作手冊，與超過1萬名KHNP的員工資料，要求南韓限時關閉3座核子反應爐，否則就要釋出更多機密資訊。

- 根據外電報導，南韓政府調查發現駭客利用了美國、日本，與南韓的虛擬私人網路等不同路徑以迴避追蹤，而最原始的攻擊IP則來自中國的瀋陽。由於瀋陽靠近中國與北韓的邊界，再加上瀋陽為北韓駭客聚集之地，南韓懷疑幕後黑手為北韓，並請求中國政府協助調查。

資料來源: ithome
http://www.ithome.com.tw/news/93200

事件發生時間表(1)

日期/時間	事件說明
2014.11.28	惡意HWP文件製作
2014.12.09 05:00—15:00	發送5980封惡意郵件給3571人
2014.12.10 11:00	惡意程式被觸發並執行
2014.12.10	內部網路惡意連線被偵測
2014.12.15	駭客在Naver部落格開始張貼文章
2014.12.15 20:01	駭客的facebook帳號建立

事件發生時間表(2)

日期/時間	事件說明
2014.12.15 20:14	部落格第一次發文
2014.12.15 20:33	部落格第二次發文, 公佈內部員工資料
2014.12.15 20:37	部落格第三次發文, 勒索金錢
2014.12.15 20:40	部落格第四次發文, 宣稱有機密資料
2014.12.15 20:42	部落格第五次發文, 發佈海報, 駭客團體“Who AM I”
2014.12.15 23:41	駭客的twitter帳號建立

事件發生時間表(3)

日期/時間	事件說明
2014.12.16 01:00	Twitter首次發佈鏈結, 可下載資料
2014.12.18 14:00	Twitter二度發佈鏈結, 公佈另外下載資料
2014.12.18 18:40	Naver的駭客帳號變成私密帳號
2014.12.19 20:20	Twitter三度發佈鏈結, 公佈另外下載資料
2014.12.21 01:30	Twitter四度發佈鏈結, 公佈另外下載資料
2014.12.23 15:07	Twitter五度發佈鏈結, 公佈另外下載資料

事件發生時間表(4)

日期/時間	事件說明
2014.12.23	韓國政府聯合調查團 發現攻擊來源是從三個VPN端點, 並請求中國協助調查
2014.12.25	青瓦台召開核能電廠中斷可能性安全評估10人小組
2014.12.26	決議核電營運繼續, 然後緊急反應小組待命到12/31日
	同日3號機組氣體外洩導致三人死亡, 排除跟本次駭客相關
	北韓官方”民主朝鮮”否認本次行動
2014.12.28	KHNP自行調查結果發現共有12類型,117件資料外洩

惡意程式列表

檔名	類型
사업계획서.hwp　(商業計劃書.hwp)	Dropper
외교통일안보요지서.hwp (外交與統一的安全框架.hwp)	Dropper
훈련소.hwp (培訓學校.hwp)	Dropper
보고서취합본.hwp (報告匯整.hwp)	Dropper
안보의견.hwp (安全意見.hwp)	Dropper
제어program(최신-W2).hwp (控制程序(最新-W2).hwp)	Dropper
자료_2014.hwp (數據_2014.hwp)	Dropper
wsss.dll	Wiper

攻擊意示圖

攻擊ＩＰ

中國瀋陽　美國　日本

南韓境內三家VPN業者

Facebook　Twitter　Pastebin

連結散佈

Dropbox　NAVER

外洩資料

KHNP

外部電腦

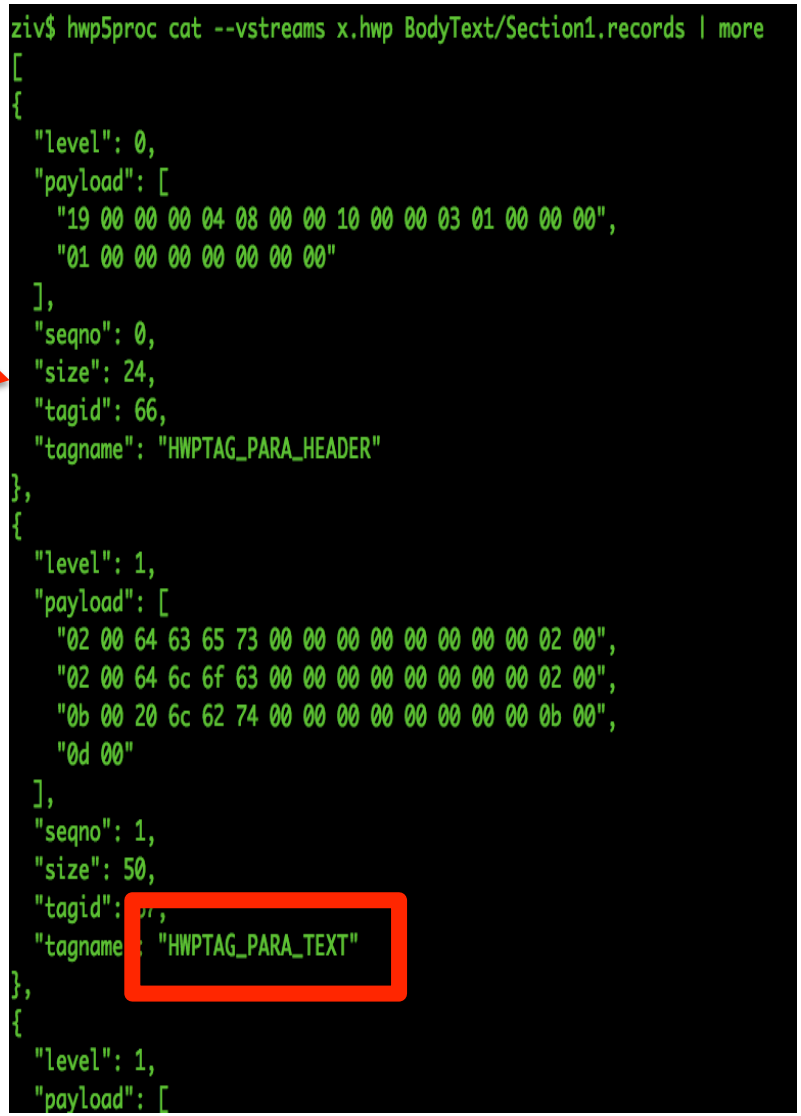
內網電腦

惡意程式分析


Spearphishing email
TROJ_MDROP.WQA
TROJ_WHAIM.A
Targets 32-bit playform.
Contains an embedded
64-bit version
Infection Chain for MBR Wiper Attack

惡意程式分析 II

```
ziv$ hwp5proc ls x.hwp
\x05HwpSummaryInformation
BodyText/Section0
BodyText/Section1
BodyText/Section2
BodyText/Section3
BodyText/Section4
BodyText/Section5
BodyText/Section6
DocInfo
DocOptions/_LinkDoc
FileHeader
PrvImage
PrvText
Scripts/DefaultJScript
Scripts/JScriptVersion
```



企業如何因應！？

- 防護思維要改變
  - 重兵防守前線的時代已經過去, 要思考駭客在大後方作亂的解決方案
  - 不要關起門來處理, 要廣邀外界專家協助
- 緊急事件反應小組(IR)要成立
  - 要有專職人員隨時注意外界資安新知/消息
- 擁抱新科技
  - SDN security, IoT/IoE security,.....
  - 桌移小強出的新概念