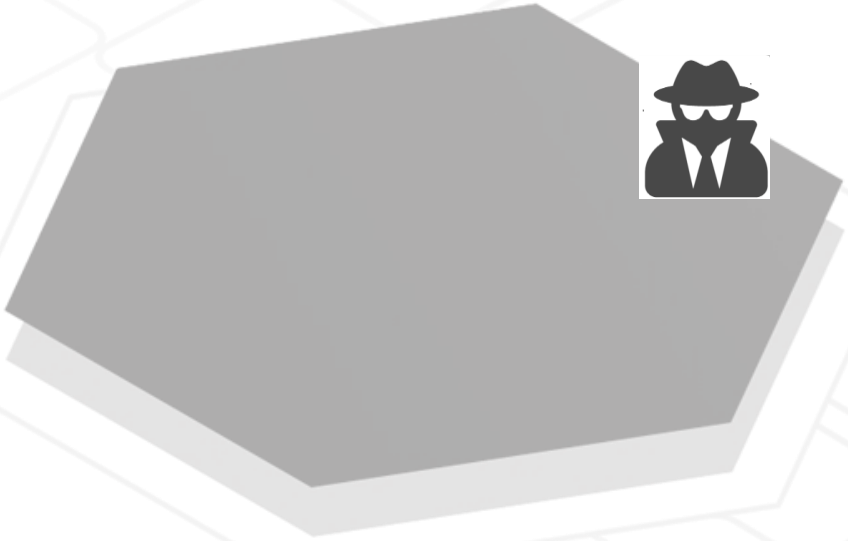
詮睿科技
TALENT JUMP

以藍隊角度探討
入侵事件處理常見問題



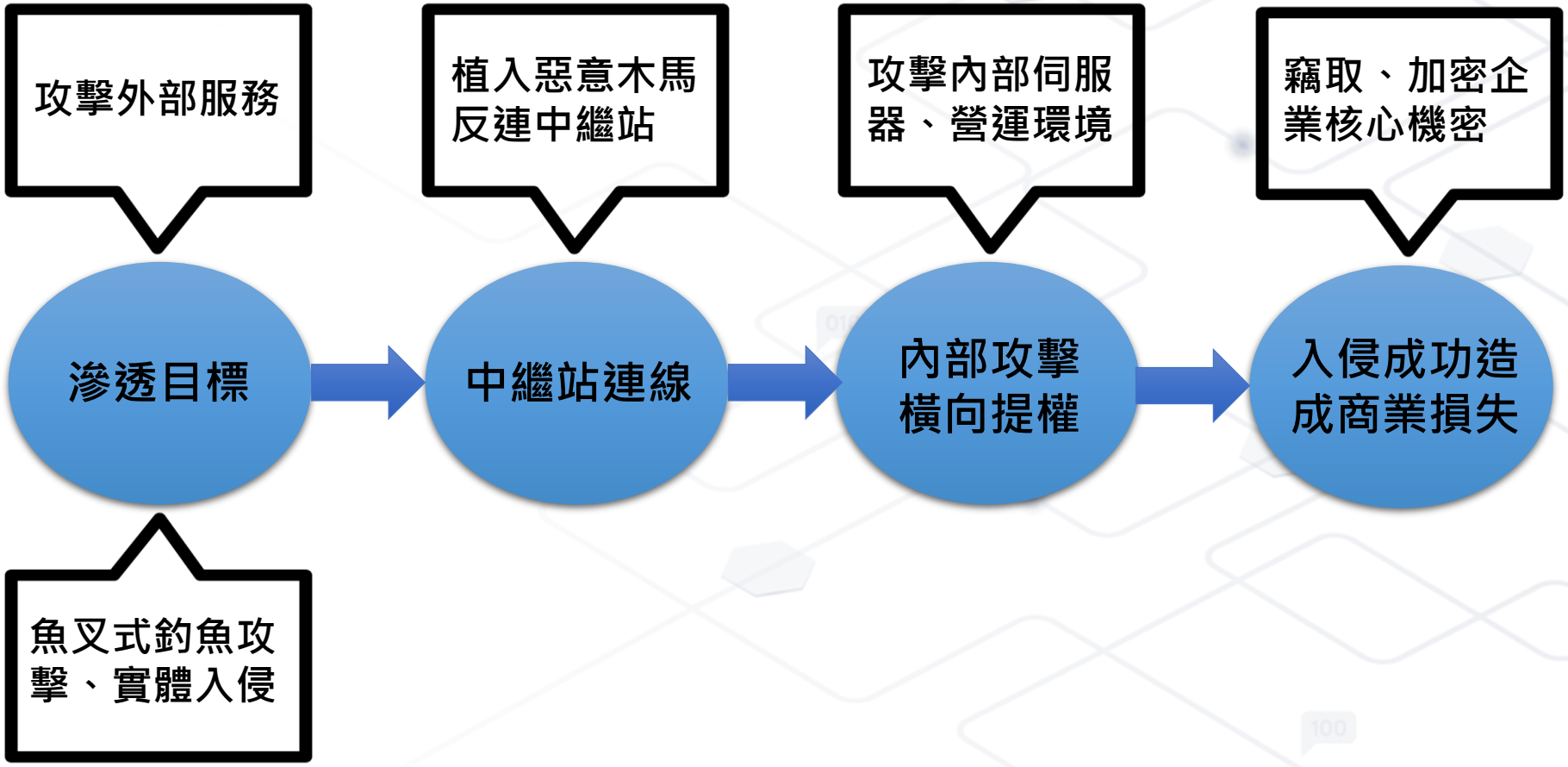
- Zero Chen (祭肉陳)
- 詮睿科技股份有限公司
- 自 2008 年開始從事資安相關工作
- 專長是邊喝酒邊打站或挖貓胃 (X　撸貓 (O
- KMPlayer SCA、Operation DRBControl

Agenda

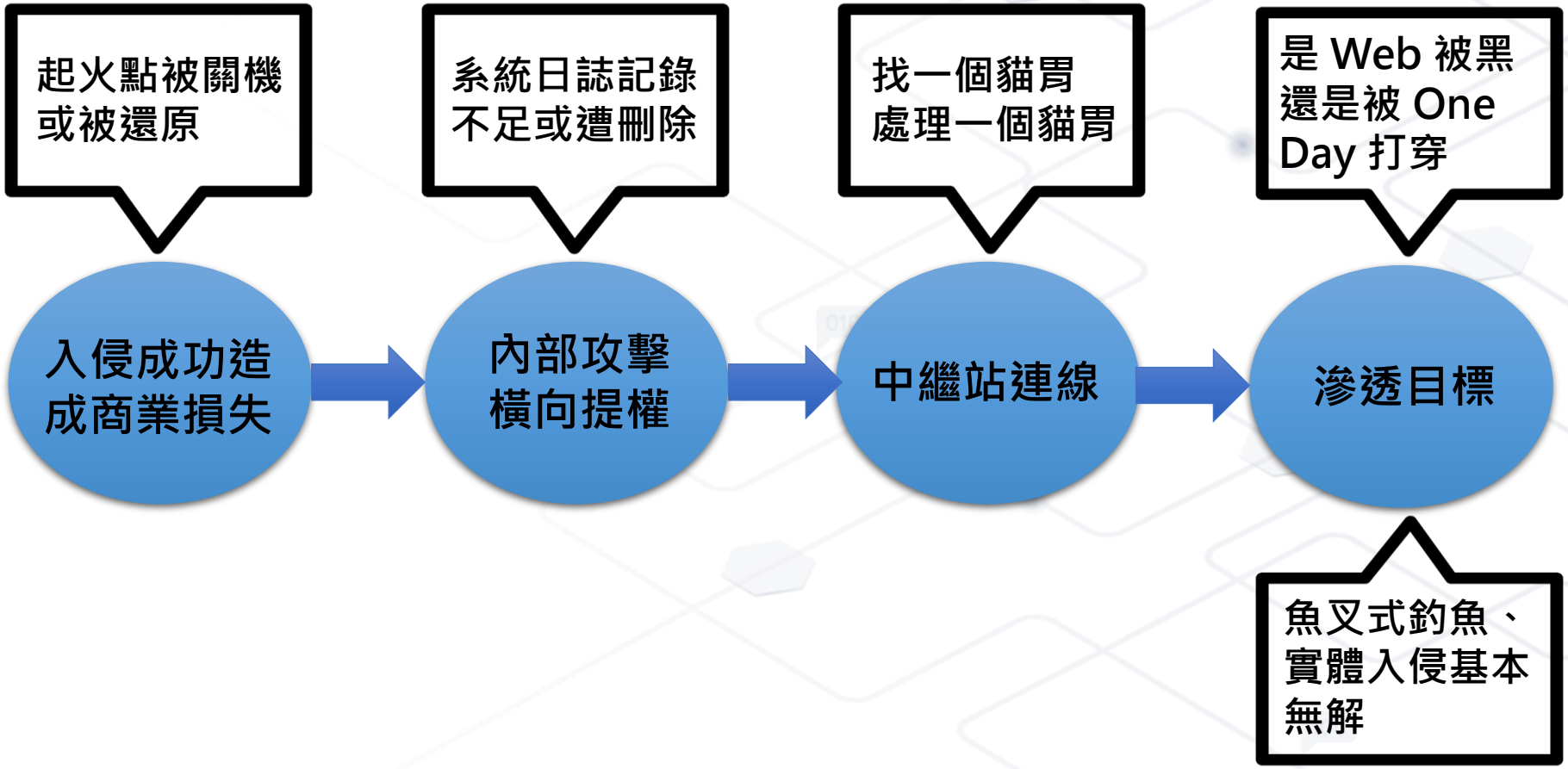
- 事件處理經常遇到的困擾
- 常被攻擊者利用的對象
- 主動出擊的小撇步
- 事前、事中與事後

事件處理經常遇到的困擾

攻擊者入侵流程


攻擊外部服務
植入惡意木馬
反連中繼站
攻擊內部伺服
器、營運環境
竊取、加密企
業核心機密
滲透目標
中繼站連線
內部攻擊
橫向提權
入侵成功造
成商業損失
魚叉式釣魚攻
擊、實體入侵

事件處理流程


起火點被關機
或被還原
系統日誌記錄
不足或遭刪除
找一個貓胃
處理一個貓胃
是 Web 被黑
還是被 One
Day 打穿
入侵成功造
成商業損失
內部攻擊
橫向提權
中繼站連線
滲透目標
魚叉式釣魚、
實體入侵基本
無解

常見困擾，常見解法

- 盡可能保留現場進行事件調查

- 系統日誌是調查事件的主要依據之一
  - 存放空間務必確認足夠
  - Audit Policy 必須統一
  - Process Command-line Audit 切記打開
  - 盡可能將日誌收容到 SIEM 備查
  - 可以的話把 Sysmon 也裝起來

- 避免與攻擊者龜兔賽跑
  - 優先調查並確認、隔離確保營運環境可正常運作
  - 全面調查搜集相關威脅情資指標
  - 做好完善的隔離、重置計劃後一次處理

- 在處理過程盡可能找出事件根源並改善
  - 找不到怎麼辦？從網路、系統管理架構下手
  - 平行單位不配合，怎麼辦?

常被攻擊者利用的對象

眼見不一定為真

- 貓胃藏在系統的各種手法
  - 直接寫成一個新的 Service
  - 掛在 TaskScheduler 裡
  - Payload 分段混淆後寫在機碼表裡
  - 利用各大廠公用程式做 dll side-loading
  - 直接掛 Windows Default Service 裡
  - Powershell fileless 藏在 WMI consumer instance 裡
  - … 族繁不及備載

- 共通點：Loader 大部份都透過正常程序做掛載

千萬不要期待貓胃還會長的這麼容易辨識

svchostt_vi...

搜尋 svchostt_virus

名稱	修改日期	類型	大小
svchostt.exe	2019/10/6 上午 05:47	應用程式	661 KB

svchostt.exe - 內容

一般 | 相容性 | 安全性 | 詳細資料 | 以前的版本

svchostt.exe

檔案類型:	應用程式 (.exe)
描述:	svchostt.exe
位置:	C:\Users\zerochen\Desktop
大小:	660 KB (676,352 位元組)
磁碟大小:	664 KB (679,936 位元組)
建立日期:	2019年10月6日, 上午 05:58:1
修改日期:	2019年10月6日, 上午 05:47:1
存取日期:	2021年5月5日, 下午 07:25:38

svchostt.exe - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

?l%S#[k= 叡7H??凳 = ?V1 ?氦糖焲2= 綁q ??? ?= 例阽 ? ?5 = x職/@? "B <1= ? -!y?= X?z
萃?~?b>?= ? 跘?? #.X'= HBO &??? ~ = x 在b? . ?= 釮默 ?y7 i9+= v轅?? 操?= 0誧??2媔 ?8= x D?
X?1?= 濛? 濛? Q? Q? 謶? 謶? ?? ?? ?? ?? ? ?]?]? P ? P ? 拂? 拂? 豥? 豥?
(? (? `脂? `脂? ? ? ?? ?? 譆? 譆? 肛? 肛? ?? ?? p嬯? p嬯? 忱? 忱? (e? (e?
@#? @#? 凈? 凈? `耒? `耒? hk? hk? ?? ?? x灃? x灃? 碩? 碩? ? ? 鑞? 鑞? x ?
x ? p蔎? p蔎? 鉦? 鉦? 堷? 堷? HN? HN? ?? ?? ? ? ? ? p ? p ? Xi? Xi? ??
?? ?? ?? 橤? 橤? 娷? 娷? 8 ? 8 ? s? s? pl? pl? ?? ?? ? ? ? ? 銊? 銊? o? o? *?
*? 濮? 濮? ` ? ` ? Z? Z? ?? ?? 0笴? 0笴? ?? ?? PY? PY? ?? ?? `蓏? `蓏? 薴? 薴?
pm? pm? /? /? 鼲? 鼲? 檢? 檢?Unknown exception : generic Fail to schedule the chore! This function
cannot be called on a default constructed task broken promise future already retrieved promise already satisfied
no state future bad locale name * \ S O F T W A R E \ M e d u s a N a m e
S O F T W A R E \ M i c r o s o f t \ W i n d o w s \ C u r r e n t V e r s i o n \ P o l i c i e s \ S y s t e m E n a b l e L i n k e d C o n n e c t i o n s S O F T W A R E \ M i c r o s o f t \ W i n d o w s \ C u r r e n t V e r s i o n \ P o l i c i e s \ S y s t e m E n a b l e L i n k e d C o n n e c t i o n s [L O C K E R] S c a n P r e s s O K t o c o n t i n u e [L O C K E R] I s r u n n i n g
{ 8 7 6 1 A B B D - 7 F 8 5 - 4 2 E E - B 2 7 2 - A 7 6 1 7 9 6 8 7 C 6 3 } [L O C K E R] I s a l r e a d y r u n n i n g
[L O C K E R] P r i v : A D M I N
[L O C K E R] P r i v : U S E R
Its just a business. If we do not do our work and liabilities- nobody will not cooperate with us.<b
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:
<d>{{IDENTIFIER}}</d>

詮睿科技 TALENT JUMP

Oracle

jjs.exe
msvcr100.dll
svchost.bin

jjs.exe - 內容

一般 | 相容性 | 數位簽章 | 安全性 | 詳細資料

簽章清單

簽署人的...	摘要演算...	時間戳記
Oracle A...	sha1	2018年3月2...

jjs.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	Java(TM) Platform SE binary
類型	應用程式
檔案版本	8.0.1710.11
產品名稱	Java(TM) Platform SE 8
產品版本	8.0.1710.11
著作權	Copyright © 2018
大小	16.4 KB
修改日期	2018/4/27 下午 12:34
語言	中性語言
原始檔名	jjs.exe

CyberArk

- config.ini
- msmpeng.exe
- thumb.dat
- vftrace.dll

msmpeng.exe - 內容

一般 | 相容性 | 數位簽章 | 安全性 | 詳細資

簽章清單

簽署人的...	摘要演算...	時間戳記
Viewfinit...	sha1	2016年1月5.

msmpeng.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	CyberArk Viewfinity
類型	應用程式
檔案版本	5.5.10.101
產品名稱	CyberArk Viewfinity
產品版本	5.5.10.101
著作權	Copyright © 1999-2016 CyberArk Software Ltd. All Ri...
大小	343 KB
修改日期	2020/9/25 下午 01:24
語言	英文 (美國)
原始檔名	vf_host.exe

詮睿科技
TALENT JUMP

Windows Defender

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

簽章清單

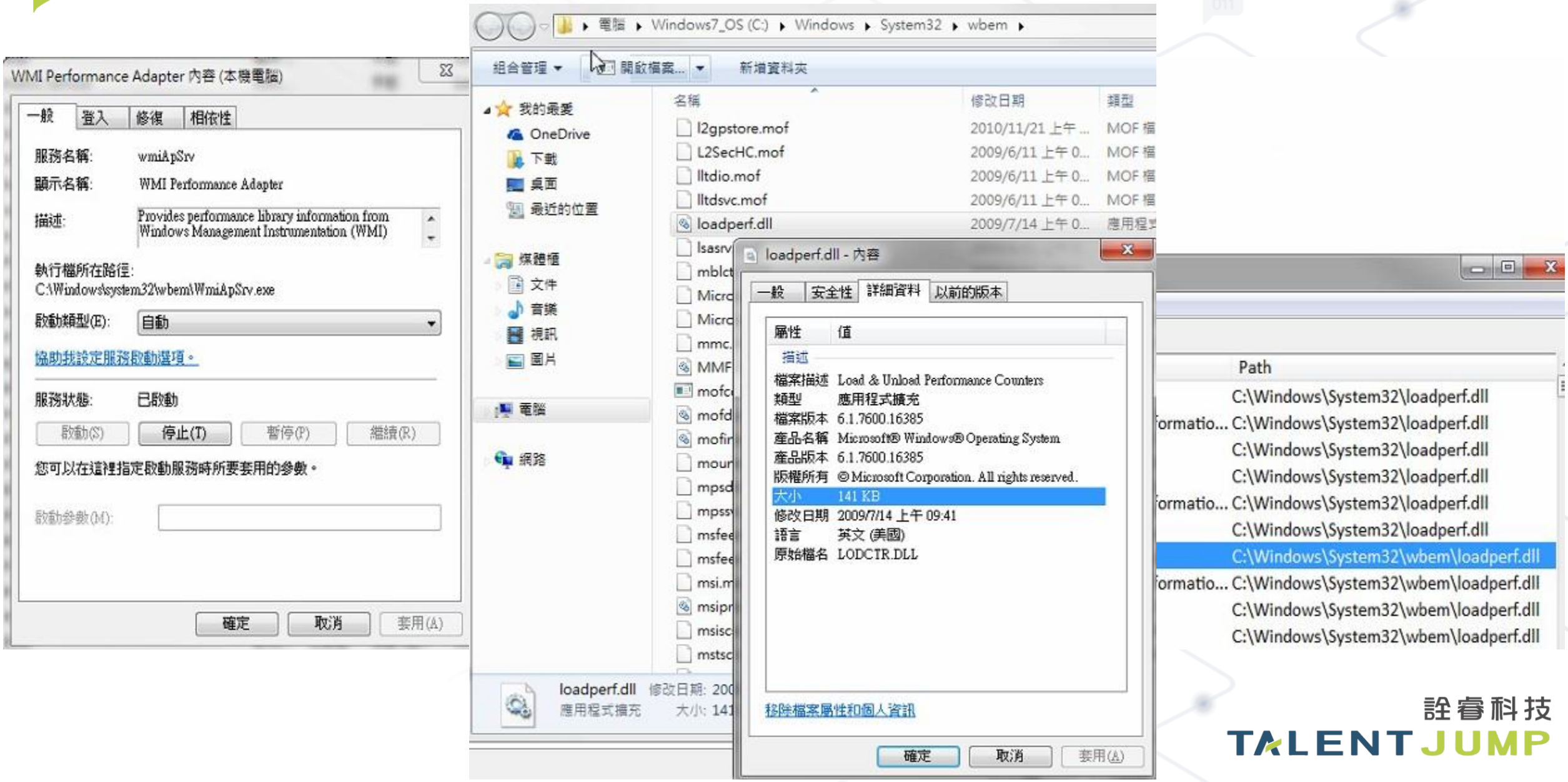
簽署人的名稱:	摘要演算...	時間戳記
Microsoft Corporation	sha1	2015年4月3...
Microsoft Corporation	sha256	2015年4月3...

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

Windows WMI



詮睿科技
TALENT JUMP

Symantec

ctLXcGcaxC
NAVLU.dll
VPDN_LU.exe

VPDN_LU.exe - 內容

一般 | 相容性 | 數位簽章 | 安全性 | 詳細資料 | 以

簽章清單

簽署人的名稱:	摘要演算...	時間戳
Symantec Corporation	sha1	2007年

VPDN_LU.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	Symantec AntiVirus
類型	應用程式
檔案版本	10.1.6.6000
產品名稱	Symantec AntiVirus
產品版本	10.1.6.6000
著作權	Copyright 1991 - 2006 Symantec Corporation. All rig...
大小	74.1 KB
修改日期	2014/8/27 上午 11:57
語言	英文 (美國)

詮睿科技
TALENT JUMP

McAfee

Mc.cp
Mc.exe
McUtil.dll

Mc.exe - 內容

一般 相容性 數位簽章 安全性 詳細資

簽章清單

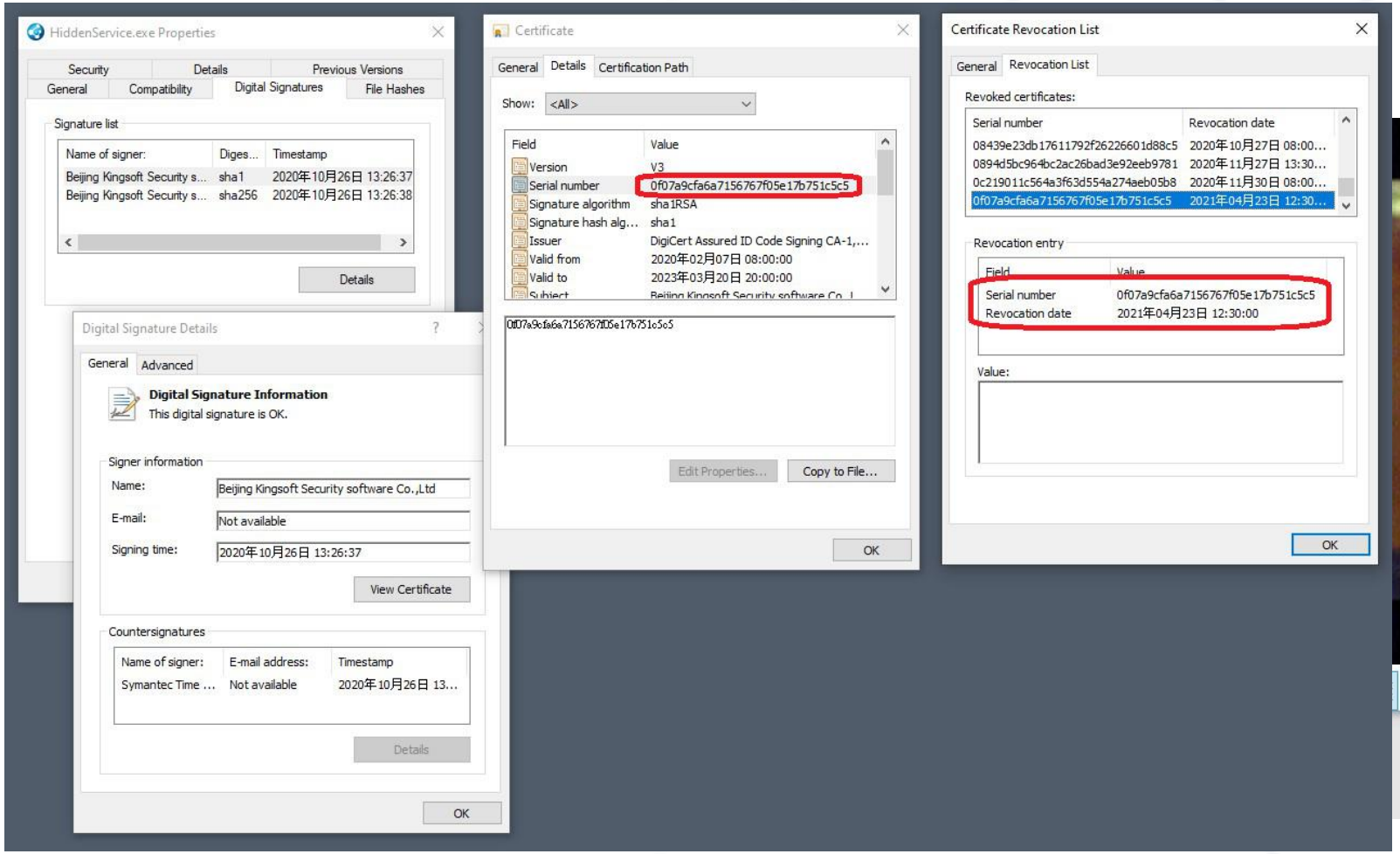
簽署人的...	摘要演算...	時間戳記
McAfee, I...	md5	2008年6月1

Mc.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	McAfee OEM Info Copy Files
類型	應用程式
檔案版本	2.1.115.0
產品名稱	McAfee Oem Module
產品版本	2,1,0,0
著作權	Copyright © 2006 McAfee, Inc.
大小	137 KB
修改日期	2008/6/12 上午 12:40
語言	英文 (美國)
原始檔名	mcoemcpy.exe

Iron Tiger aka APT 27 Luckymouse

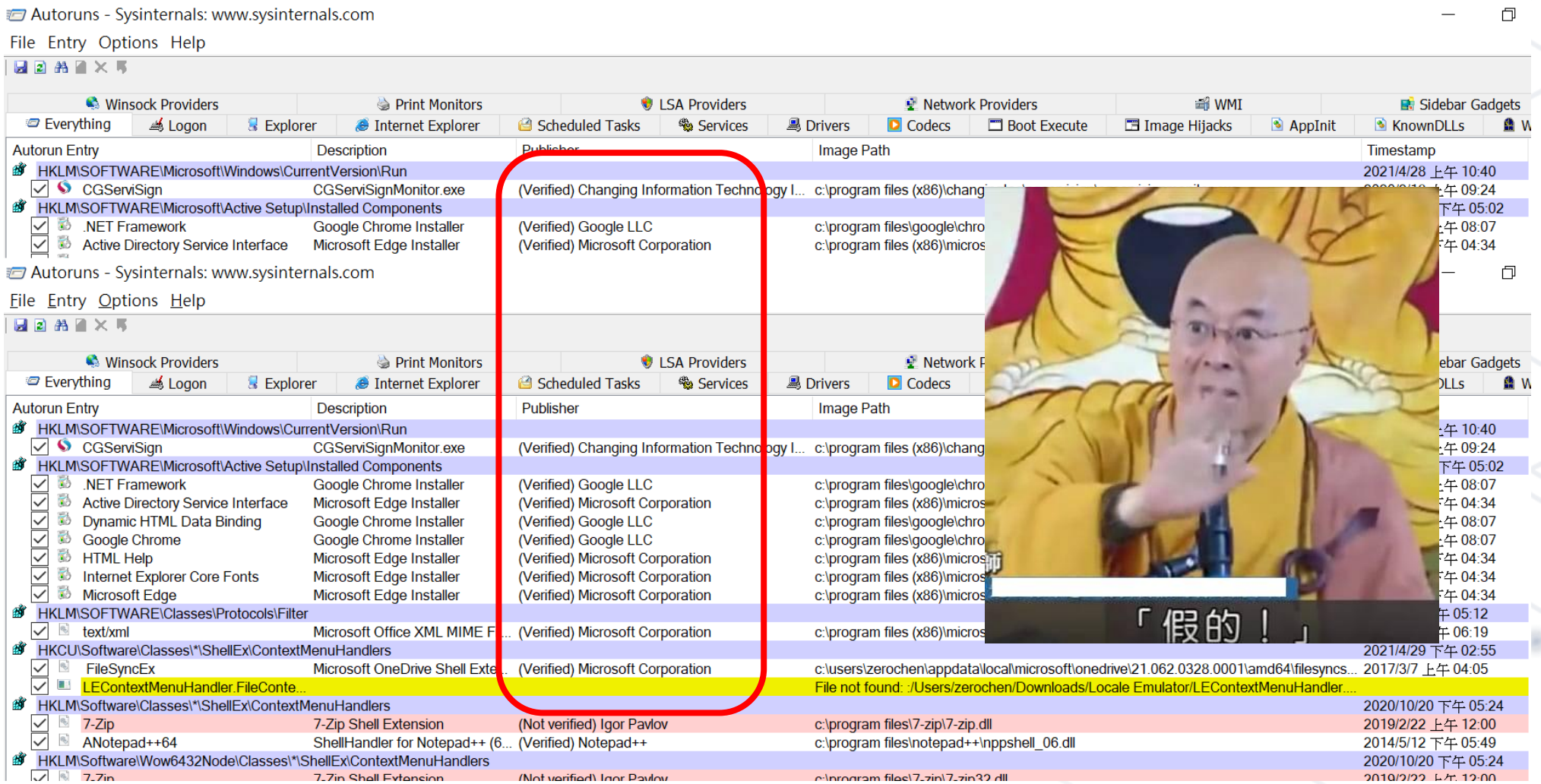


下午 08:21
星期三
2021/5/5

https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

詮睿科技 TALENT JUMP

常用的工具：Autoruns



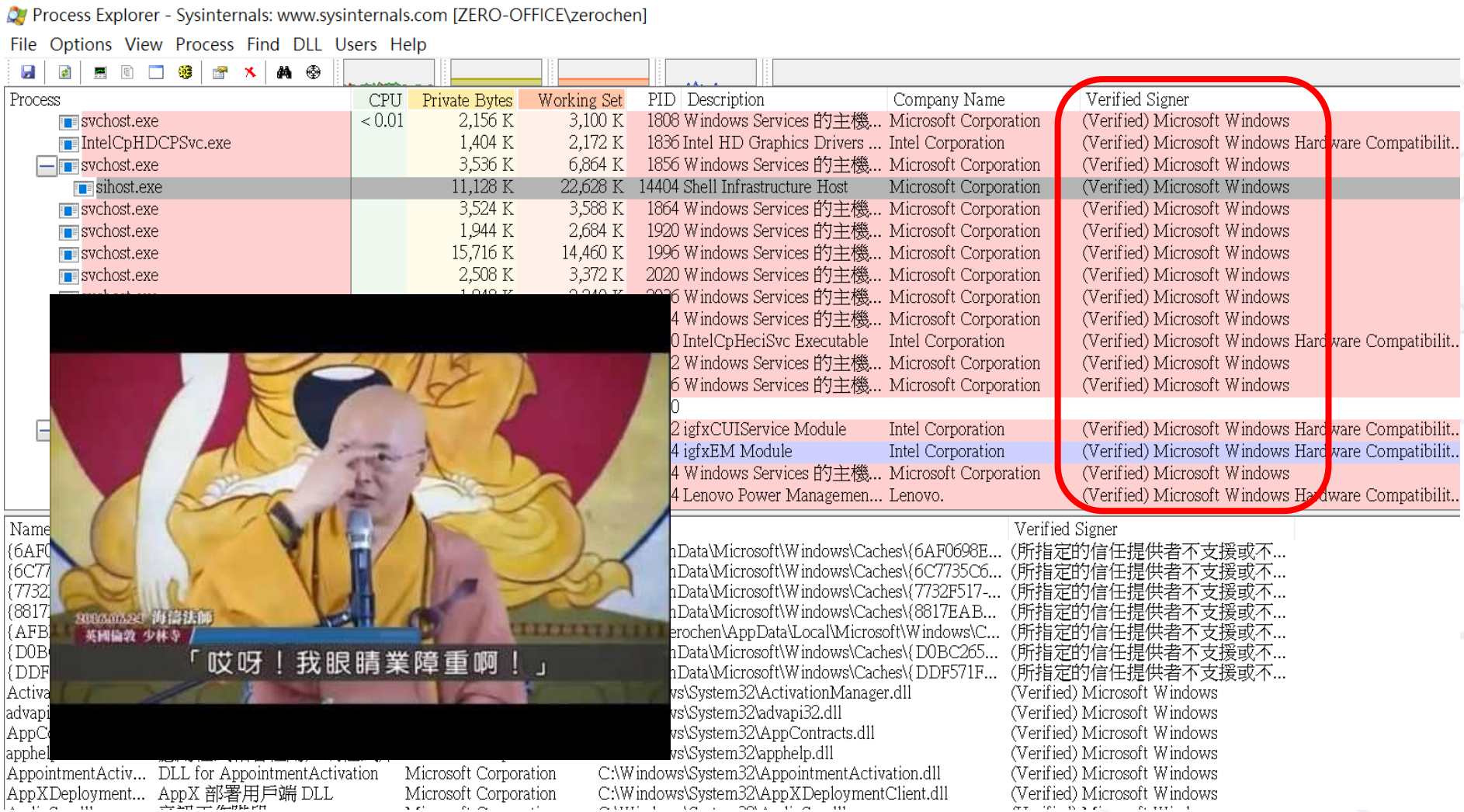
詮睿科技
TALENT JUMP

眼見不一定為真 (Part 2)

- 貓胃喜歡注入的程序
  - svchost.exe
  - explorer.exe
  - msiexec.exe
  - iexplorer.exe
  - msdtc.exe
  - dllhost.exe
  - … 族繁不及備載

- 共通點：大多是注入到正常的公用程序

常用的工具：Process Explorer



詮睿科技
TALENT JUMP

現況反思

- 第三方或官方程式遭利用成 Loader 已是不爭的事實
- 數位憑證被盜用(?)於簽屬貓胃已相當常見
- 被注入的程序基本都是正常程序
- 敵暗我明，攻擊者深知如何運用合法掩飾非法

主動出擊的小撇步

小撇步一：第一時間知道資料被撈了

- 主動出擊，在重要的資料庫內插入特定(假)資料

- 透過各種方式進行監控(假)資料
  - DB Auditing 工具
  - 程式自己寫 Log
  - 寫個 Trigger 偵測

- 假資料一般不會被撈取，主動式守株待兔的概念

- 但如果必須遵守法規這招可能就…（Ex: PCI-DSS、資通安全法）

小撇步二：偵測疑似惡意活動

- 將 Event ID 7045 拉出來做個 Index List
  - 每日比對，找出差異項目（Outlier）做檢查
  - 針對特定常用於橫向攻擊的字串做檢查（Ex: PsExec / PSEXECSVC）

- 開啟 Process Command-line Audit，Event ID 4688
  - nmap, copy, xcopy, rar, nbtscan, net use
  - powershell.exe -w hidden -enc
  - ping –n 1 xxx.xxx.xxx
  - 還有很多，這裡講不完

- 但前提是得有個 SIEM，有的話可以參考這裡

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation

小撇步三：利用 YARA 偵測具特定特徵的貓胃

- 以前述 jjs.exe 為例子
  - Loader 一樣，但 dll 有小改 C2 DDNS 不同，無法透過 HASH 一次清查
  - 透過各種靜態、動態分析的方式分析樣本的威脅指標（IoCs）

jli.dll - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

```
g: ?  (u      R fnx   V   ?g:       UO
g: ? \翅掞/T沖 0 W e b _ C l i e n t   uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
 s v c h o s t . b i n  \svc   ho st. exe a c:\users\hellokety.ini EINFO_INDENT   %s 渠葬反
卞勾中化）毕銘旎狟及撈弇30爛毛蛅丹懂爛2堎24    及?癩宅萎摽午允月源砑匹捼淕
眕蔥'旎狟撈弇30爛宅萎卞饜   求渠葬捼淕  H U I H W A S D I H W E I U D H D S F S F E F
E F W F W E W D      H                                p    讋          託 胇 ?            ?
```

jli.dll - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

```
a  FreeEnvironmentStringsW ?GetEnvironmentStringsW  ?QueryPerformanceCounter
f  SetFilePointer  ?GetConsoleCP  ?GetConsoleMode  r  GetCPInfo h  GetACP  7  GetO
  IsValidCodePage g  MultiByteToWideChar ? CreateFileA d CompareStringW  V  SetEn
HeapReAlloc ?SetStdHandle  $  WriteConsoleW-  LCMapStringW  i  GetStringTypeW
W  FlushFileBuffers  S  SetEndOfFile  ?ReadFile                    Z?            (?  <?  P?
jli.dll JLI_CmdToArgs JLI_GetStdArgc JLI_GetStdArgs JLI_Launch JLI_MemAlloc
```

jli_dll.yar - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

```
rule jli_dll_hellokety
{
        meta:
                author = "talent-jump.com"
                date = "2019/03"
                maltype = "PlugX Java Launcher jli.dll"
                filetype = "dll"

        strings:
                $string0 = "LoadLibraryA"
                $string1 = "CreateProcessA"
                $string2 = "CreateRemoteThread"
                $string3 = "hellokety"
                $string4 = "JLI_Launch"
                $string5 = "WriteProcessMemory"

        condition:
                all of them
}
```

  - 但要有個支援 YARA 的工具，更多細節可參考：
    https://github.com/VirusTotal/yara/releases

詮睿科技 TALENT JUMP

小撇步四：防毒的參考指標

- 防毒軟體的現況
  - 裝安心的，反正偵測不到太多新型病毒
  - 有病毒警訊就重灌啊，哪次不重灌的
  - 但倘若偵測到的檔案路徑是以下這些....

/Windows/
/Windows/System32/
/Windows/System32/{$RandomNamed}/
/Windows/System32/wbem/
/ProgramData/
/Users/{$YourName}/AppData/
/Program Files/Common Files/
/$RECYCLE.BIN/

- 我們其實可以再給防毒軟體一個機會

小撇步五：資安規範很重要，但續命的取捨?

- 情境範例：某公司資安規範
  - Endpoint、伺服器均需加入 AD 進行統一管控
  - 因此即便是 Backup Server 也需遵守此規範

- 攻擊者進到內部環境後
  - 當然先拿 Credential 啊
  - 然後立馬打 AD 啊，哪次不打的
  - AD 被打穿，包含 Backup Server 在內全通
  - 內網摸透後來個加密勒索，Backup Server 當然也一併加密囉

- 所以… 開特例把 Backup Server 特別隔離的取捨?

小撇步六：有時被黑可以反追蹤唷

- 以 DRBControl 為案例
  - 在調查過程中發現攻擊者植入的樣本
  - 經過分析調查發現樣本有與 Dropbox 互動傳遞資料
  - 逆向分析過程發現 Dropbox 的 API Access Token
  - 運用該 API Access Token 進行反追蹤

```
dropbox_token[0] = 'c';
dropbox_token[1] = '3';
dropbox_token[2] = 'K';
dropbox_token[3] = 'C';
dropbox_token[4] = 'C';
dropbox_token[5] = 'd';
dropbox_token[6] = 'c';
dropbox_token[7] = '9';
dropbox_token[8] = 'Y';
dropbox_token[9] = 'z';
dropbox_token[10] = '[redacted]';
dropbox_token[11] = '[redacted]';
dropbox_token[12] = '[redacted]';
dropbox_token[13] = '[redacted]';
dropbox_token[14] = '[redacted]';
dropbox_token[15] = '[redacted]';
dropbox_token[16] = '[redacted]';
dropbox_token[17] = '[redacted]';
dropbox_token[18] = '[redacted]';
dropbox_token[19] = '[redacted]';
dropbox_token[20] = '[redacted]';
dropbox_token[21] = '[redacted]';
dropbox_token[22] = '[redacted]';
dropbox_token[23] = '[redacted]';
```

- 進一步分析 Dropbox 上的資料可得知
  - 攻擊者偷取的資料與確切的受駭範圍
  - 更多可進一步分析的樣本與 IoCs
  - 可讓事件處理的更加有效率與完整

http://www.talent-jump.com/article/2020/02/17/CLAMBLING-A-New-Backdoor-Base-On-Dropbox/

事前、事中與事後

SANS Incident Response 6 steps

Preparation

- People
- Notes
- Relationships
- Policies
- Procedures
- Coms plan
- Tools
- Mgt Tng
- Training
- Jump Bag

Identification

- Awareness
- Need to Know
- Unusual processes
- Unusual Security Evts
- Alert Early
- Use OOB Comms
- New Accts / Privs
- Primary IR Handler
- Passive monitoring
- Odd Sch Tasks
- Unusual Files
- Analyze Logs
- Chain of Custody

Containment

- Stop Bleeding
- Categorize
- Notify Mgt
- Remove LAN Cbl
- Memory Captures
- Chg Pswds
- Short-term
- Criticality
- Asgn Primary IRH
- FW/IDS Filters
- Adjacent Host Logs
- Kill Backdoors
- Back-up
- Sensitivity
- Low Profile
- ISP coord
- Patch Exploited Vuln(s)
- Long-term
- Document Actions
- Infected Vlan
- Forensic Images

Eradication

- Del Artifacts
- Apply All Patches
- Black Hole IP's
- Root Cause
- Addl FW / IDS Filters
- Seek other Host footholds
- Restore Back-up
- Chg DNS Names
- Wipe/Format/Rebuild
- Remove Malware
- Rescan network

Recovery

- Return to Ops
- Monitor (signs/shells/artifacts/events)
- Test /Doc Baseline
- Move to Production (Approval)
- Script searches for attacker artifacts

Lessons Learned

- Document Incident
- All affected parties review / comment on draft
- Finalize Report
- Seek Required Changes
- Immediately upon recovery Phase
- Provide Exec Summary
- Seek Funding
- Assign to on-Scene IRH
- Reach Report Consensus
- Address Process not people
- Update Procedures

詮睿科技
TALENT JUMP

SANS Incident Response 6 steps

- Preparation
  - 訂立企業資安策略
  - 定期進行風險評估
  - 定義企業核心資產及應關注事件
  - 成立 CSIRT 小組
- Identification
  - 監控系統異常事件
  - 分析事件實際影響層級
  - 確認事件後收集證據、記錄實際狀況
- Containment
  - 進行網路隔離遏止攻擊繼續擴散
  - 持續監控並控制現況
  - 維持系統可用性並執行重建計劃
- Eradication
  - 確認事件根源
  - 清理確認或疑似受駭系統
  - 透過各資安設備阻擋事件 IoCs
- Recovery
  - 確認還原、重建後的系統完整性
  - 提升系統安全性
  - 持續監控異常事件
- Lesson Learned
  - 記錄事件發生詳細情況
  - 檢視事件處理流程是否完善
  - 針對事件根因策劃未來改善方向

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

很重要所以我得呼籲個三次

- 資安的層級倘若與其他單位相對等，CSIRT 的領導者就必須是居上位者
- 資安的層級倘若與其他單位相對等，CSIRT 的領導者就必須是居上位者
- 資安的層級倘若與其他單位相對等，CSIRT 的領導者就必須是居上位者

HITCON 2021

WORK FROM HOME, HACK INTO HOME

AGENDA & PANEL

全球聯防	人才培育	Cyber Physical System
金融聯防	CISO Round Table	5G Security
資安新創	Exploit	Talent Education
隱私與人權	Malware	Blue Team
企業經驗分享	IoT Hacking	AI Hacking

CALL FOR PAPER

2021.03.23(Tue) ~ 06.01(Tue)

https://hitcon.org

WORK FROM HOME, HACK INTO HOME

Hacking the Data Traversing in Reality-virtuality Hybrid World Recovery and Collaboration - Vaccine for CyberSecurity

格萊天漾大飯店 14-15 樓

2021.8.27(Fri) ~ 28(Sat)

早鳥售票：5/4 開始！

虛擬活動

#HITCON Online
#駭客貓歷險記
#Session Live
#煉蠱

實體活動

- 駭客貓歷險記
- 實體駭客 Village
- Bounty House

CALL FOR SPONSORSHIPS

<sponsorship@hitcon.org>

Thank You