Response Before Incident：
制敵機先！主動式資安事件處理

Chen-yu Dai (GD), Team T5

呂建鋒 (John Lu), 杜浦數位

TEAM T5
Cyber Security Research

DOPPLER
Cyber Threat Solutions

Agenda

- Introduction
  - 流行攻擊手法 數十年來演進
  - Supply Chain Attacks 供應鏈攻擊
  - 「系統遲早會被入侵」思維
  - 資安事件處理 必須化被動為主動

- Proactive Defense How-to
  - 從視野建構 到態勢感知
  - 內部主動處理：Threat Hunting 威脅狩獵
  - 外部專家知識：Threat Intelligence 威脅情資
  - 內外兼攻防禦：Threat Fusion 威脅整合
  - 完整防禦循環、多層次威脅防禦

- Threat Hunting 心法
  - 兩種 Threat Hunting: Host, Network
  - Pivoting: 假設和證據 Ping-Pong
  - 使用威脅情資分類優先順序
  - 情資導向的 Threat Hunting Cycle
  - 如何善用內外情資 達成 Threat Fusion

- Threat Hunting 實戰案例
  - 找出異常數位簽章的程式
  - 找出異常功能屬性的程式
  - 找出異常 cmd line 的程式
  - 找出異常 IP 連線的程式

- 跟 HITCON 一樣內容，聽過可去隔壁聽
- 投影片會放出

台灣自主研發團隊

DOPPLER

Cyber Threat Solution

Powered by Team T5

成立日期
2013 年 1 月

辦公室
台北

員工人數
30+ 人

Website
https://www.doppler.tw

- **資安顧問服務**
  - Threat Intelligence　網路威脅情資追蹤研究
  - Threat Hunting　資安事件處理與調查
  - Malware Forensics　惡意軟體分析鑑識
  - Consulting Service　綜合資安諮詢顧問
- **世界級堅強團隊**
  - 經營團隊成員來自各資安大廠，十年以上網路威脅研究經驗
  - 多位成員長期擔任台灣駭客年會 HITCON 議程委員或義工
  - 於 Black Hat, CODE BLUE 等國際頂尖研討會發表研究成果
  - 實驗室多位成員參與 DEF CON CTF等國際比賽獲獎無數
- **客戶遍及全球**
  - 擅長亞太區網路間諜防護、防護許多全球百大企業
  - 日本：電信集團、電機製造商、綜合商社、政府單位
  - 台灣：半導體廠、金融業、顧問業、各大SOC 、政府單位
  - 美國、歐洲、韓國：結盟知名資安大廠，服務金融業客戶

Chen-yu Dai (GD)

I thought what I'd do was, I'd pretend to be one of those deaf-mutes

CTO, Team T5 Inc.

- 專長：DFIR 數位鑑識與事件調查、惡意程式分析、企業資安應變團隊 CSIRT 建置、威脅情資平台整合
- 偶爾擔任義工：HITCON Review Board 核心成員
- 偶爾打打比賽：資安金盾獎共五屆冠軍、兩屆亞軍, DEFCON IntelCTF 亞軍, AVTokyo CTF 亞軍 etc.
- 偶爾出國演講：2016~2017 於 IEEE GCCE, HITCON, CODE BLUE, TROOPERS, HITCON, VXRL, DragonCon 等國內外資安研討會發表 Gogoro 藍牙加密弱點 etc

✉ gd@teamt5.org

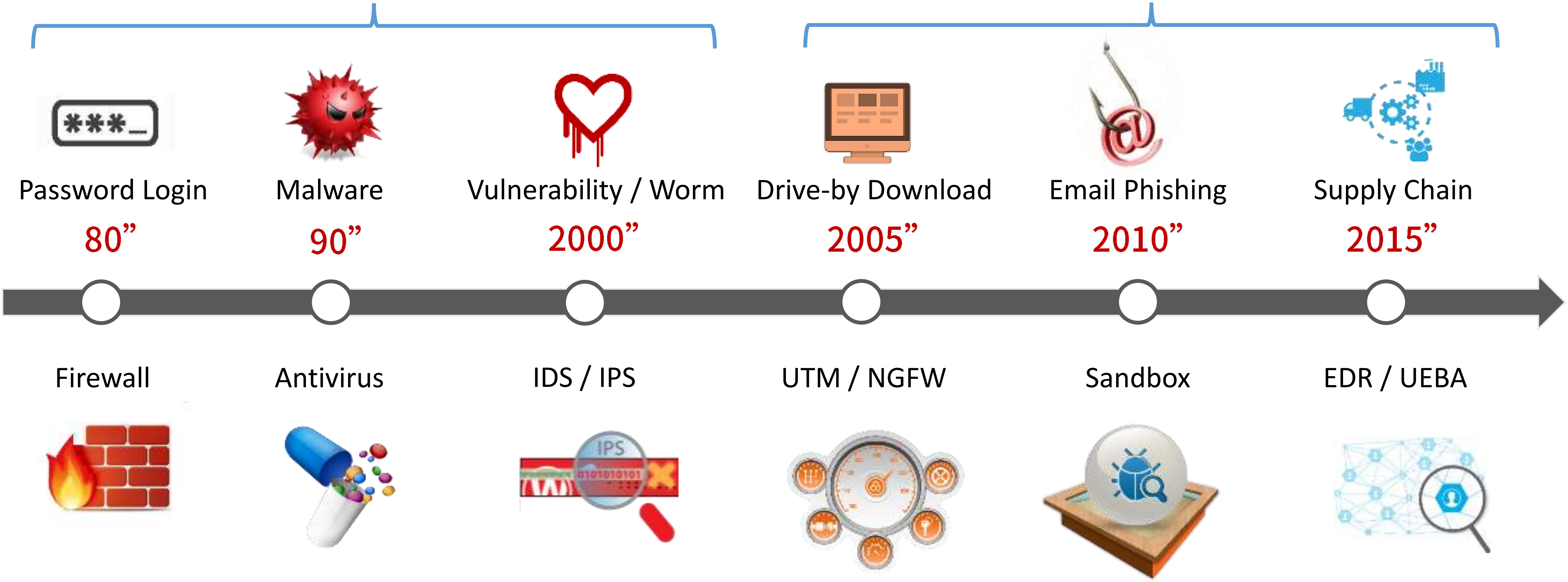
Introduction

TEAM T5

Cyber Security Research

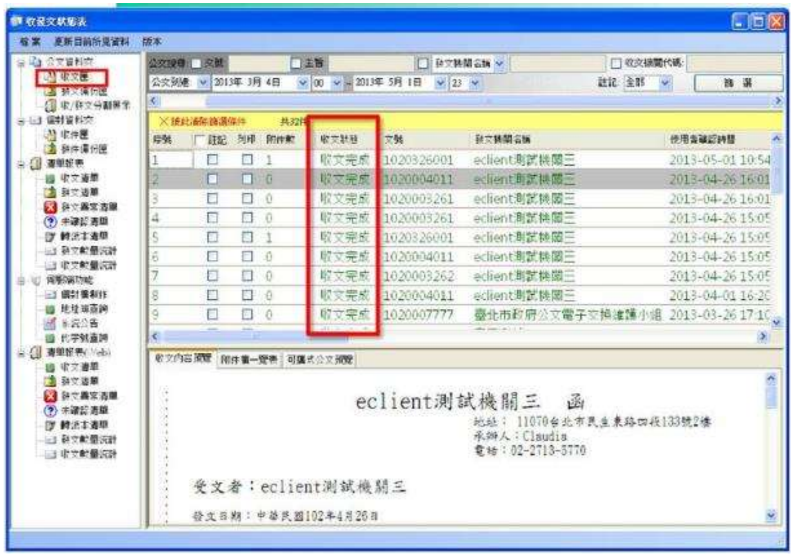
流行攻擊手法 數十年來演進

網路的 0day & 機會主義 → 端點的 0day & 針對性攻擊



Password Login	Malware	Vulnerability / Worm	Drive-by Download	Email Phishing	Supply Chain
80”	90”	2000”	2005”	2010”	2015”
Firewall	Antivirus	IDS / IPS	UTM / NGFW	Sandbox	EDR / UEBA

Supply Chain Attacks 供應鏈攻擊



檔案 更新目前所見資料 版本
收文匣
公文別總 2013年 3月 4日 00 ~ 2013年 5月 1日 23
註記 全部
篩選
共32件

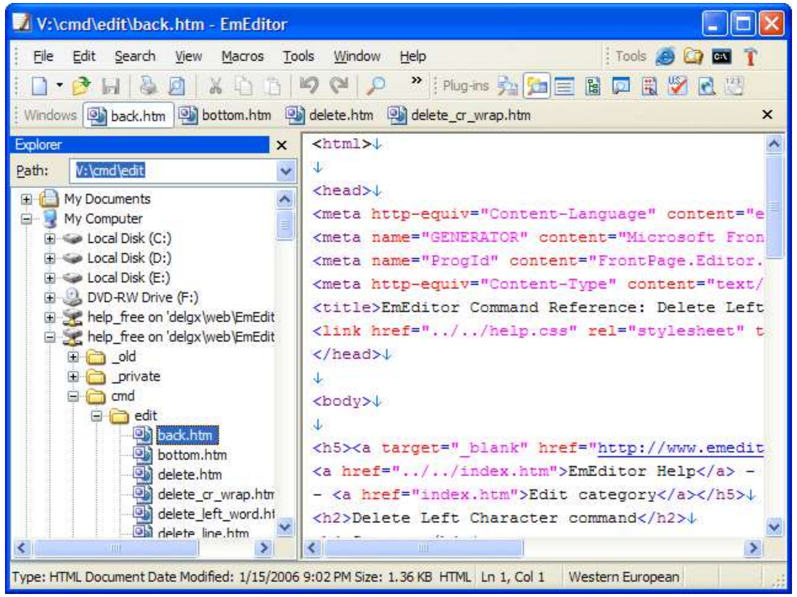
序號	註記	列印	附件數	收文狀態	文號	發文機關名稱	使用者確認時間
1	□	□	1	收文完成	1020326001	eclient測試機關三	2013-05-01 10:54
2	□	□	0	收文完成	1020004011	eclient測試機關三	2013-04-26 16:01
3	□	□	0	收文完成	1020003261	eclient測試機關三	2013-04-26 16:01
4	□	□	0	收文完成	1020003261	eclient測試機關三	2013-04-26 15:05
5	□	□	1	收文完成	1020326001	eclient測試機關三	2013-04-26 15:05
6	□	□	0	收文完成	1020004011	eclient測試機關三	2013-04-26 15:05
7	□	□	0	收文完成	1020003262	eclient測試機關三	2013-04-26 15:05
8	□	□	0	收文完成	1020004011	eclient測試機關三	2013-04-01 16:20
9	□	□	0	收文完成	1020007777	臺北市政府公文電子交換建議小組	2013-03-26 17:10

eclient測試機關三　函

地址：11070台北市民生東路四段133號2樓
承辦人：Claudia
電話：02-2713-5770

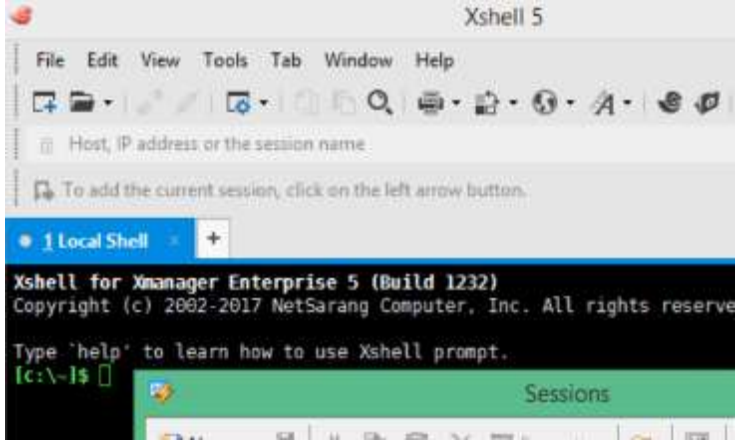
受文者：eclient測試機關三

發文日期：中華民國102年4月26日



```
<html>↓
↓
<head>↓
<meta http-equiv="Content-Language" content="e
<meta name="GENERATOR" content="Microsoft Fron
<meta name="ProgId" content="FrontPage.Editor.
<meta http-equiv="Content-Type" content="text/
<title>EmEditor Command Reference: Delete Left
<link href="../../help.css" rel="stylesheet" t
</head>↓
↓
<body>↓
↓
<h5><a target="_blank" href="http://www.emedit
<a href="../../index.htm">EmEditor Help</a> -
- <a href="index.htm">Edit category</a></h5>↓
<h2>Delete Left Character command</h2>↓
```

Type: HTML Document Date Modified: 1/15/2006 9:02 PM Size: 1.36 KB HTML Ln 1, Col 1 Western European



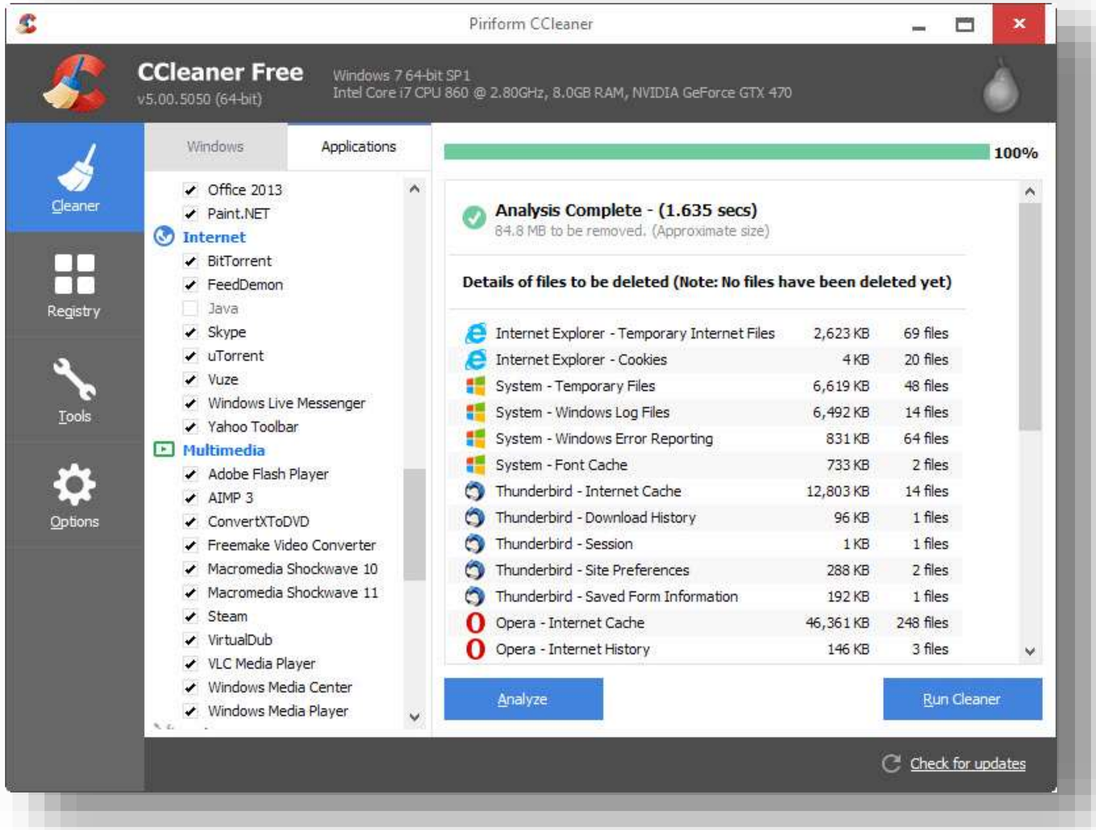
Xshell 5
File Edit View Tools Tab Window Help
Host, IP address or the session name
To add the current session, click on the left arrow button.
1 Local Shell
+
Sessions

```
Xshell for Xmanager Enterprise 5 (Build 1232)
Copyright (c) 2002-2017 NetSarang Computer, Inc. All rights reserve

Type `help' to learn how to use Xshell prompt.
[c:\~]$ 
```

2017-08 系統工具 CCleaner 事件

- 知名系統清理工具官網下載被加料
  一個多月期間被下載兩百萬次
  沒有任何防毒軟體偵測到
- 攻擊者鎖定 Intel、Google、微軟、Akamai、三星、Sony、VMware、HTC、Linksys、D-Link、Cisco 近 20 家科技廠商觸發
- 從雲端服務下載後門指令
  植入二階段後門
- Kaspersky: 此後門與 APT17 所用後門片段 base64 相似



☑ Office 2013
☑ Paint.NET
Internet
☑ BitTorrent
☑ FeedDemon
□ Java
☑ Skype
☑ uTorrent
☑ Vuze
☑ Windows Live Messenger
☑ Yahoo Toolbar
Multimedia
☑ Adobe Flash Player
☑ AIMP 3
☑ ConvertXToDVD
☑ Freemake Video Converter
☑ Macromedia Shockwave 10
☑ Macromedia Shockwave 11
☑ Steam
☑ VirtualDub
☑ VLC Media Player
☑ Windows Media Center
☑ Windows Media Player

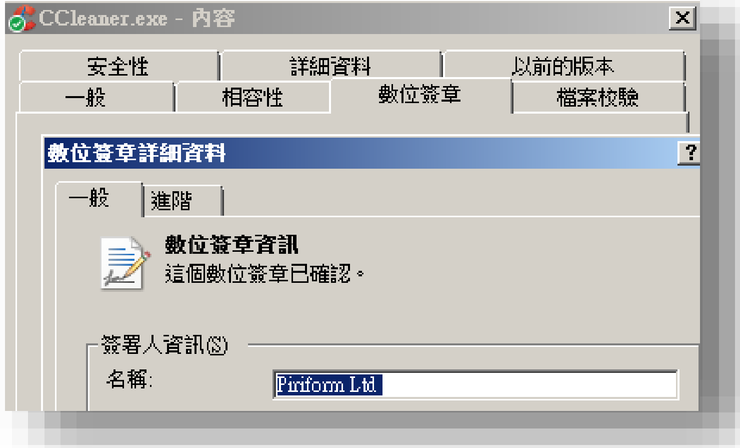
Analysis Complete - (1.635 secs)
84.8 MB to be removed. (Approximate size)

Details of files to be deleted (Note: No files have been deleted yet)

Internet Explorer - Temporary Internet Files	2,623 KB	69 files
Internet Explorer - Cookies	4 KB	20 files
System - Temporary Files	6,619 KB	48 files
System - Windows Log Files	6,492 KB	14 files
System - Windows Error Reporting	831 KB	64 files
System - Font Cache	733 KB	2 files
Thunderbird - Internet Cache	12,803 KB	14 files
Thunderbird - Download History	96 KB	1 files
Thunderbird - Session	1 KB	1 files
Thunderbird - Site Preferences	288 KB	2 files
Thunderbird - Saved Form Information	192 KB	1 files
Opera - Internet Cache	46,361 KB	248 files
Opera - Internet History	146 KB	3 files

傳統偵測技術失效

- 大家都以為自己誤判
  - 數位簽章合法是原廠的
  - 母公司是 Avast 防毒公司
- Host-based 特徵碼偵測時差太久
  - 2017-08-15 CCleaner 網站換置
  - 2017-09-14 開源 ClamAV 社群病毒碼
  - 2017-09-18 公開後還不到十家偵測
- Network-based 難偵測加密
  - 二階段 payload 放 https://github.com , https://wordpress.com 等雲端服務
  - 中繼站連線通訊行為，跟搜尋部落格相同

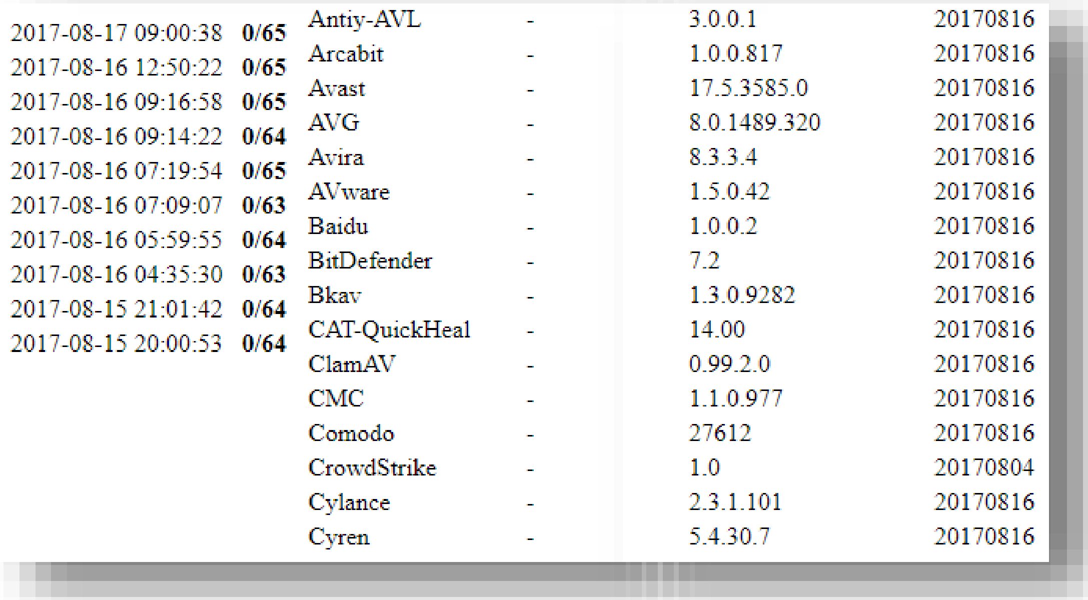


數位簽章資訊

這個數位簽章已確認。

簽署人資訊(S)

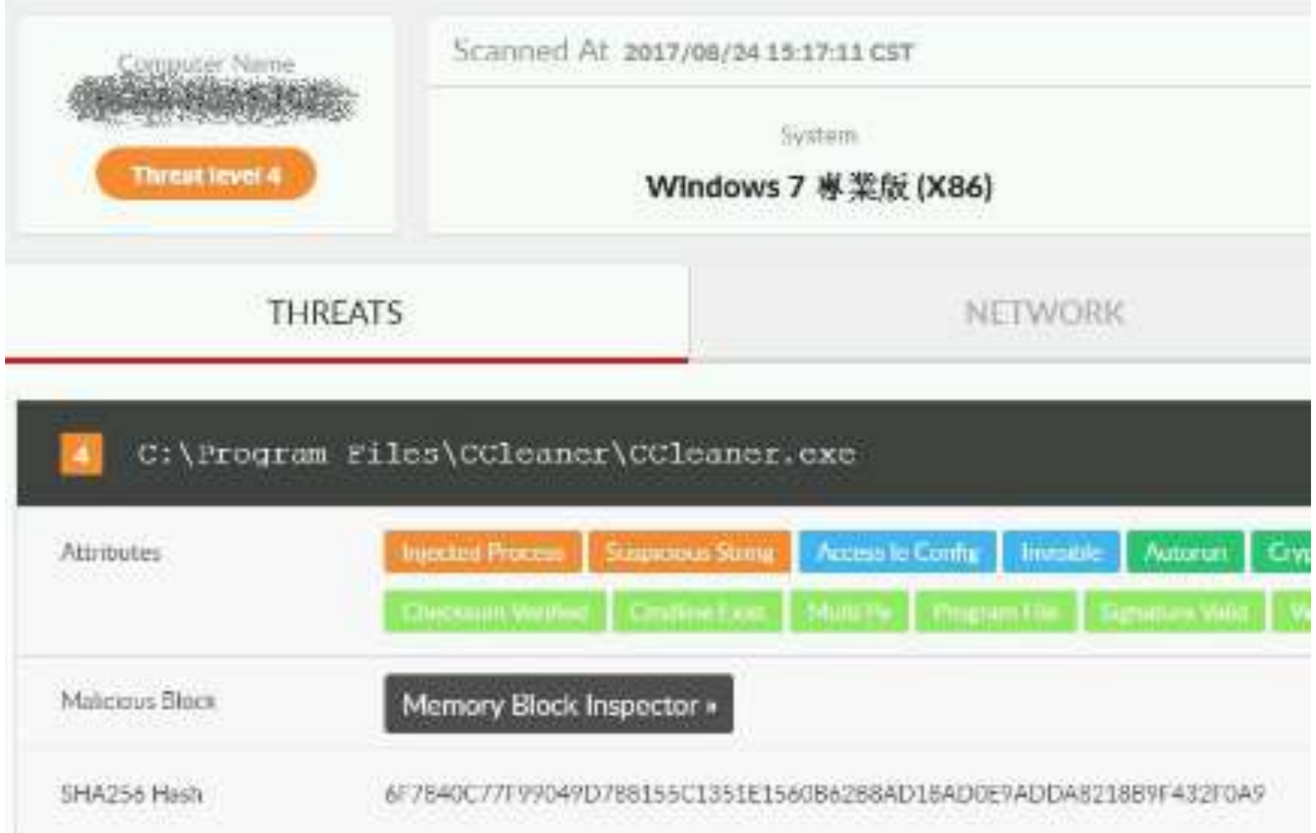
名稱: Piriform Ltd



2017-08-17 09:00:38	**0/65**
2017-08-16 12:50:22	**0/65**
2017-08-16 09:16:58	**0/65**
2017-08-16 09:14:22	**0/64**
2017-08-16 07:19:54	**0/65**
2017-08-16 07:09:07	**0/63**
2017-08-16 05:59:55	**0/64**
2017-08-16 04:35:30	**0/63**
2017-08-15 21:01:42	**0/64**
2017-08-15 20:00:53	**0/64**

Antiy-AVL	-	3.0.0.1	20170816
Arcabit	-	1.0.0.817	20170816
Avast	-	17.5.3585.0	20170816
AVG	-	8.0.1489.320	20170816
Avira	-	8.3.3.4	20170816
AVware	-	1.5.0.42	20170816
Baidu	-	1.0.0.2	20170816
BitDefender	-	7.2	20170816
Bkav	-	1.3.0.9282	20170816
CAT-QuickHeal	-	14.00	20170816
ClamAV	-	0.99.2.0	20170816
CMC	-	1.1.0.977	20170816
Comodo	-	27612	20170816
CrowdStrike	-	1.0	20170804
Cylance	-	2.3.1.101	20170816
Cyren	-	5.4.30.7	20170816

Behavior-based detection 行為偵測技術



Computer Name
[redacted]

Threat level 4

Scanned At 2017/08/24 15:17:11 CST

System
Windows 7 專業版 (X86)

4 C:\Program Files\CCleaner\CCleaner.exe

Attributes

Injected Process, Suspicious String, Access to Config, Invisible, Autorun, Cryp, Checksum Verified, Cmdline Exist, Multi Pe, Program File, Signature Valid, W

Malicious Block

Memory Block Inspector »

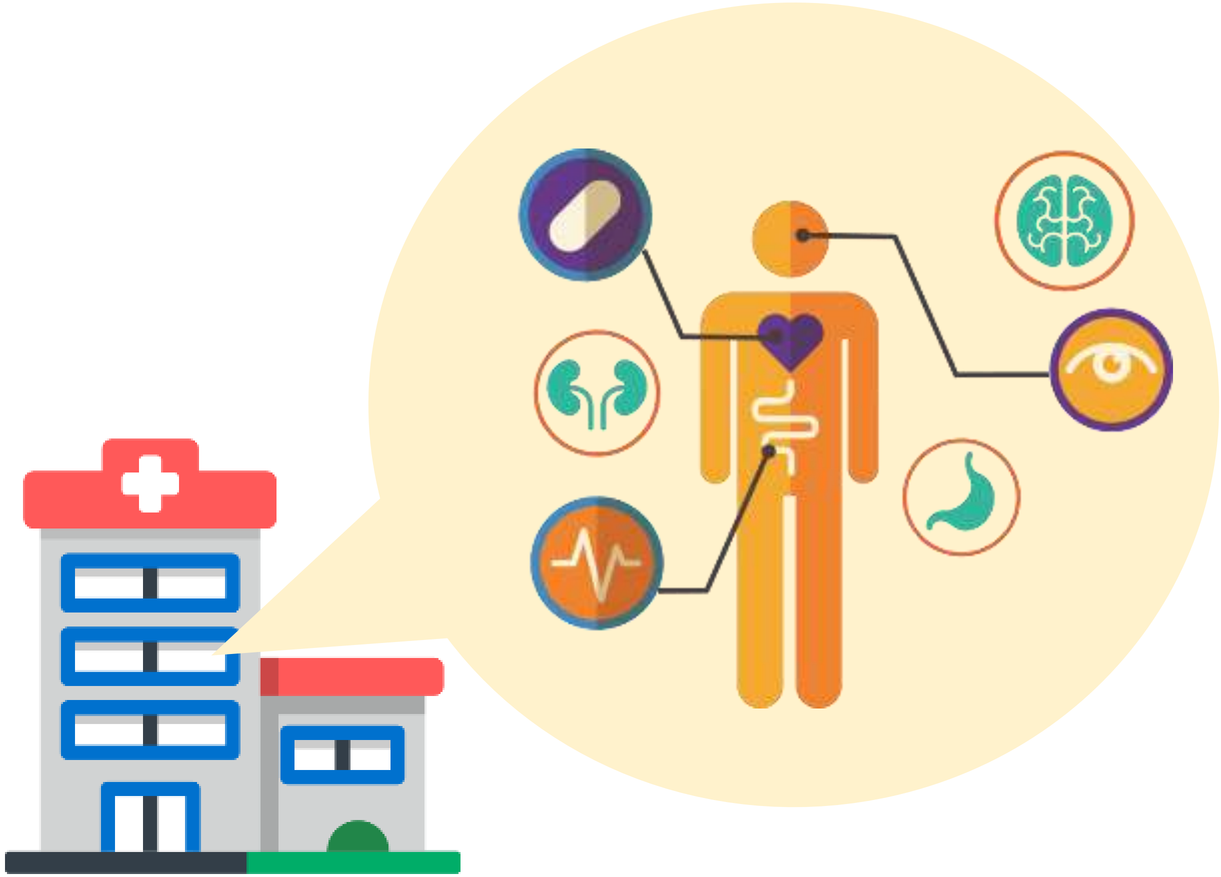
SHA256 Hash

6F7840C77F99049D788155C1351E1560B62B8AD18AD0E9ADDA8218B9F432F0A9

8/14 CCleaner compromised
8/17,24 ThreatSonar detected
9/14 First Antivirus detection

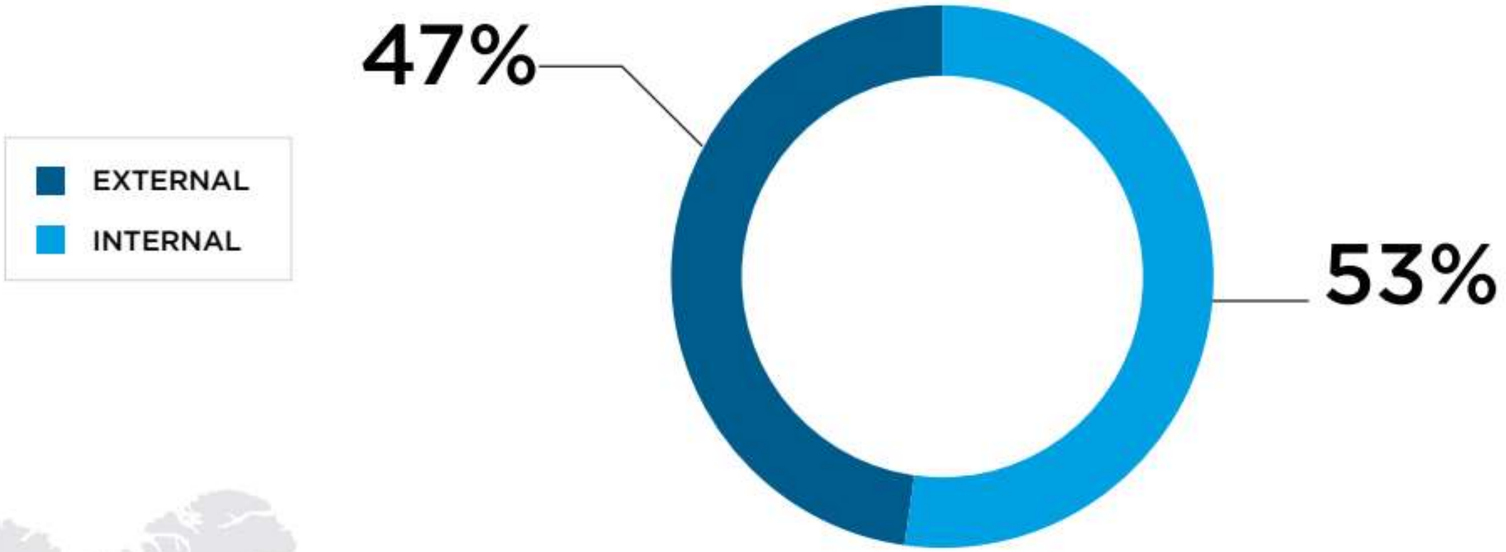
「系統遲早會被入侵」思維

- 人體總是會感冒的
  - 感冒並不可怕，不要變成肺炎就好
  - 經常運動的人，恢復的自然快
- 系統總是會被入侵的
  - 沒有防火牆/防毒軟體能 100% 阻擋
  - 及早發現問題，及早解決事件
- 系統跟人體 都需要健康檢查
  - 預防勝於治療

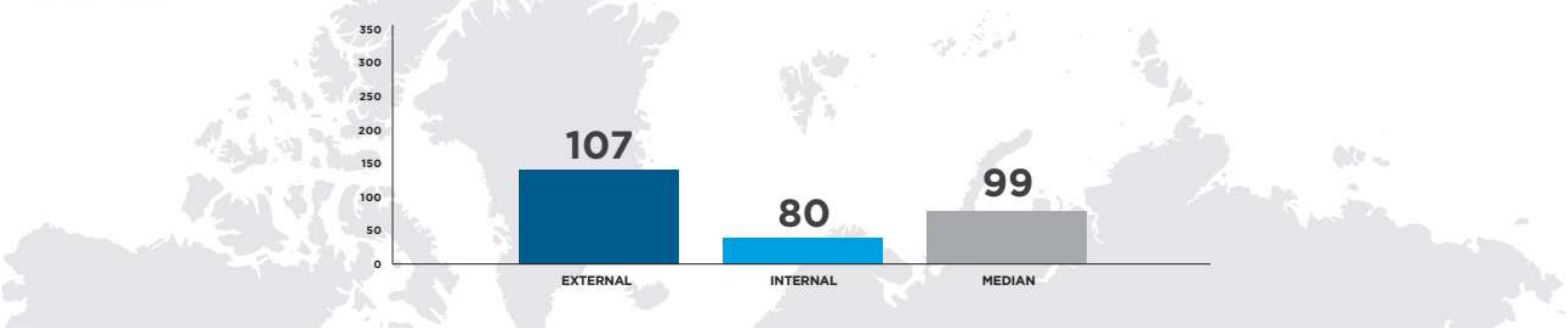


APT 半數來自外部通報，MTTR 平均百日

NOTIFICATION SOURCES TOTAL



DWELL TIMES



FireEye Mandiant M-Trends 2017 Report

資安事件處理 必須化被動為主動

Digital Forensics → Incident Response → Proactive Incident Handling

Disk Forensics

1997

Memory Forensics

2001

Private CSIRT

2005

Stuxnet / APT

2010

Remote Forensics EDR

2013

Threat Hunting

2016

1999

Network Forensics

2003

National CERT

2007

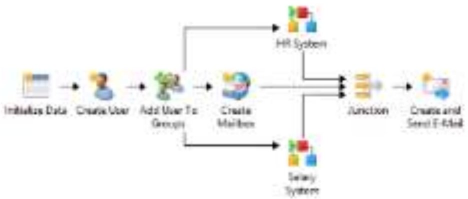
SIEM, SOC, MSSP

2011

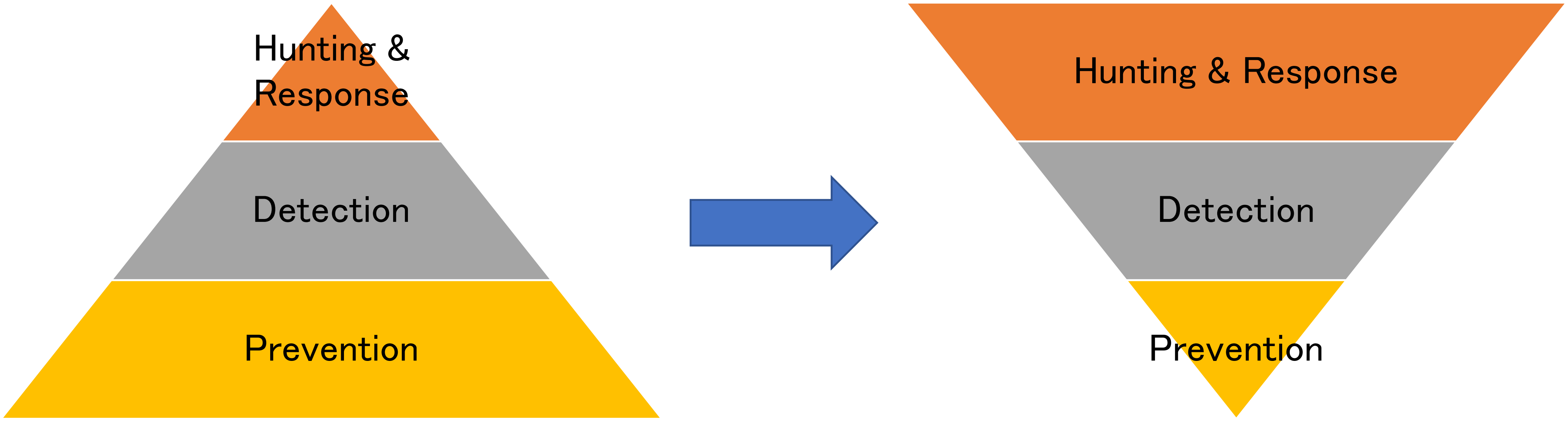
Threat Intelligence

2015

Orchestration



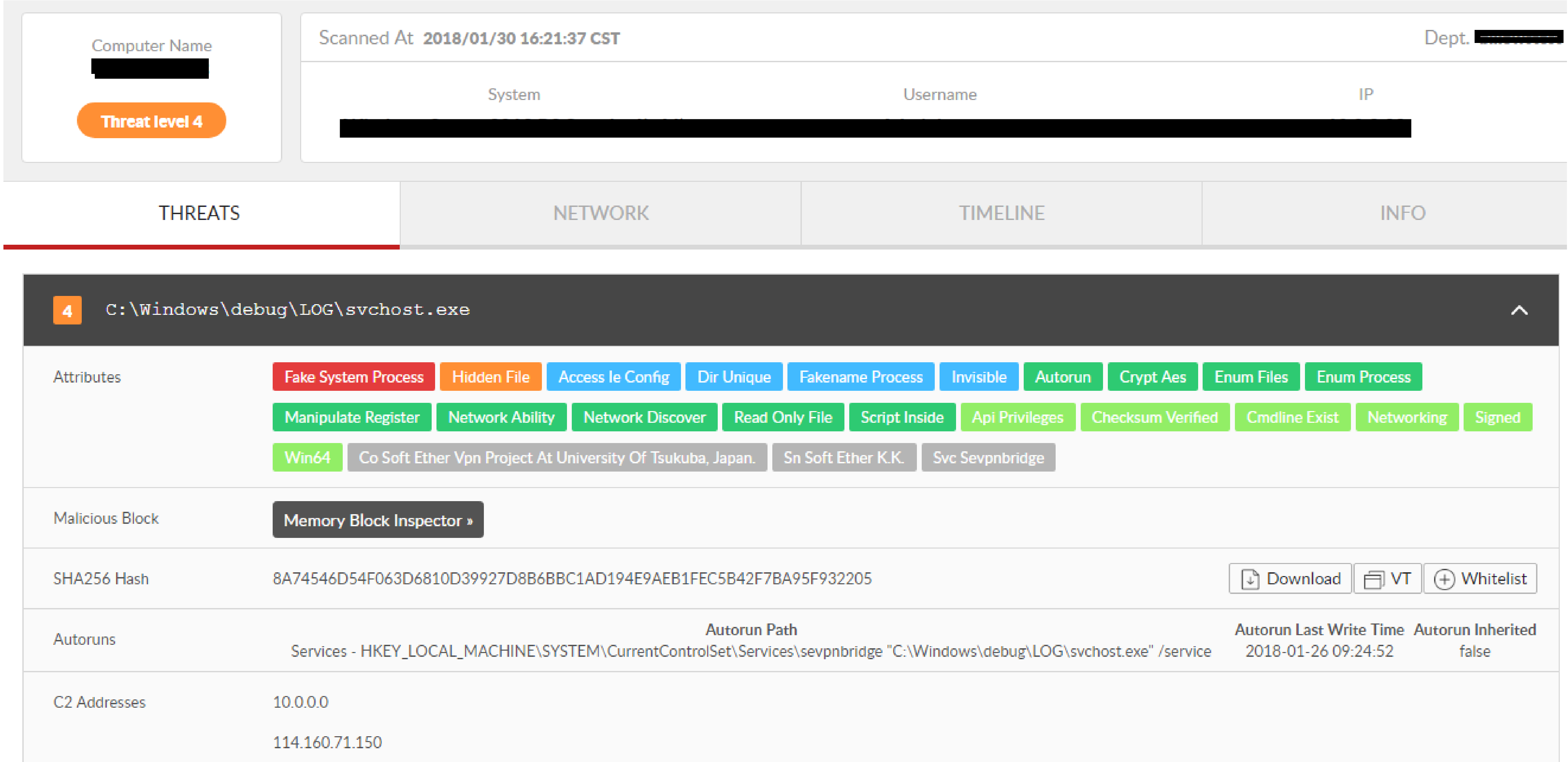
理想的 CSIRT 資源配置



目前多數公司預算分配

理想的主動防禦公司

找出違反policy軟體(私架VPN)(APT案例)



Computer Name
[redacted]

Threat level 4

Scanned At 2018/01/30 16:21:37 CST

Dept. [redacted]

System	Username	IP
[redacted]	[redacted]	[redacted]

4 C:\Windows\debug\LOG\svchost.exe

Attributes: Fake System Process, Hidden File, Access Ie Config, Dir Unique, Fakename Process, Invisible, Autorun, Crypt Aes, Enum Files, Enum Process, Manipulate Register, Network Ability, Network Discover, Read Only File, Script Inside, Api Privileges, Checksum Verified, Cmdline Exist, Networking, Signed, Win64, Co Soft Ether Vpn Project At University Of Tsukuba, Japan., Sn Soft Ether K.K., Svc Sevpnbridge

Malicious Block: Memory Block Inspector »

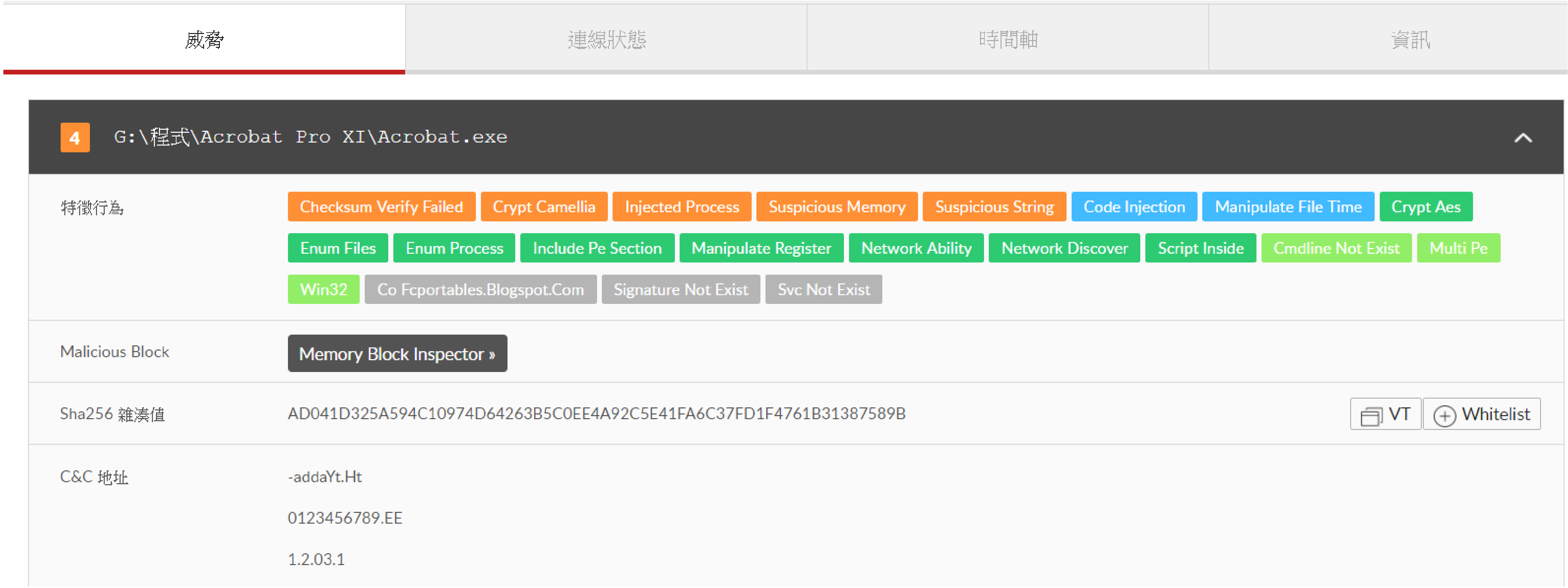
SHA256 Hash: 8A74546D54F063D6810D39927D8B6BBC1AD194E9AEB1FEC5B42F7BA95F932205

Autoruns

Autorun Path	Autorun Last Write Time	Autorun Inherited
Services - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sevpnbridge "C:\Windows\debug\LOG\svchost.exe" /service	2018-01-26 09:24:52	false

C2 Addresses: 10.0.0.0
114.160.71.150

找出非授權軟體 (免安裝 Adobe 盜版行為)



威脅 | 連線狀態 | 時間軸 | 資訊

4 G:\程式\Acrobat Pro XI\Acrobat.exe

特徵行為	Checksum Verify Failed Crypt Camellia Injected Process Suspicious Memory Suspicious String Code Injection Manipulate File Time Crypt Aes Enum Files Enum Process Include Pe Section Manipulate Register Network Ability Network Discover Script Inside Cmdline Not Exist Multi Pe Win32 Co Fcportables.Blogspot.Com Signature Not Exist Svc Not Exist
Malicious Block	Memory Block Inspector »
Sha256 雜湊值	AD041D325A594C10974D64263B5C0EE4A92C5E41FA6C37FD1F4761B31387589B
C&C 地址	-addaYt.Ht 0123456789.EE 1.2.03.1

Proactive Defense How-to

TEAM T5

Cyber Security Research

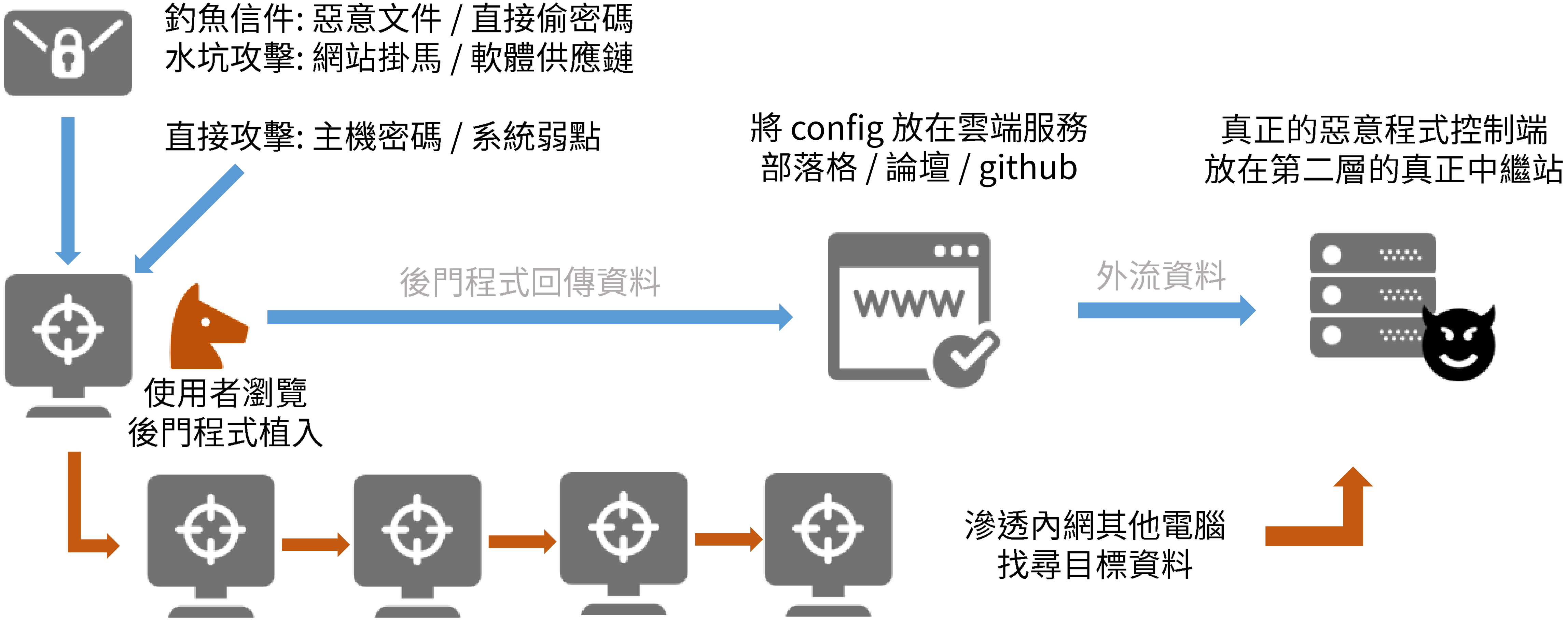
從視野建構 到態勢感知

- 視野建構：在重要的資產和通道加裝監視攝影機
  - Critical Data, Users, Assets, Network, Backup Plan, Physical Location
- 態勢感知：即時掌握狀況「發生什麼事情」
  - Know what to know, too much information is no information.

駕駛艙外視野
天氣狀況如何？
航道是否順暢？

駕駛艙內儀表板
引擎機械狀況？
油料航向高度？

針對性攻擊手法



釣魚信件: 惡意文件 / 直接偷密碼
水坑攻擊: 網站掛馬 / 軟體供應鏈

直接攻擊: 主機密碼 / 系統弱點

使用者瀏覽
後門程式植入

後門程式回傳資料

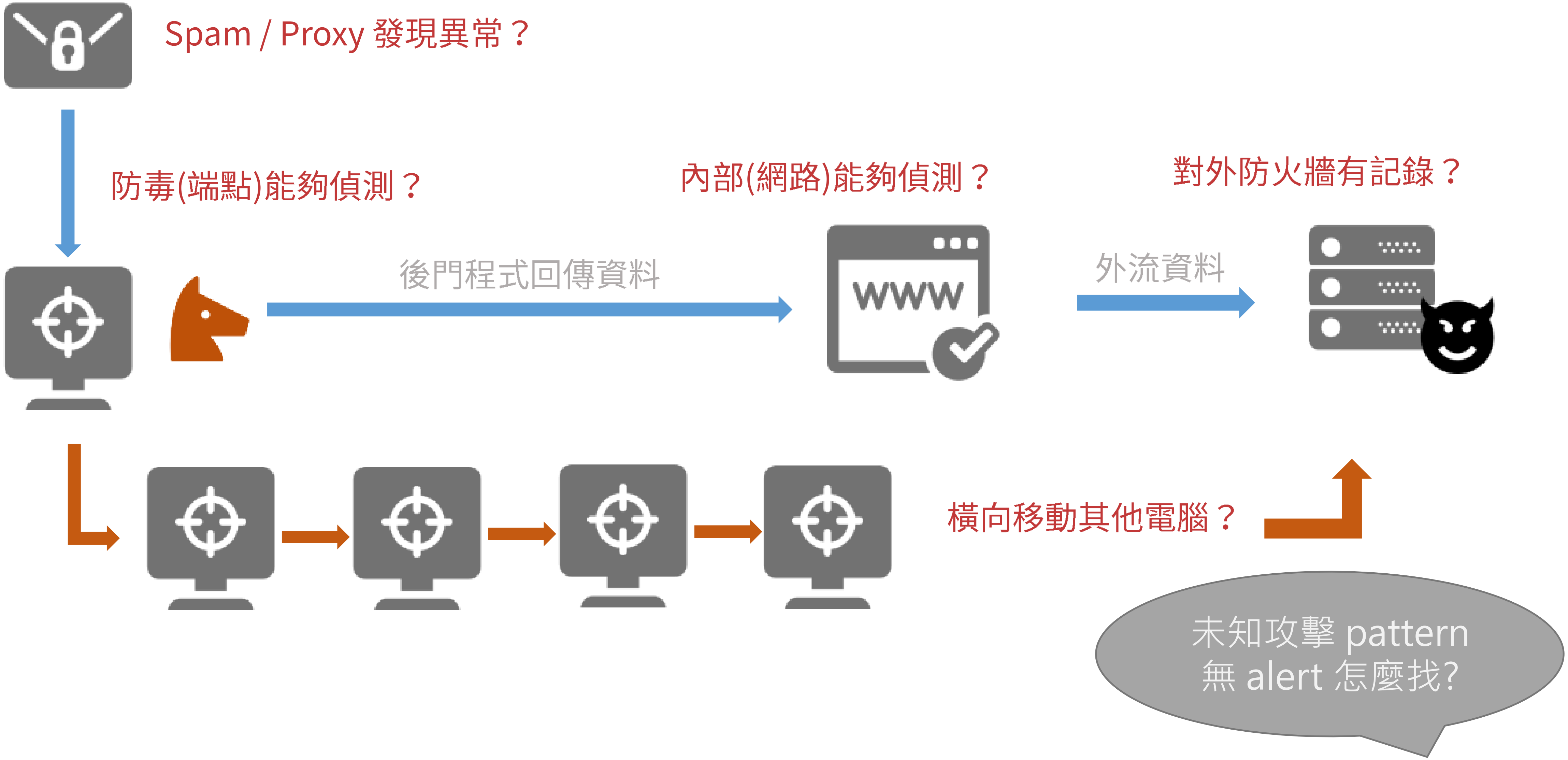
將 config 放在雲端服務
部落格 / 論壇 / github

外流資料

真正的惡意程式控制端
放在第二層的真正中繼站

滲透內網其他電腦
找尋目標資料

內部主動處理：Threat Hunting（威脅狩獵）



Spam / Proxy 發現異常？

防毒(端點)能夠偵測？

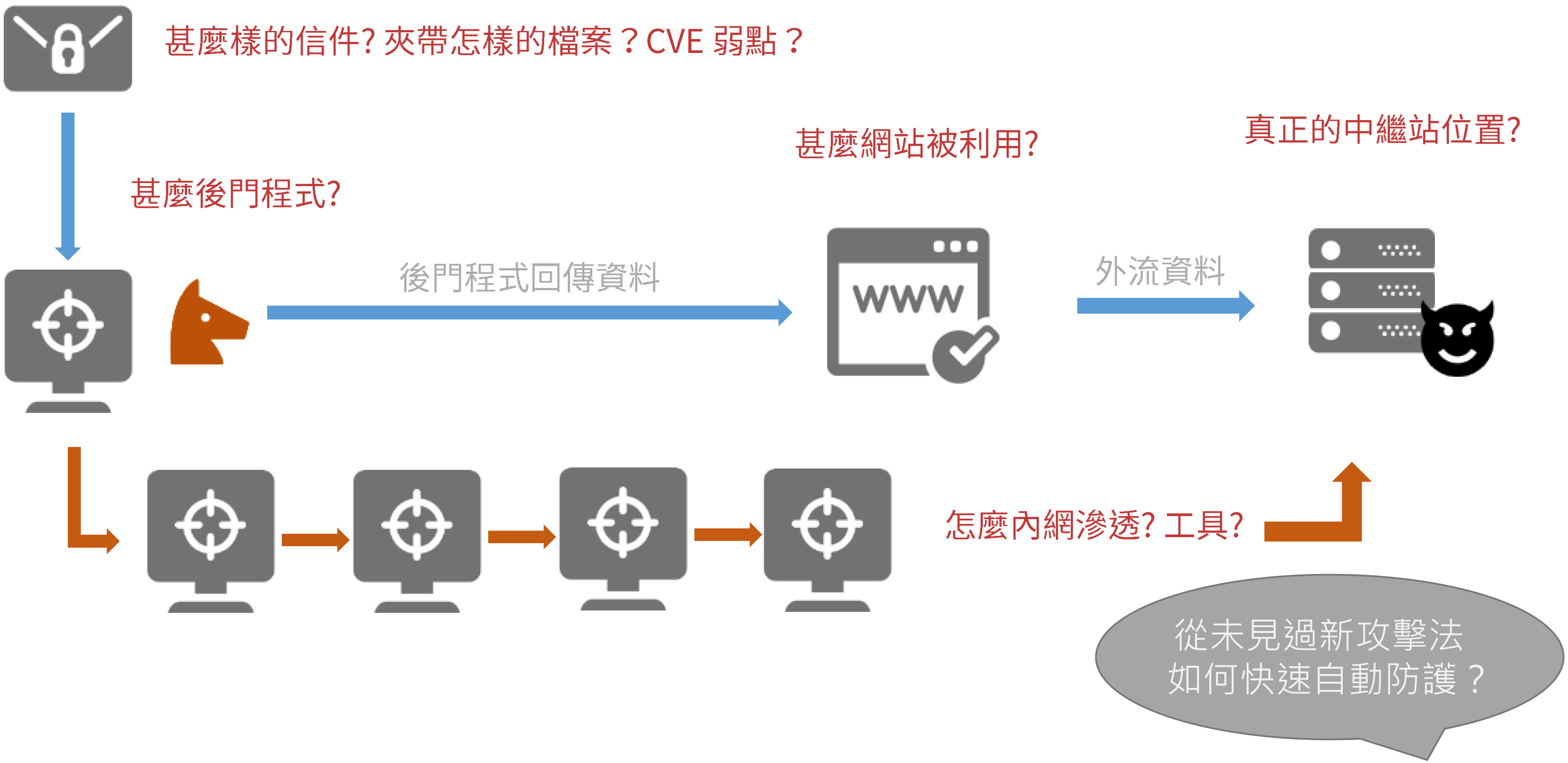
內部(網路)能夠偵測？

對外防火牆有記錄？

橫向移動其他電腦？

未知攻擊 pattern
無 alert 怎麼找?

外部專家知識：Threat Intelligence（威脅情資）



甚麼樣的信件? 夾帶怎樣的檔案？CVE 弱點？

甚麼後門程式?

後門程式回傳資料

甚麼網站被利用?

外流資料

真正的中繼站位置?

怎麼內網滲透? 工具?

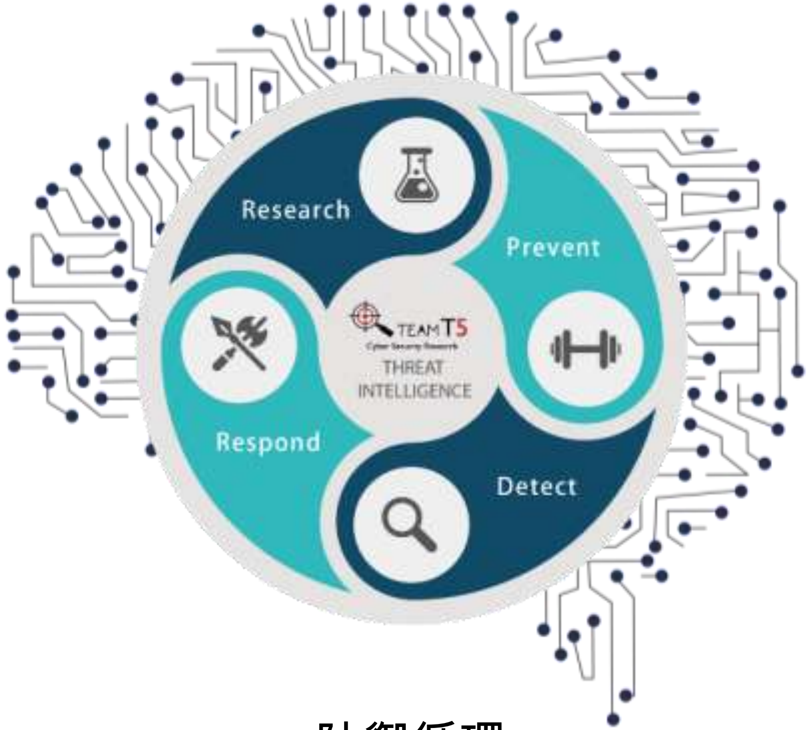
從未見過新攻擊法
如何快速自動防護？

內外威脅統一防禦：Threat Fusion (威脅整合)

情資平台

INTERNAL

Threat Hunting 威脅狩獵



防禦循環

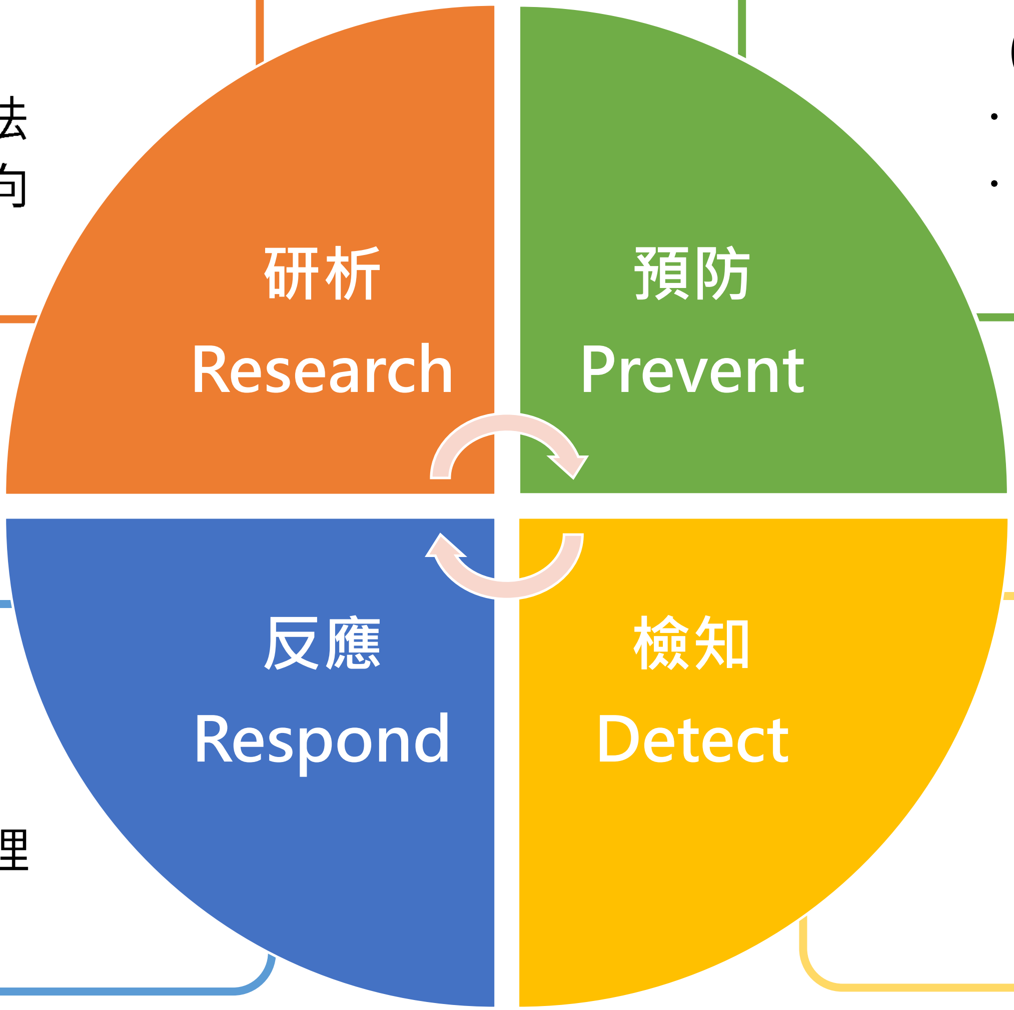
EXTERNAL

Threat Intel 威脅情資

完整防禦循環

- 私家偵探
  (Threat Analyst)
- 調查攻擊者的手法
- 持續追蹤風險面向

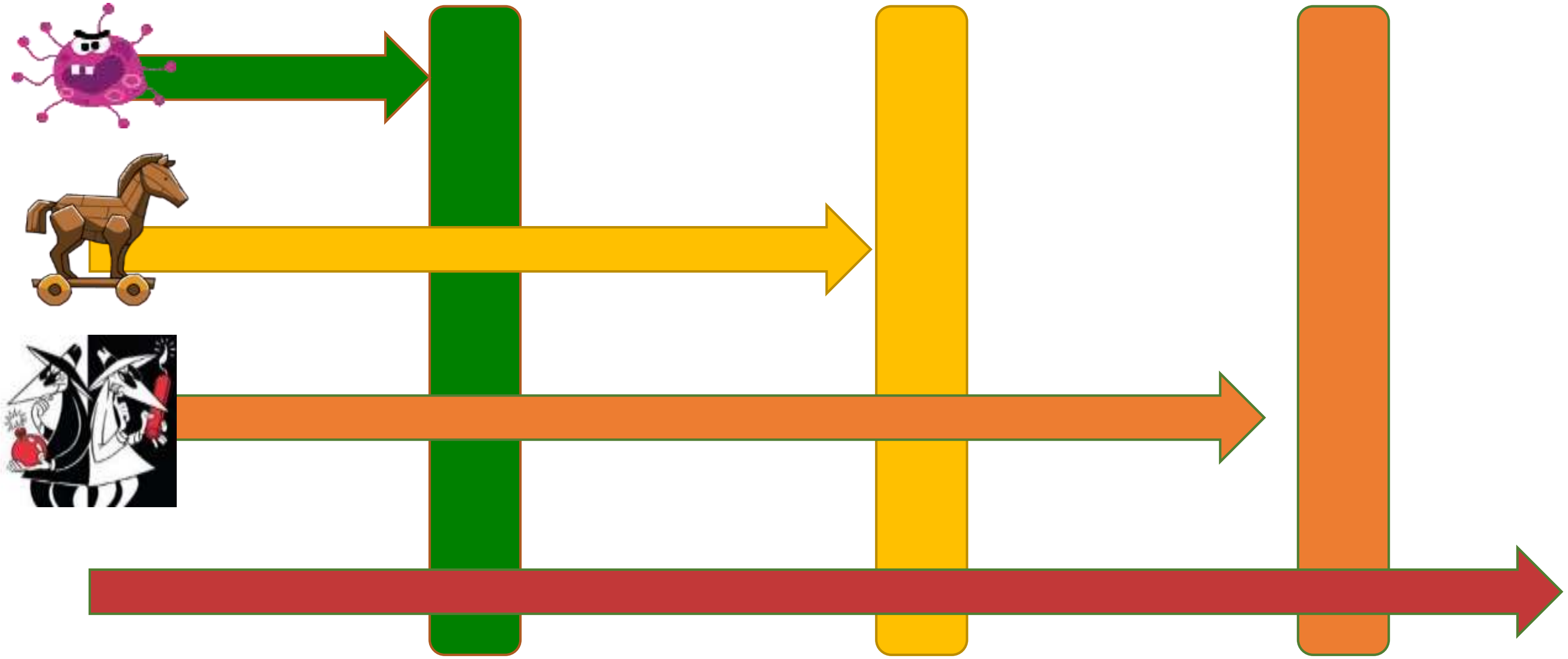
- 預防醫生
  (CISO/Manager)
- 組織溝通取得資源
- 防禦策略規劃演練



- 緊急應變小組
  (CSIRT/IR Team)
- 進入案發現場處理
- 狩獵殘存入侵者

- 警衛保全
  (SOC/MSSP)
- 24小時監控
- 發現異常通報

多層次威脅防禦



產品本身判斷

ISAC 外部情資

Managed Hunting

Blue Team

Known-Known

Known-Unknown

Unknown-Unknown

還是有可能被打進去

IR
事件處理

Threat Modeling
威脅引擎和特徵模型
動態特徵
靜態特徵

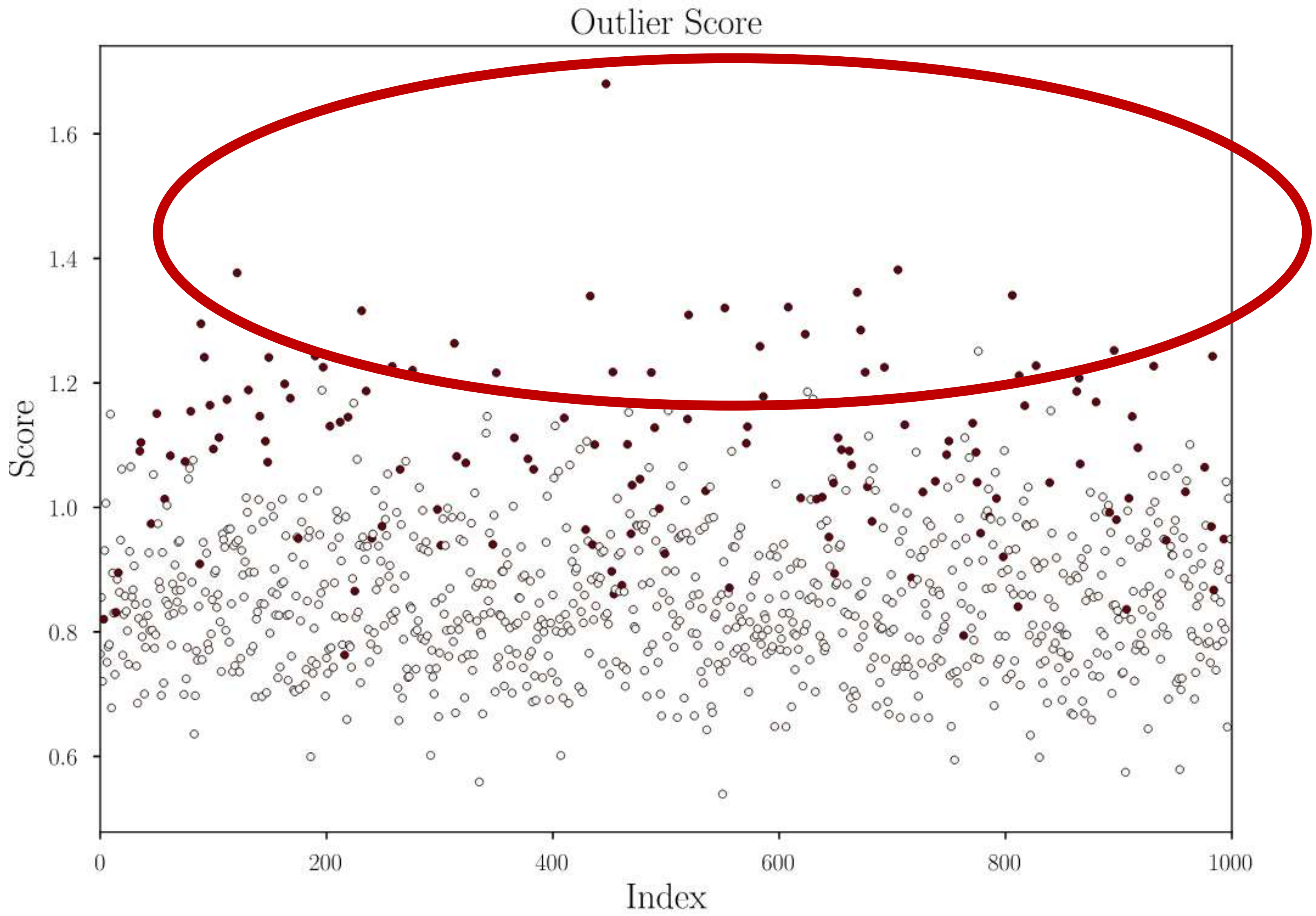
Threat Intelligence
威脅情資(原廠或外部)
雲查殺*、匯入自訂 Yara
中繼站 IP Domain 等

Threat Hunting
威脅獵殺(專家模式)
Behavior Analytics
統計關連、找出未知

Threat Hunting 心法

TEAM T5
Cyber Security Research

獵殺什麼？找出 Outlier 異常者

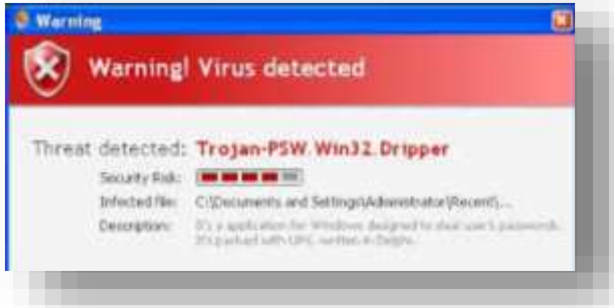


兩種 Threat Hunting 領域

- Network-based 網路 Hunting
  - 找什麼？ 中繼站連線、資料外流、內網橫向移動
  - 從哪裡？Firewall, IPS, Proxy, NAT, Moloch, etc
  - 異常是？packet with most outbound IP, longest, largest amount?
  - 技術成熟，一台設備可搜尋和管理上千電腦流量

- Host-based 端點 Hunting
  - 找什麼？ 駭客活動跡象的端點（桌機、伺服器、設備裝置）
  - 從哪裡？Process, File, Service, MBR, Registry, Eventlog, etc
  - 異常是？ Hidden process, Unique artifacts, Autorun entry, etc
  - 近年才有成熟的工具，可一次搜尋上千台電腦
  - 作業系統的異常好找，應用程式或專屬系統的難！

Pivoting: 假設和證據 Ping–Pong



Warning

Warning! Virus detected

Threat detected: Trojan-PSW.Win32.Dripper

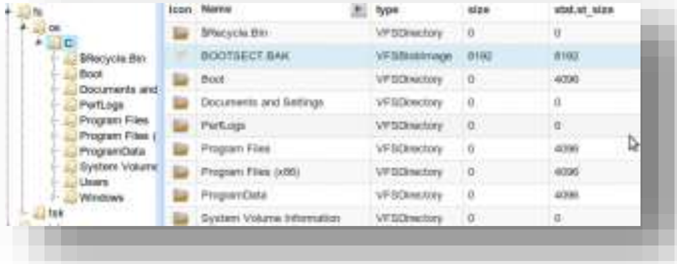
Security Risk: ■■■■■

Infected file: C:\Documents and Settings\Administrator\Recent\...

Description: It's a application for Windows designed to steal user's passwords. It's packed with UPX, written in Delphi.

%Temp%\RarSFX1\1.exe looks suspicious dropper,
Is this a ransomware, banking Trojan or APT ?
> Not sure, check network side.

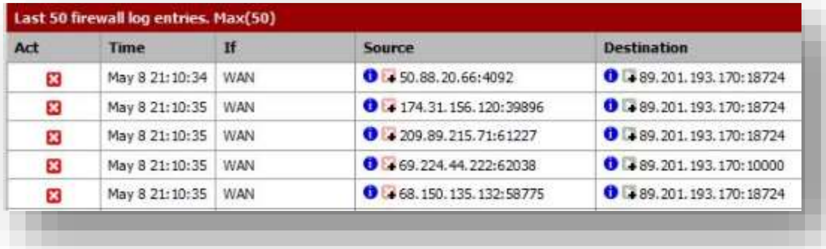
Any suspicious outgoing connection or DNS
from this endpoint at the timeframe of alert?
> Yes, one suspicious VPS IP found.



Icon	Name	type	size	stat.st_size
	$Recycle.Bin	VFSDirectory	0	0
	BOOTSECT.BAK	VFSBlobImage	8192	8192
	Boot	VFSDirectory	0	4096
	Documents and Settings	VFSDirectory	0	0
	PerfLogs	VFSDirectory	0	0
	Program Files	VFSDirectory	0	4096
	Program Files (x86)	VFSDirectory	0	4096
	ProgramData	VFSDirectory	0	4096
	System Volume Information	VFSDirectory	0	0

Get me additional logs to build activity timeline
on this endpoint using remote forensics tools?
> Yes, this host has been compromised

Is there any other host in my organization
connecting to the same IP?
> Yes, please block all of them.



Last 50 firewall log entries. Max(50)

Act	Time	If	Source	Destination
☒	May 8 21:10:34	WAN	50.88.20.66:4092	89.201.193.170:18724
☒	May 8 21:10:35	WAN	174.31.156.120:39896	89.201.193.170:18724
☒	May 8 21:10:35	WAN	209.89.215.71:61227	89.201.193.170:18724
☒	May 8 21:10:35	WAN	69.224.44.222:62038	89.201.193.170:10000
☒	May 8 21:10:35	WAN	68.150.135.132:58775	89.201.193.170:18724

Host-based Hunting 端點策略

- 獨立存在的異常程式 Standalone code
  - Malware does not try hide itself or hijack other process
  - File name or hash is special, only appears on a few endpoints.

- 偽裝或寄生的程式片段 Masqueraded code
  - Hiding methods: Loaded using svchost.exe, DLL-Hijacking, etc.
  - Same filename but different in-memory attributes.

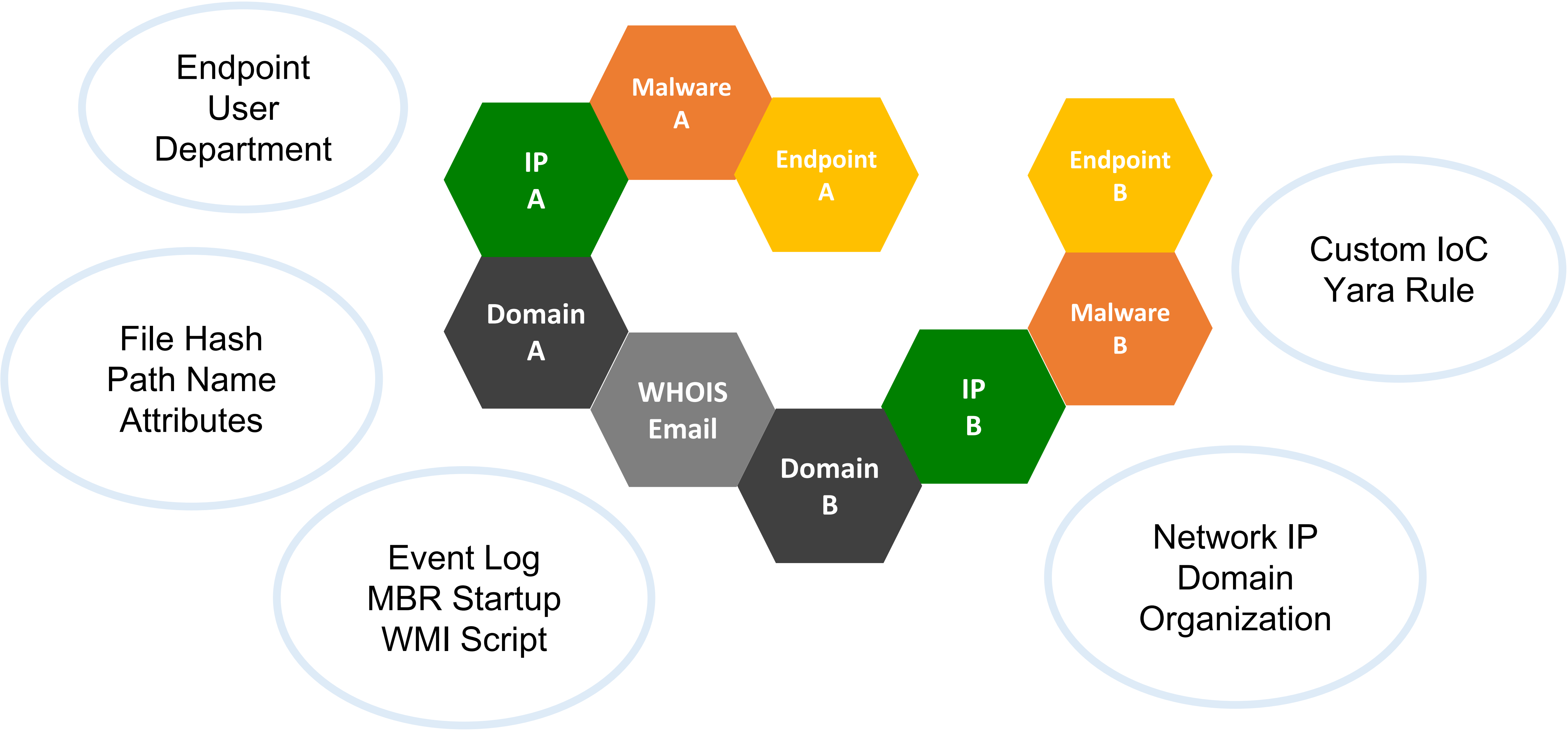
- 正常系統的異常活動 System Abnormality
  - EventLogs, Web logs, File system, Startup artifacts
  - File-less threats: PowerShell, WMI Script, In-memory

Network-based Hunting 網路策略

- 封包內容 Packet Content-based
  - Traditional IDS/IPS: Pattern recognition
  - Deep-Packet Inspection: Application-aware NG-FW
  - Full Packet Retention: Moloch etc
  - 資料量大、成本高、檢索慢，可看到完整資料並作為證據

- 中繼資料 Metadata-based
  - Netflow 連線流量: Easy to preserve for a long while.
  - Passive DNS 保留: What IP does DNSName resolved to?
  - Retro-Hunting: Compare with latest intelligence feeds.
  - 資料量少、成本低、搜索快，無法看到外流資料內容和指令

Pivoting Host & Network Indicators



Endpoint
User
Department

File Hash
Path Name
Attributes

Event Log
MBR Startup
WMI Script

Malware A

IP A

Endpoint A

Domain A

WHOIS Email

Domain B

IP B

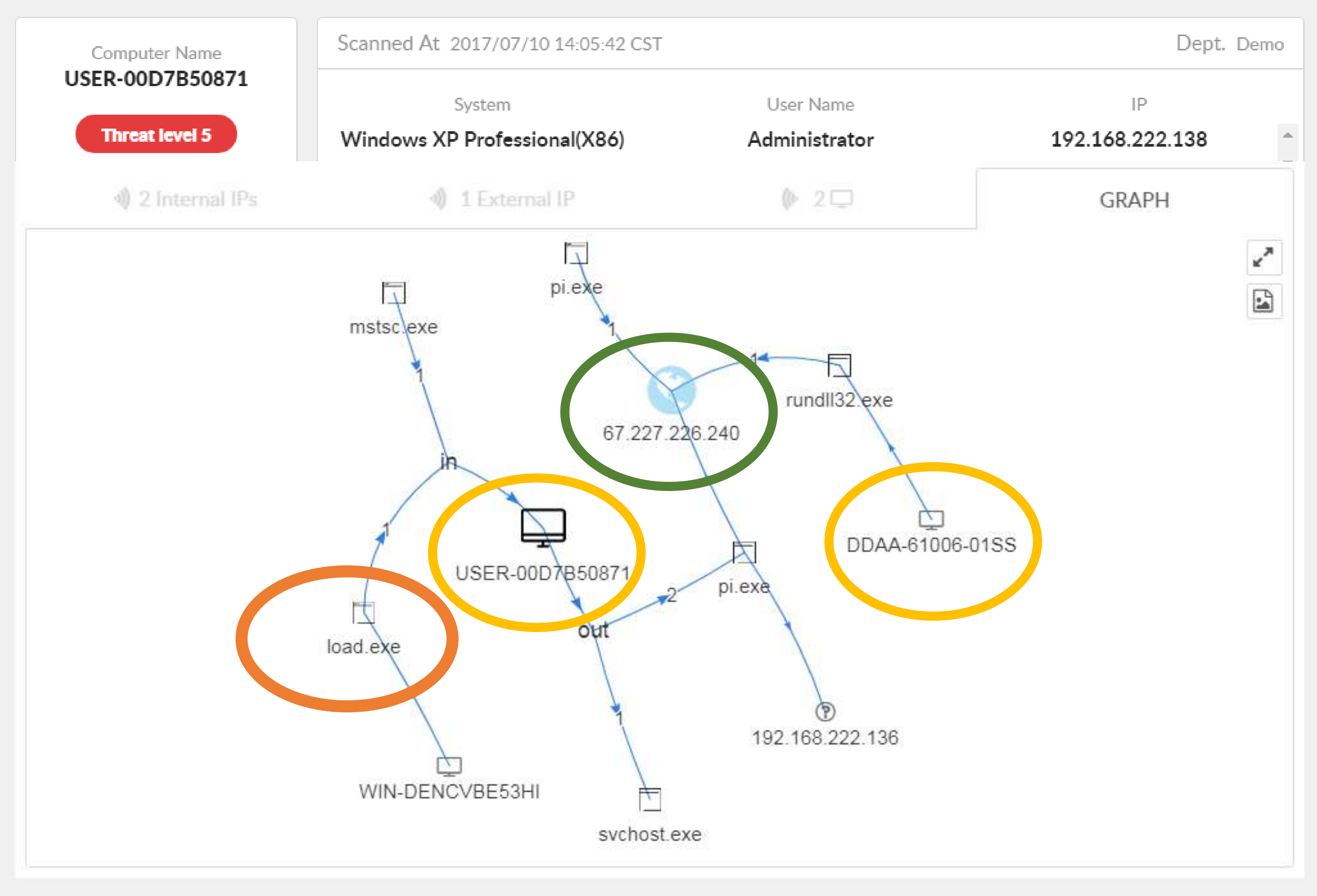
Malware B

Endpoint B

Custom IoC
Yara Rule

Network IP
Domain
Organization

Graph visualization & pivoting



Computer Name
USER-00D7B50871

Threat level 5

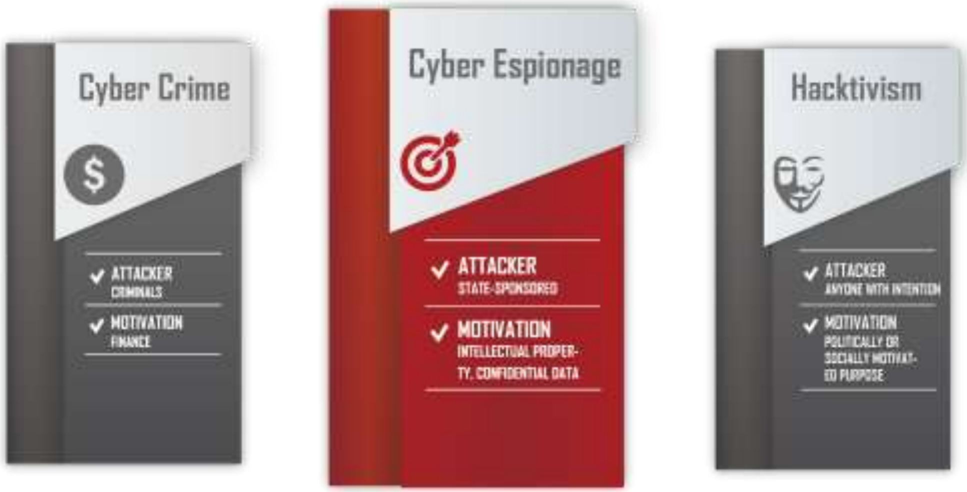
Scanned At 2017/07/10 14:05:42 CST

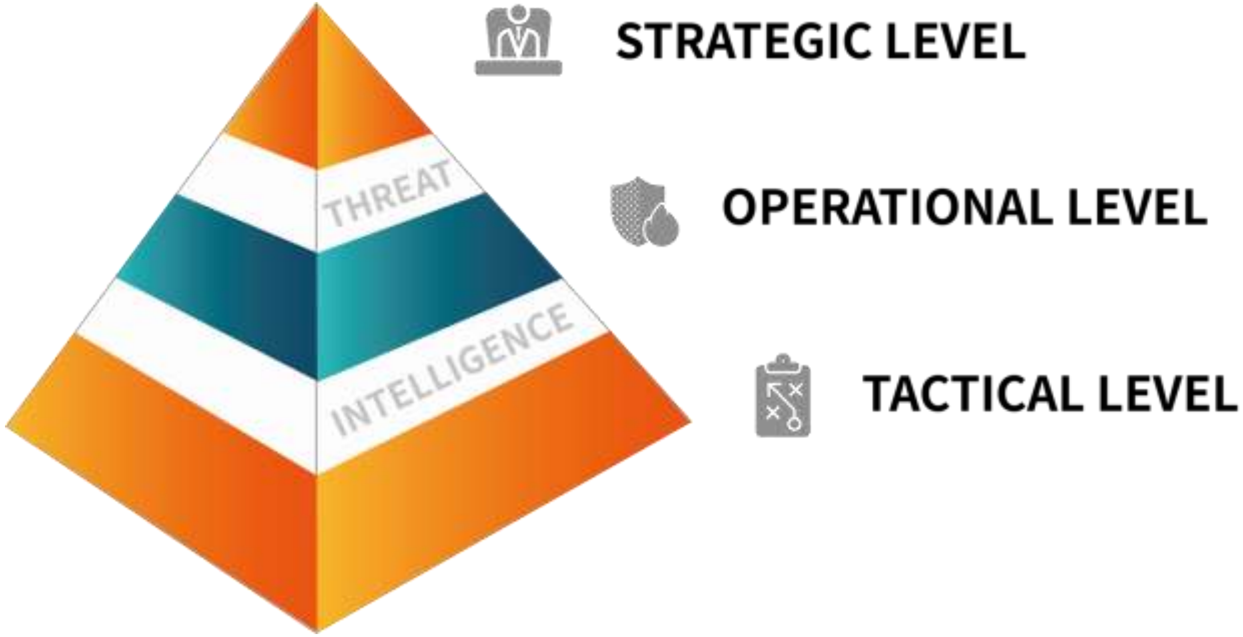
Dept. Demo

System	User Name	IP
Windows XP Professional(X86)	Administrator	192.168.222.138

使用威脅情資 Threat Intelligence 分類優先順序

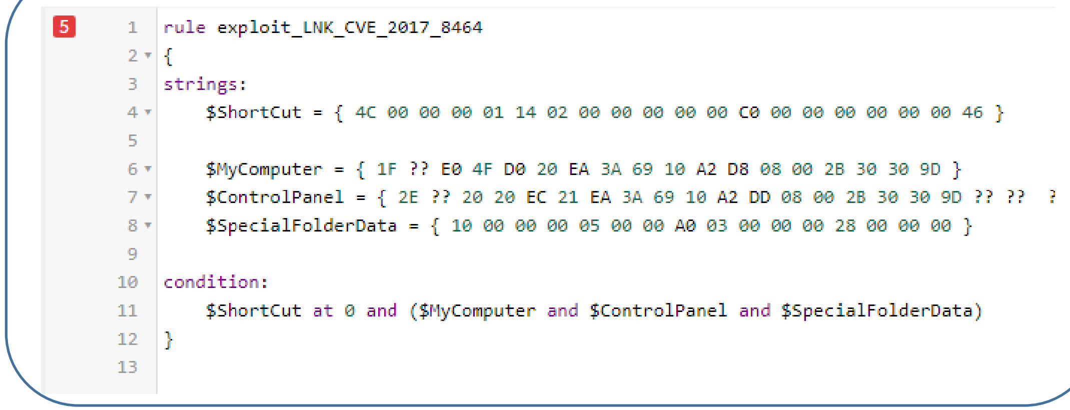
- Bring external situation awareness into your constituency
- Source: OSINT blog, commercial feeds, bring-your-own
- Matching Indicators: IP, Domain, IoC, Snort, Yara rule





情資導向的 Threat Hunting Cycle

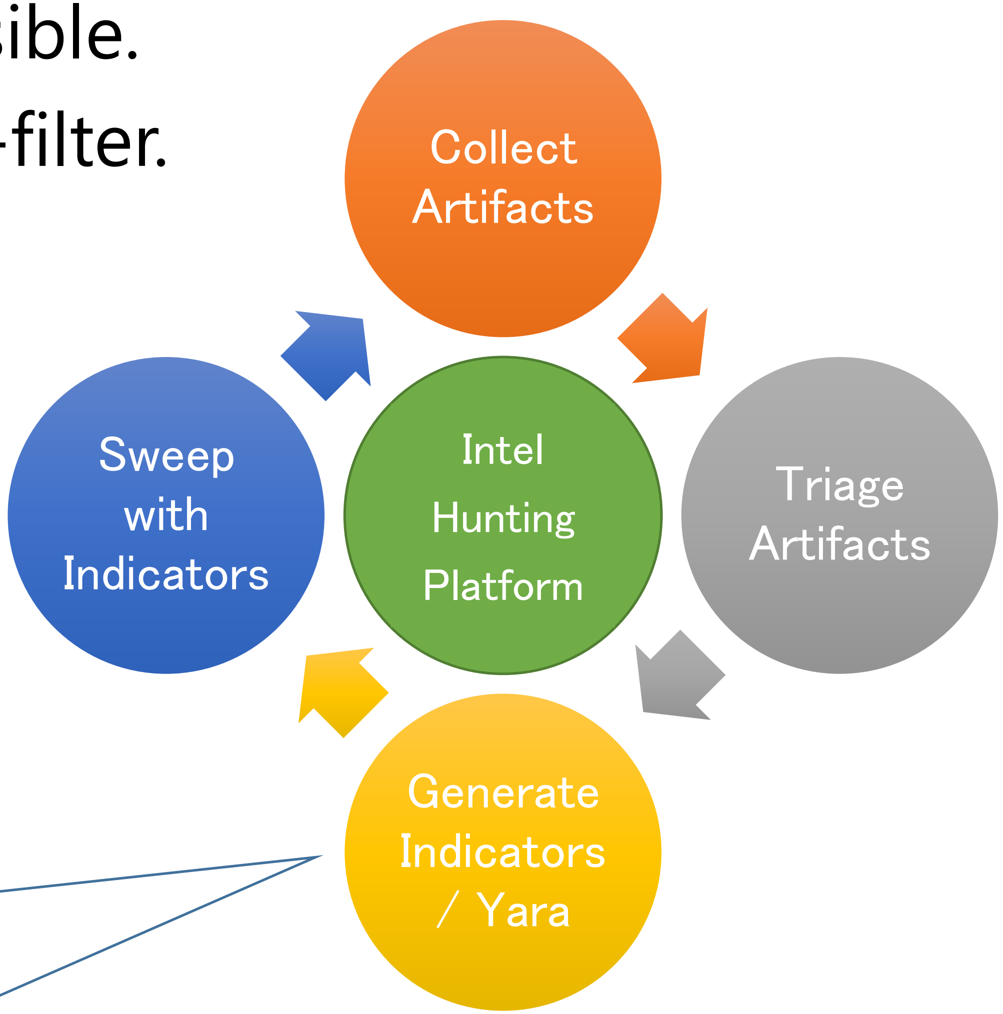
- Collect artifacts: As precise as possible.
- Triage artifacts: Pre-filter and post-filter.
- Generate new indicators
  - Create Yara Rule on-the-fly
- Sweep with indicators
  - Host & Network-based



```
rule exploit_LNK_CVE_2017_8464
{
strings:
    $ShortCut = { 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 00 00 00 46 }

    $MyComputer = { 1F ?? E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D }
    $ControlPanel = { 2E ?? 20 20 EC 21 EA 3A 69 10 A2 DD 08 00 2B 30 30 9D ?? ??  ?
    $SpecialFolderData = { 10 00 00 00 05 00 00 A0 03 00 00 00 28 00 00 00 }

condition:
    $ShortCut at 0 and ($MyComputer and $ControlPanel and $SpecialFolderData)
}
```



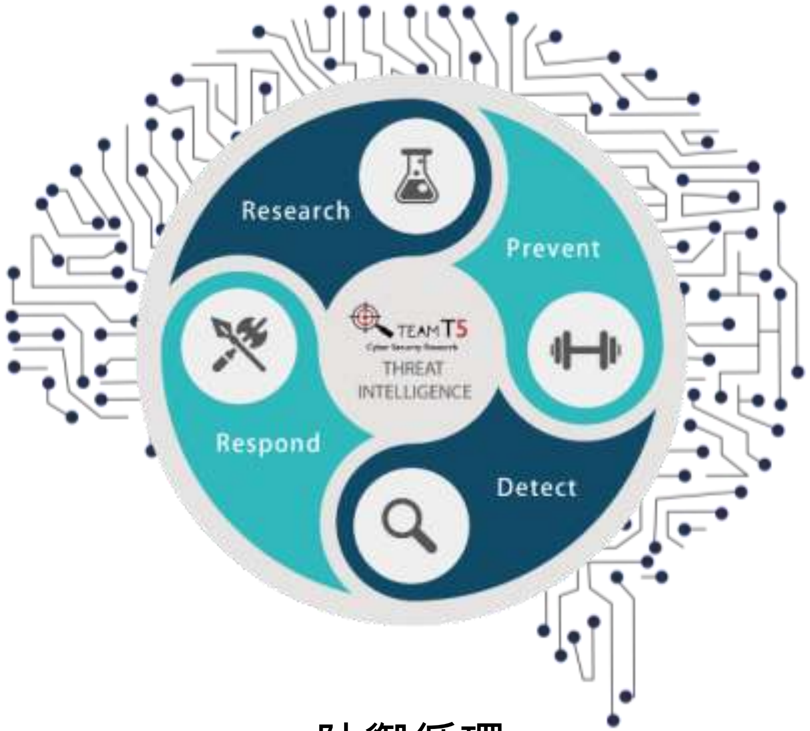
威脅整合 Threat Fusion：內外威脅統一防禦

INTERNAL

Threat Hunting 威脅狩獵

Host-based 程式活動
Network-based 網路傳輸
各種設備 log 集中搜尋
內部可疑蛛絲馬跡
過去發生資安事件

情資平台



防禦循環

EXTERNAL

Threat Intel 威脅情資

零時差軟體弱點 0day / CVE
最新惡意程式攻擊手法 TTP
長期追蹤調查對手Adversary
相關產業趨勢分析
同產業資安事件聯防

如何善用內外情資 達成 Threat Fusion

Collection

Internal Incidents
ISAC / CERT

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

OSINT
Dark Web INTEL471

Omni-sourced
Early Warning

Commercial

FLASHPOINT

iSIGHTPARTNERS

KASPERSKY lab

iDEFENSE

Filtering

python

CIRCL MISP Threat Sharing

THREATCONNECT

Threat Intel
Platform

Adversarial
Coverage

Raw Data
Process API

Detection

amazon web services

CROWDSTRIKE

Check Point SOFTWARE TECHNOLOGIES LTD.

FireEye

Blacklist rules
Snort Yara IoC

Symantec.

Blue Coat

riverbed

NETWITNESS

Analytics

LogRhythm

hp ArcSight

splunk>

SIEM / Log
Platform

Discovery
Alert Pivot

Abnormality
Modeling

Actions

External Sharing

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

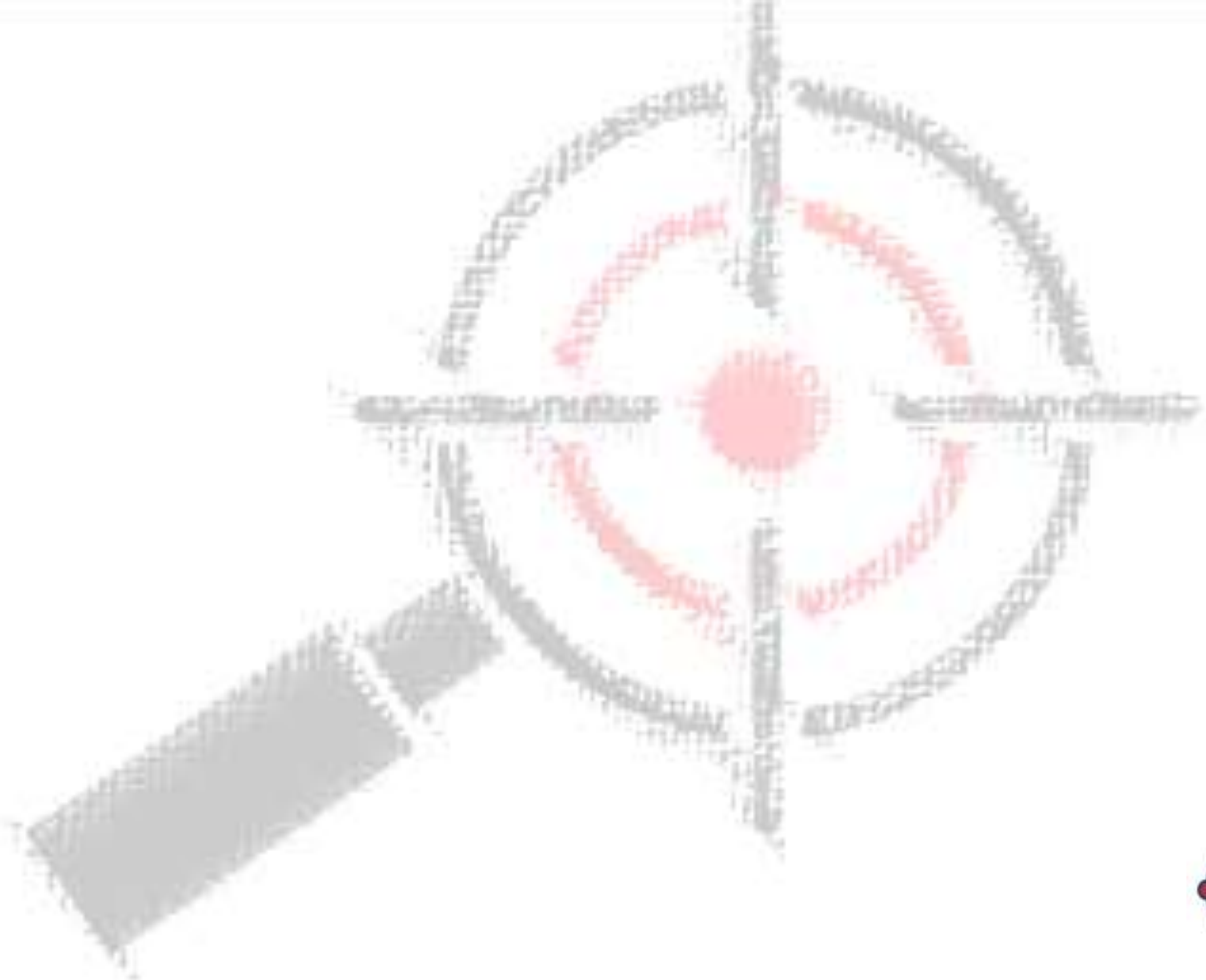
FINANCIAL SERVICES ISAC

CSIRT
Hunting

RSA Incident
Management

GRR RAPID RESPONSE

TANIUM



主動式資安事件處理

實戰案例

DOPPLER
Cyber Threat Solutions

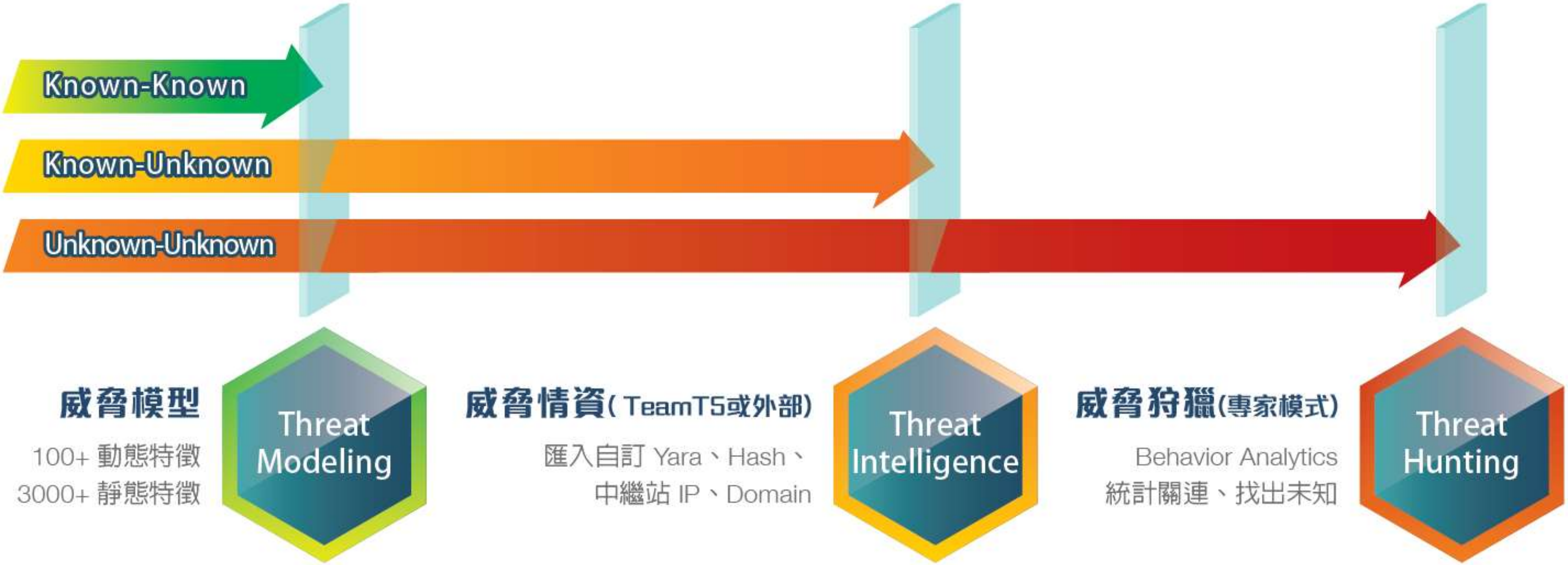
杜浦數位安全

JOHN

工欲善其事　必先利其器

ThreatSonar

多層次防禦架構



威脅模型

100+ 動態特徵
3000+ 靜態特徵

威脅情資(TeamT5或外部)

匯入自訂 Yara、Hash、
中繼站 IP、Domain

威脅狩獵(專家模式)

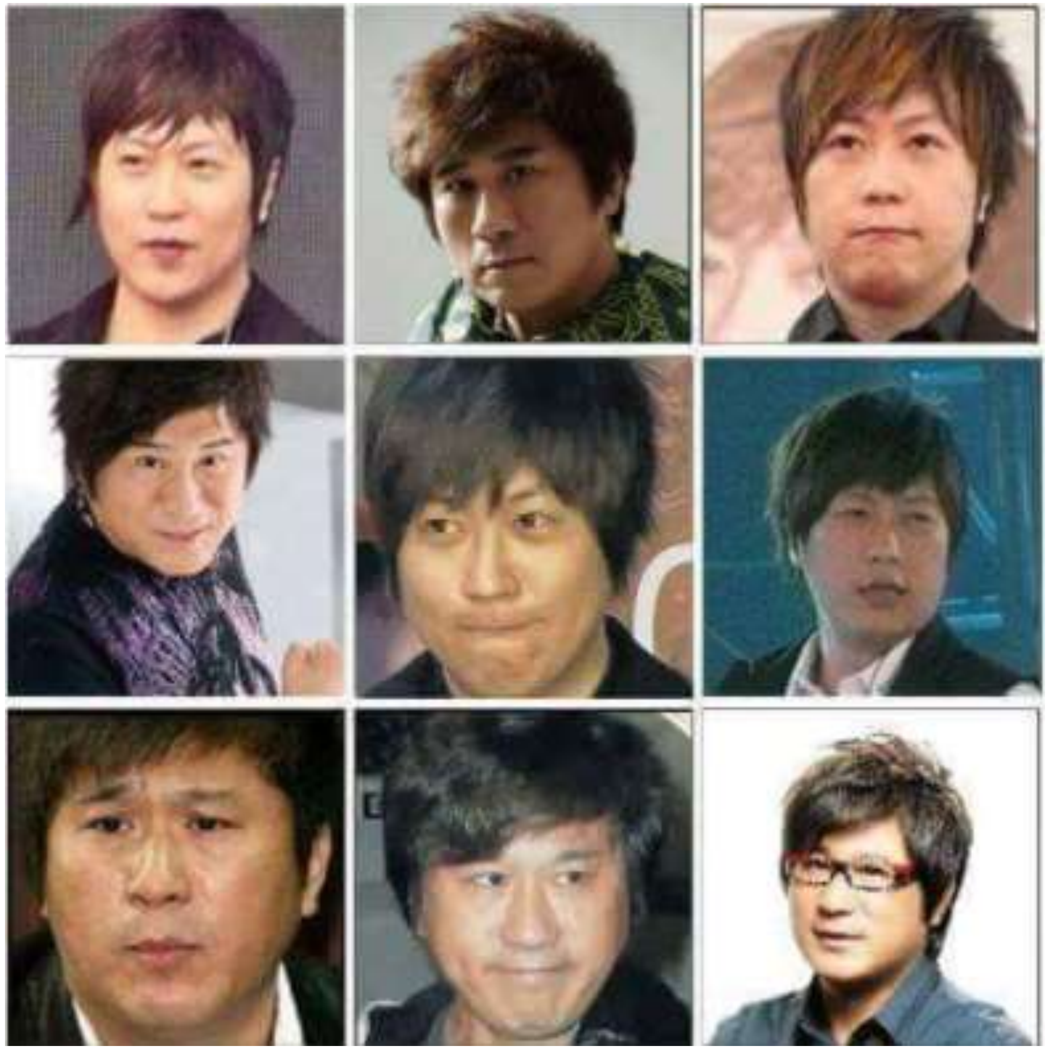
Behavior Analytics
統計關連、找出未知

主動式資安事件處理
- 威脅狩獵

TEAM T5

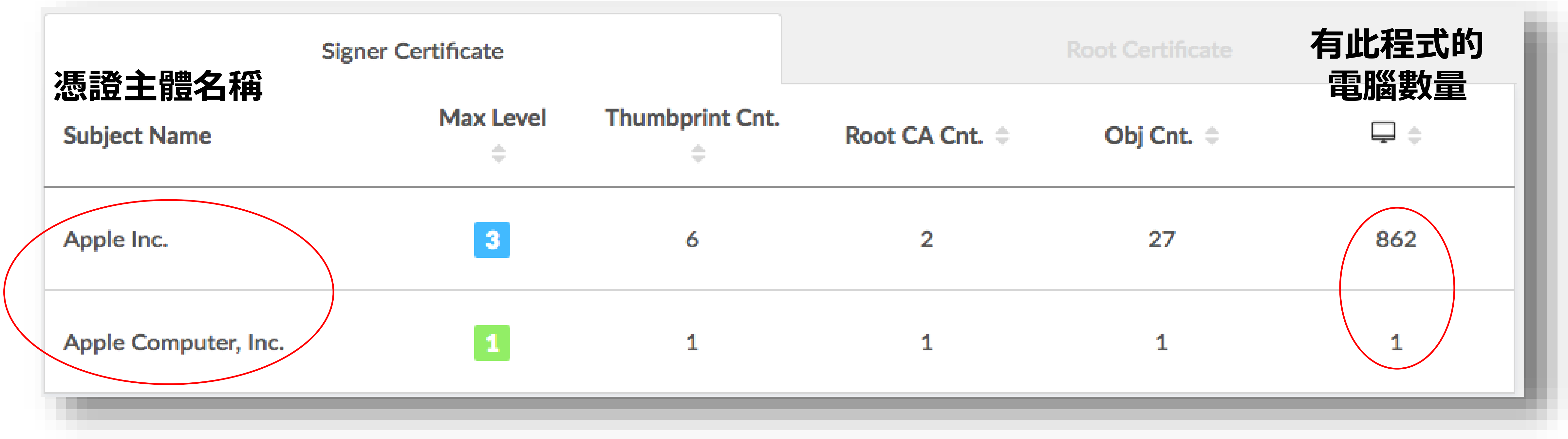
Cyber Security Research

找出異常的程式？



熱身一下

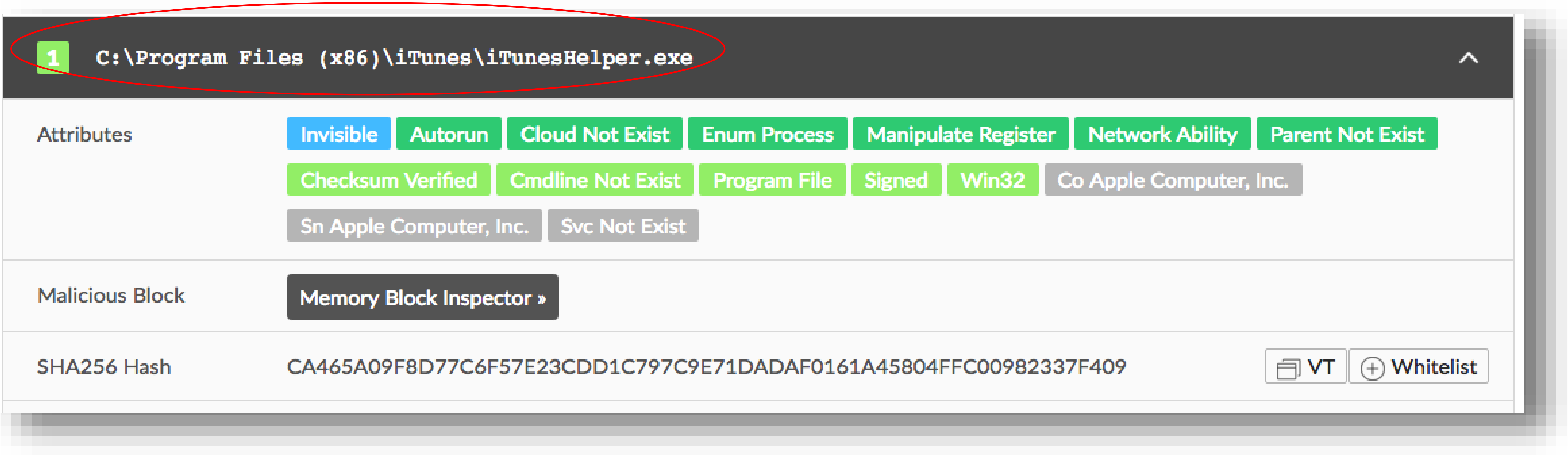
#1 APPLE



憑證主體名稱

有此程式的
電腦數量

Signer Certificate			Root Certificate		
Subject Name	Max Level	Thumbprint Cnt.	Root CA Cnt.	Obj Cnt.	🖥
Apple Inc.	3	6	2	27	862
Apple Computer, Inc.	1	1	1	1	1



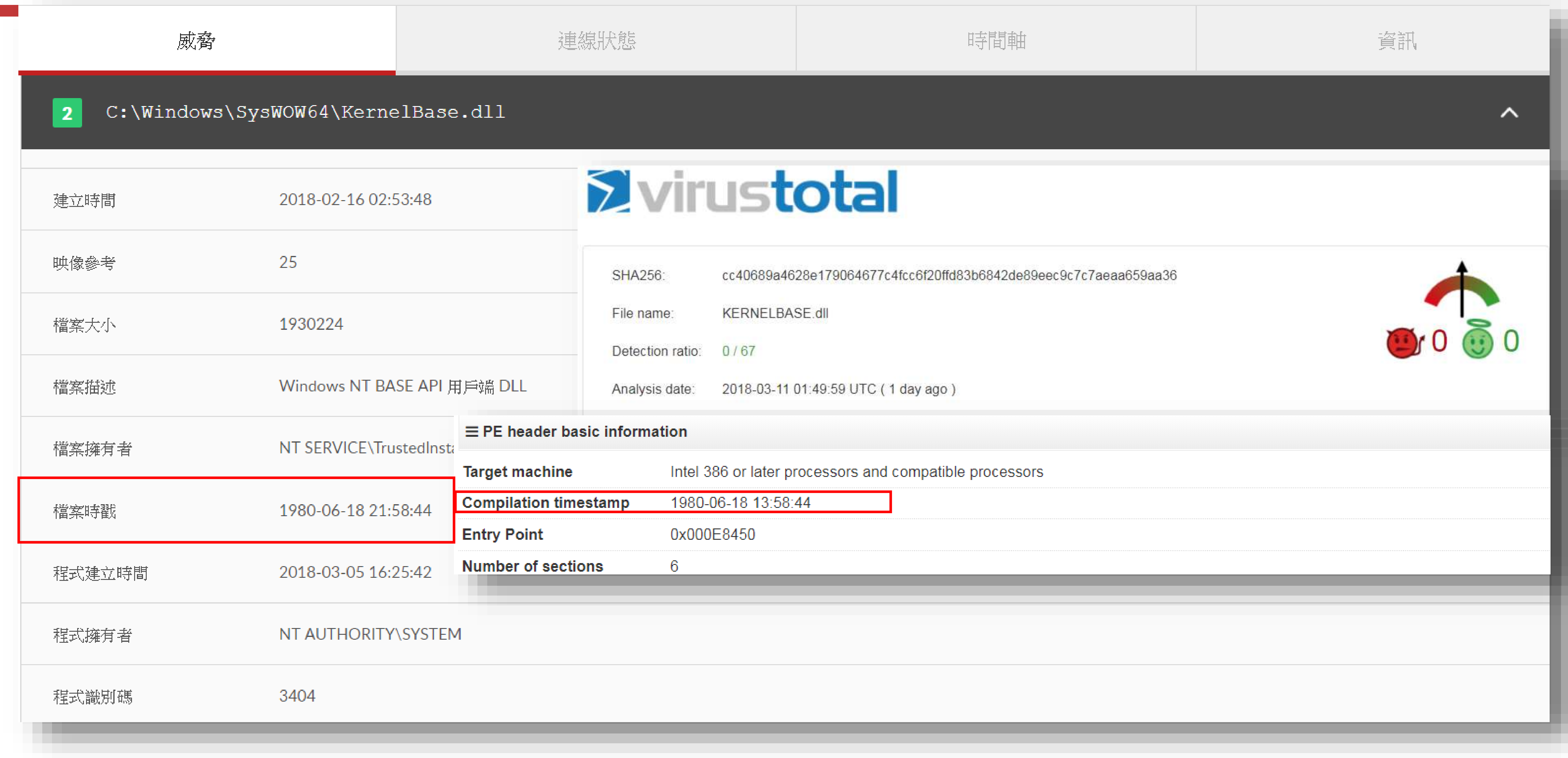
1 C:\Program Files (x86)\iTunes\iTunesHelper.exe

Attributes: Invisible, Autorun, Cloud Not Exist, Enum Process, Manipulate Register, Network Ability, Parent Not Exist, Checksum Verified, Cmdline Not Exist, Program File, Signed, Win32, Co Apple Computer, Inc., Sn Apple Computer, Inc., Svc Not Exist

Malicious Block

SHA256 Hash: CA465A09F8D77C6F57E23CDD1C797C9E71DADAF0161A45804FFC00982337F409

#2 微軟



2 C:\Windows\SysWOW64\KernelBase.dll

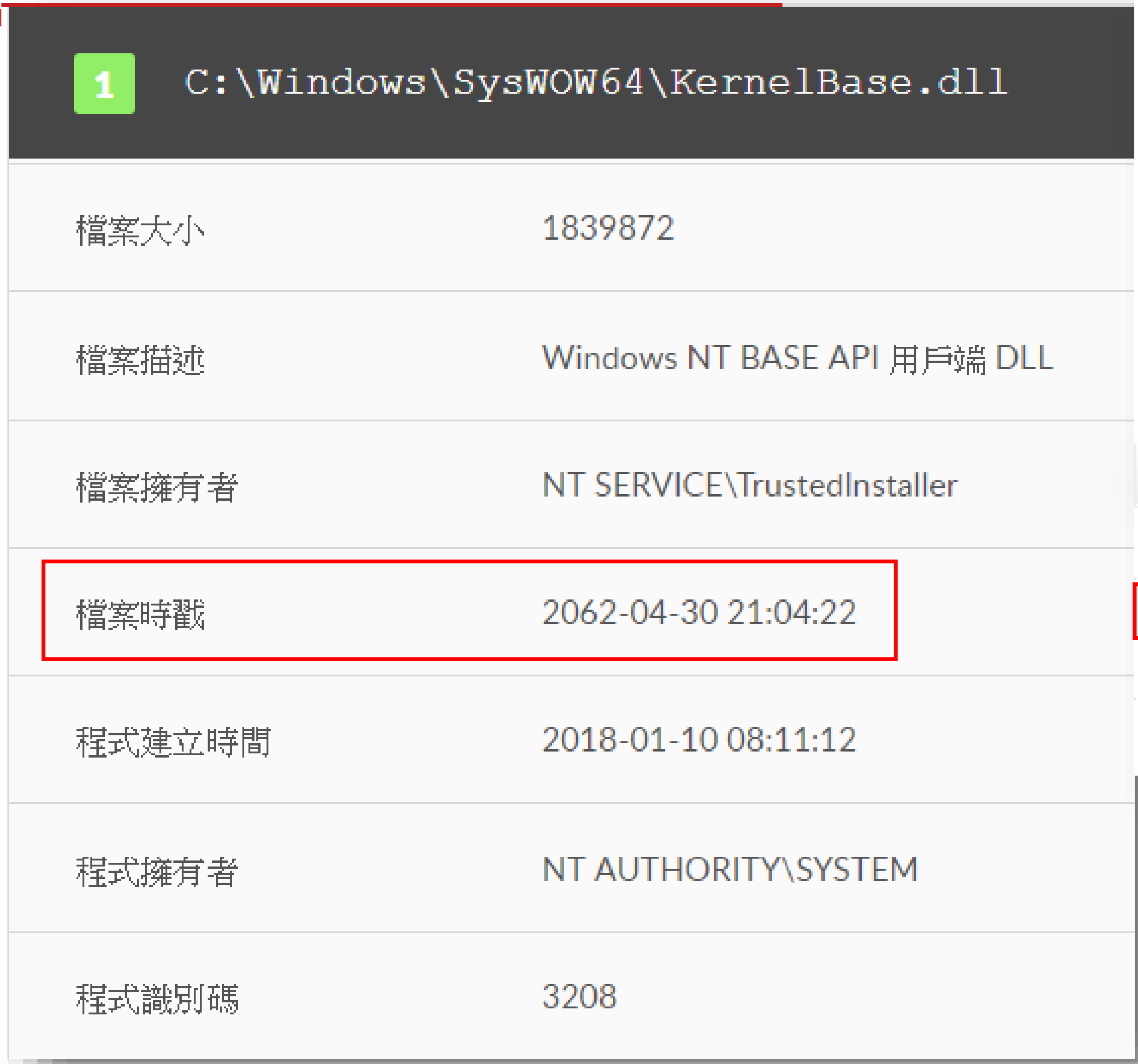
建立時間	2018-02-16 02:53:48
映像參考	25
檔案大小	1930224
檔案描述	Windows NT BASE API 用戶端 DLL
檔案擁有者	NT SERVICE\TrustedInsta
檔案時戳	1980-06-18 21:58:44
程式建立時間	2018-03-05 16:25:42
程式擁有者	NT AUTHORITY\SYSTEM
程式識別碼	3404

virustotal

SHA256:	cc40689a4628e179064677c4fcc6f20ffd83b6842de89eec9c7c7aeaa659aa36
File name:	KERNELBASE.dll
Detection ratio:	0 / 67
Analysis date:	2018-03-11 01:49:59 UTC (1 day ago)

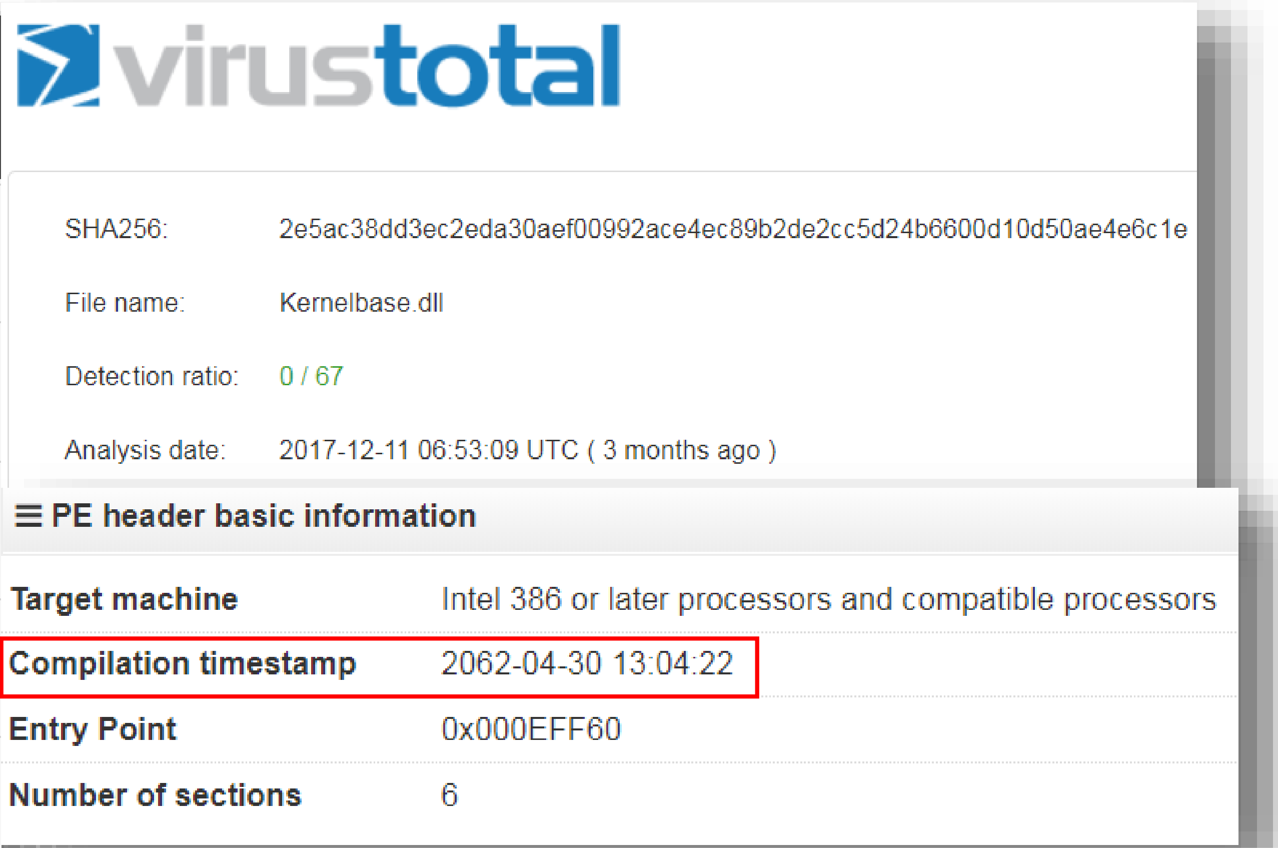
☰ PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	1980-06-18 13:58:44
Entry Point	0x000E8450
Number of sections	6



1 C:\Windows\SysWOW64\KernelBase.dll

檔案大小	1839872
檔案描述	Windows NT BASE API 用戶端 DLL
檔案擁有者	NT SERVICE\TrustedInstaller
檔案時戳	2062-04-30 21:04:22
程式建立時間	2018-01-10 08:11:12
程式擁有者	NT AUTHORITY\SYSTEM
程式識別碼	3208

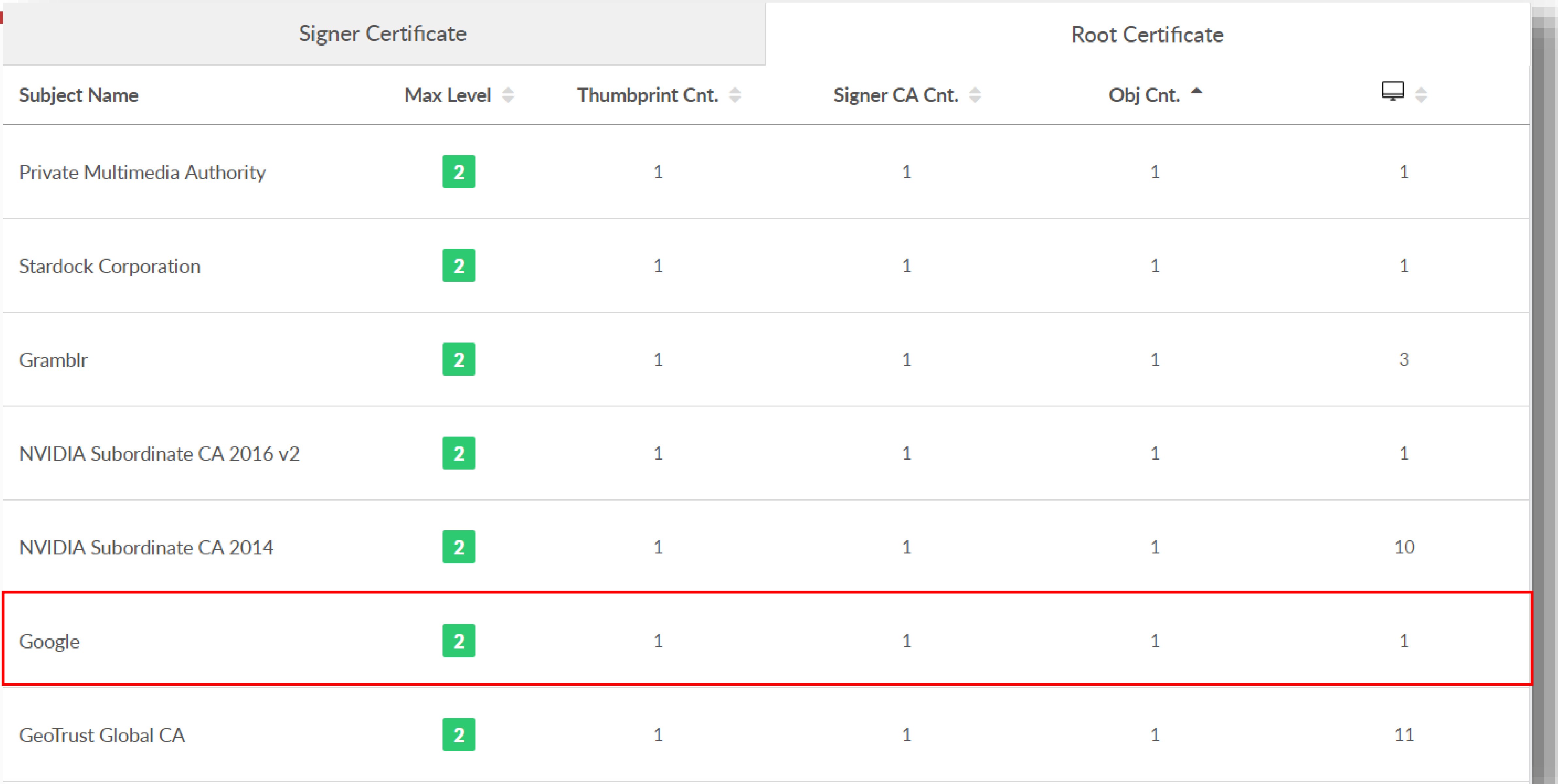


SHA256:	2e5ac38dd3ec2eda30aef00992ace4ec89b2de2cc5d24b6600d10d50ae4e6c1e
File name:	Kernelbase.dll
Detection ratio:	0 / 67
Analysis date:	2017-12-11 06:53:09 UTC (3 months ago)

≡ PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2062-04-30 13:04:22
Entry Point	0x000EFF60
Number of sections	6

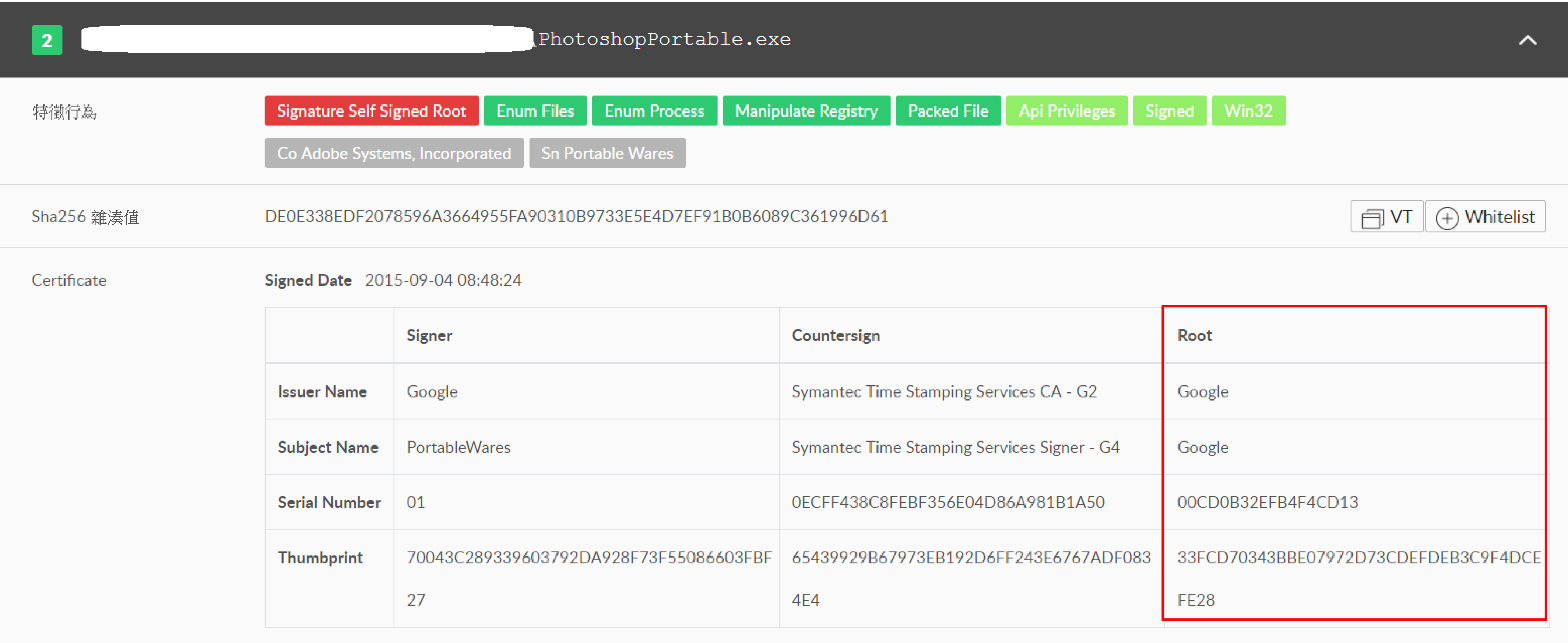
#3 root CA



Signer Certificate

Root Certificate

Subject Name	Max Level	Thumbprint Cnt.	Signer CA Cnt.	Obj Cnt.	🖥
Private Multimedia Authority	2	1	1	1	1
Stardock Corporation	2	1	1	1	1
Gramblr	2	1	1	1	3
NVIDIA Subordinate CA 2016 v2	2	1	1	1	1
NVIDIA Subordinate CA 2014	2	1	1	1	10
Google	2	1	1	1	1
GeoTrust Global CA	2	1	1	1	11



2 [redacted]PhotoshopPortable.exe

特徵行為

Signature Self Signed Root · Enum Files · Enum Process · Manipulate Registry · Packed File · Api Privileges · Signed · Win32

Co Adobe Systems, Incorporated · Sn Portable Wares

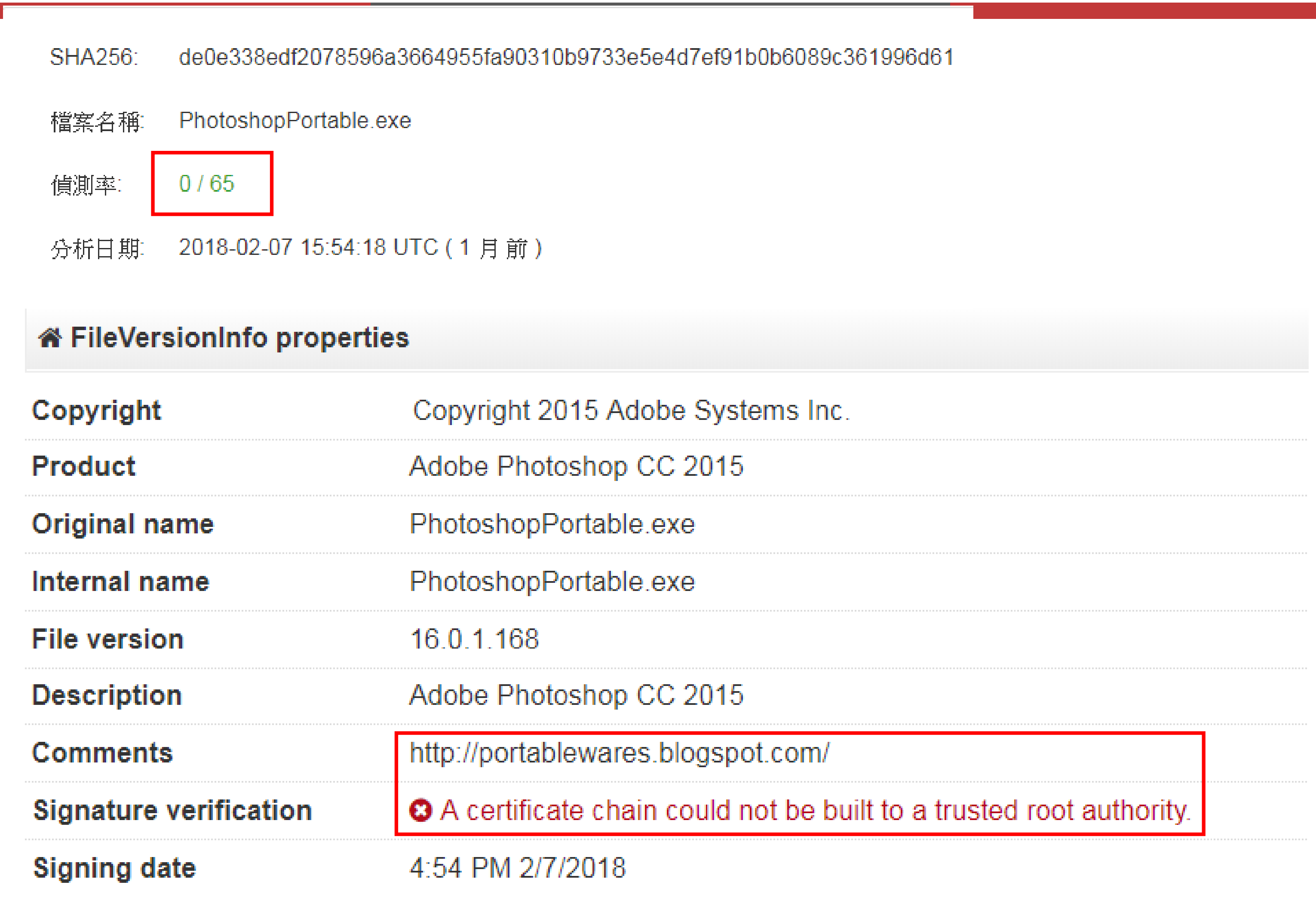
Sha256 雜湊值 DE0E338EDF2078596A3664955FA90310B9733E5E4D7EF91B0B6089C361996D61

Certificate

Signed Date 2015-09-04 08:48:24

	Signer	Countersign	Root
Issuer Name	Google	Symantec Time Stamping Services CA - G2	Google
Subject Name	PortableWares	Symantec Time Stamping Services Signer - G4	Google
Serial Number	01	0ECFF438C8FEBF356E04D86A981B1A50	00CD0B32EFB4F4CD13
Thumbprint	70043C289339603792DA928F73F55086603FBF27	65439929B67973EB192D6FF243E6767ADF0834E4	33FCD70343BBE07972D73CDEFDEB3C9F4DCEFE28

VT 0檢出



SHA256: de0e338edf2078596a3664955fa90310b9733e5e4d7ef91b0b6089c361996d61

檔案名稱: PhotoshopPortable.exe

偵測率: 0 / 65

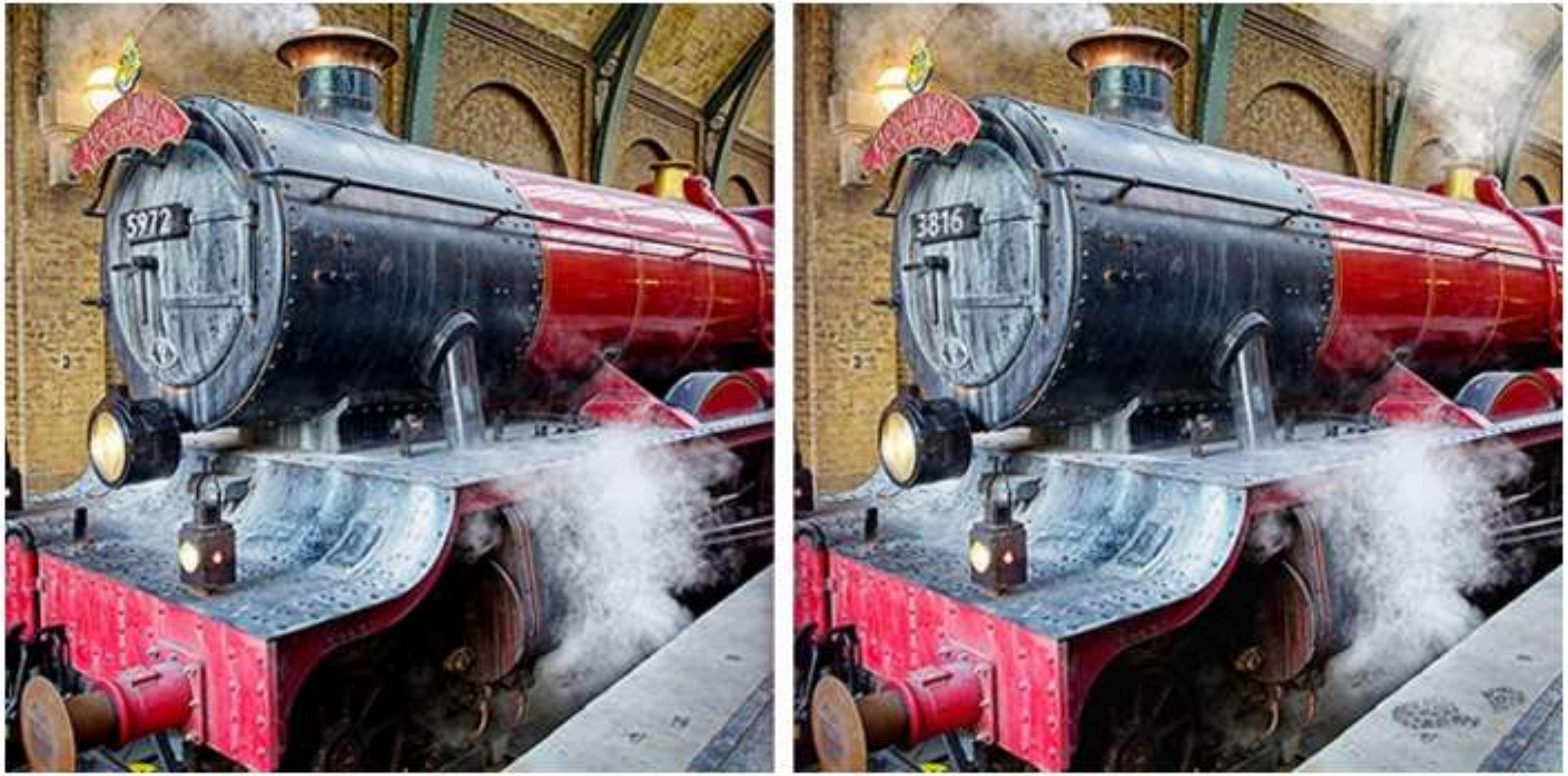
分析日期: 2018-02-07 15:54:18 UTC (1 月 前)

FileVersionInfo properties

Copyright	Copyright 2015 Adobe Systems Inc.
Product	Adobe Photoshop CC 2015
Original name	PhotoshopPortable.exe
Internal name	PhotoshopPortable.exe
File version	16.0.1.168
Description	Adobe Photoshop CC 2015
Comments	http://portablewares.blogspot.com/
Signature verification	☒ A certificate chain could not be built to a trusted root authority.
Signing date	4:54 PM 2/7/2018

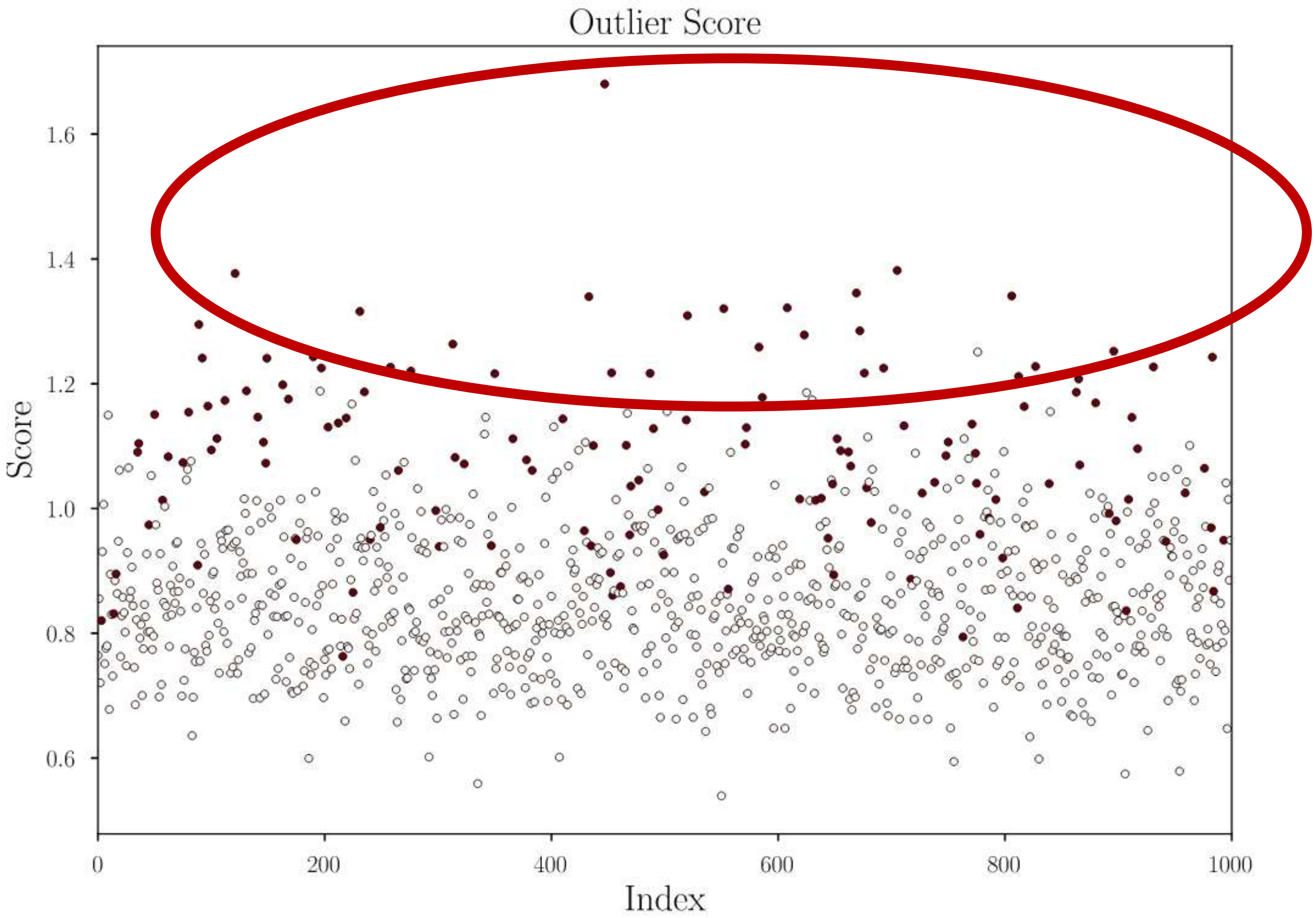
Let’s GO Hunting!

A. 相同的程式應該具備相同的功能



B. 真實環境中，惡意程式通常佔少數

找出功能異常的程式

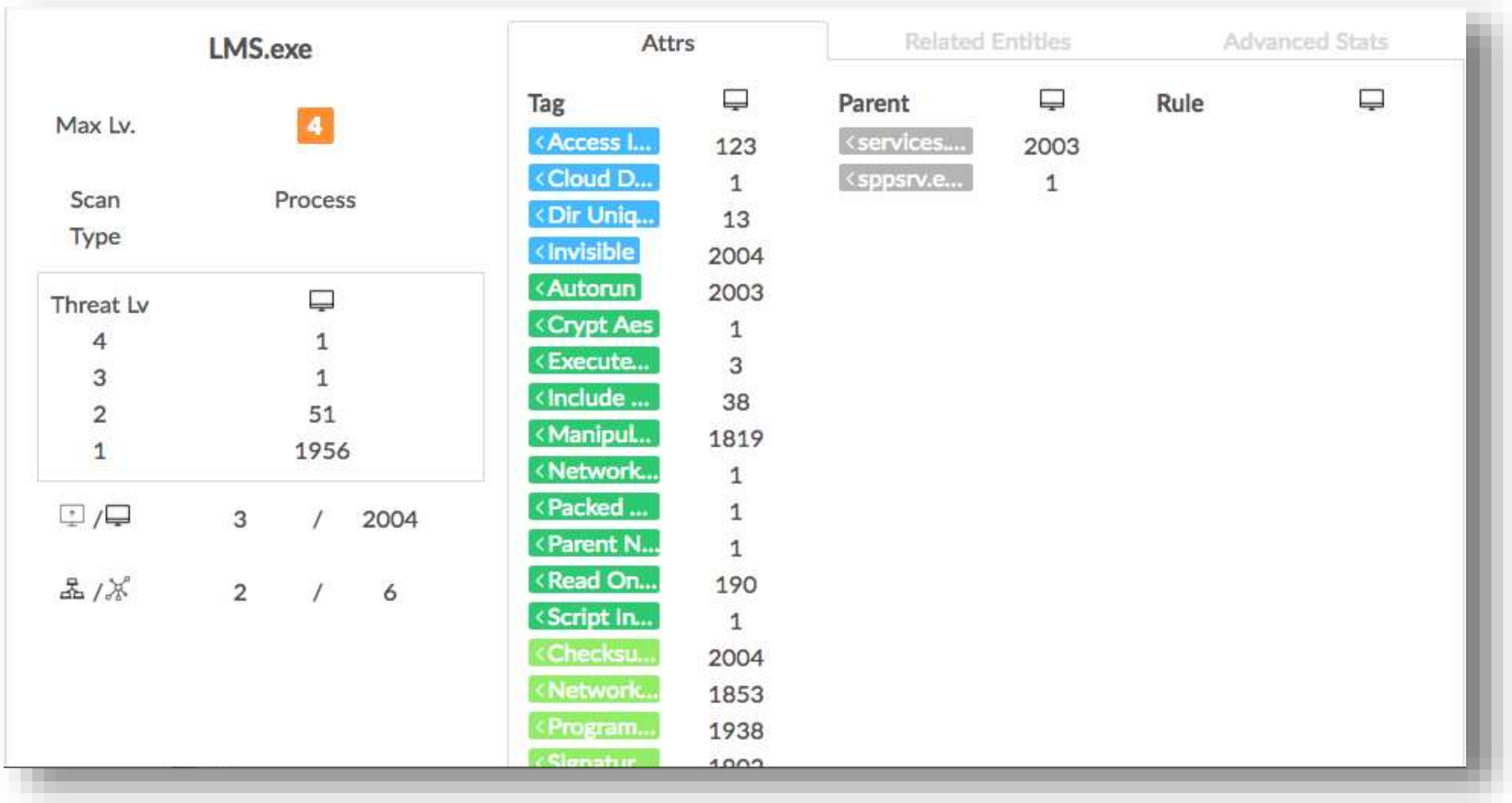

Outlier Score
Score
Index
1.6
1.4
1.2
1.0
0.8
0.6
0
200
400
600
800
1000

威脅狩獵

- 如何透過威脅狩獵來搜尋未知的惡意程式？

- 如何搜尋延伸的問題？

Case #1



LMS.exe

Max Lv.	4
Scan Type	Process

Threat Lv	🖥
4	1
3	1
2	51
1	1956

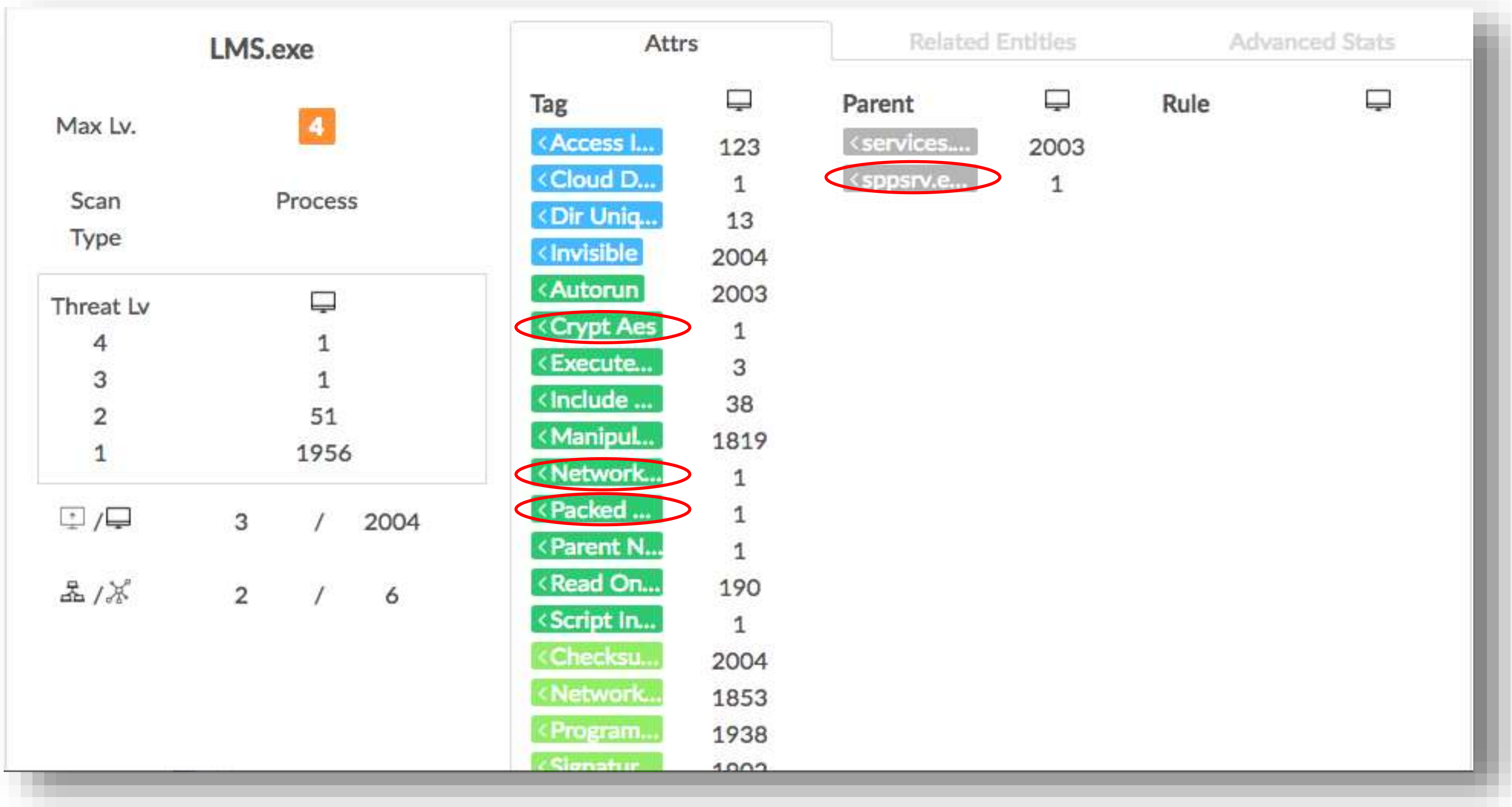
🖥 / 🖥	3	/	2004
品 / ✲	2	/	6

Tag	🖥
‹Access I...	123
‹Cloud D...	1
‹Dir Uniq...	13
‹Invisible	2004
‹Autorun	2003
‹Crypt Aes	1
‹Execute...	3
‹Include ...	38
‹Manipul...	1819
‹Network...	1
‹Packed ...	1
‹Parent N...	1
‹Read On...	190
‹Script In...	1
‹Checksu...	2004
‹Network...	1853
‹Program...	1938
‹Signatur	1993

Parent	🖥
‹services....	2003
‹sppsrv.e...	1

Rule	🖥

哪裡怪怪的？



LMS.exe

Max Lv. 4

Scan Type Process

Threat Lv	🖥
4	1
3	1
2	51
1	1956

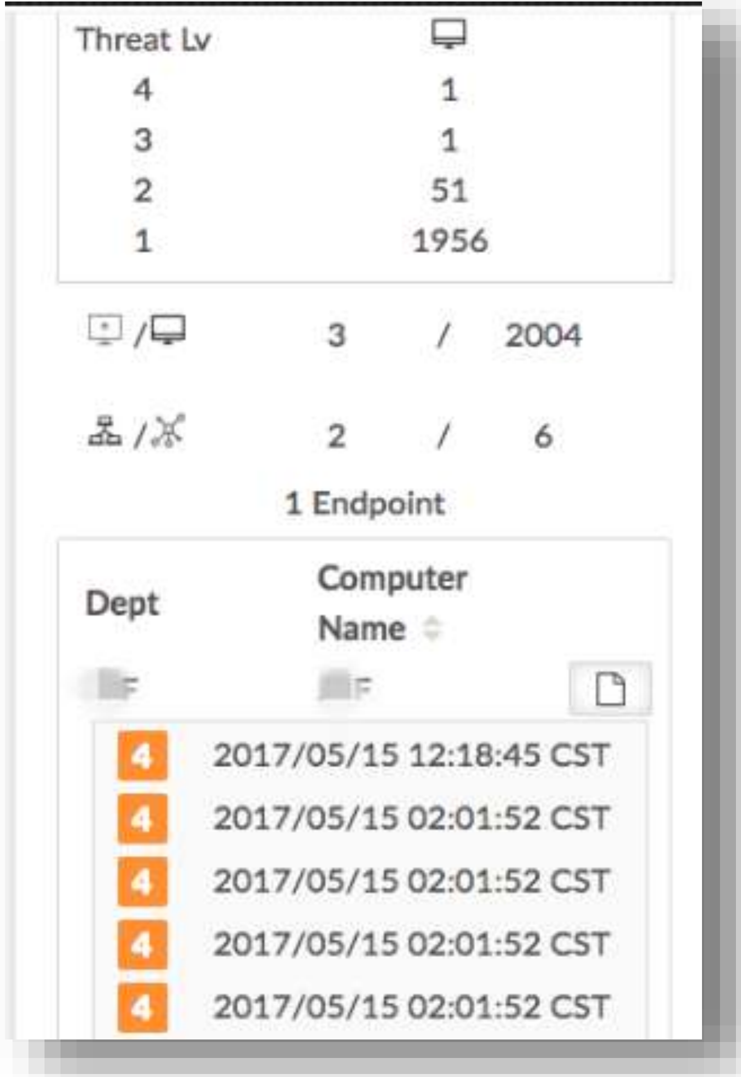
🖥 / 🖥	3 / 2004	
品 / ✲	2 / 6	

Attrs | Related Entities | Advanced Stats

Tag	🖥
Access I...	123
Cloud D...	1
Dir Uniq...	13
Invisible	2004
Autorun	2003
Crypt Aes	1
Execute...	3
Include ...	38
Manipul...	1819
Network...	1
Packed ...	1
Parent N...	1
Read On...	190
Script In...	1
Checksu...	2004
Network...	1853
Program...	1938
Signatur	1803

Parent	🖥
services....	2003
sppsrv.e...	1

Rule	🖥



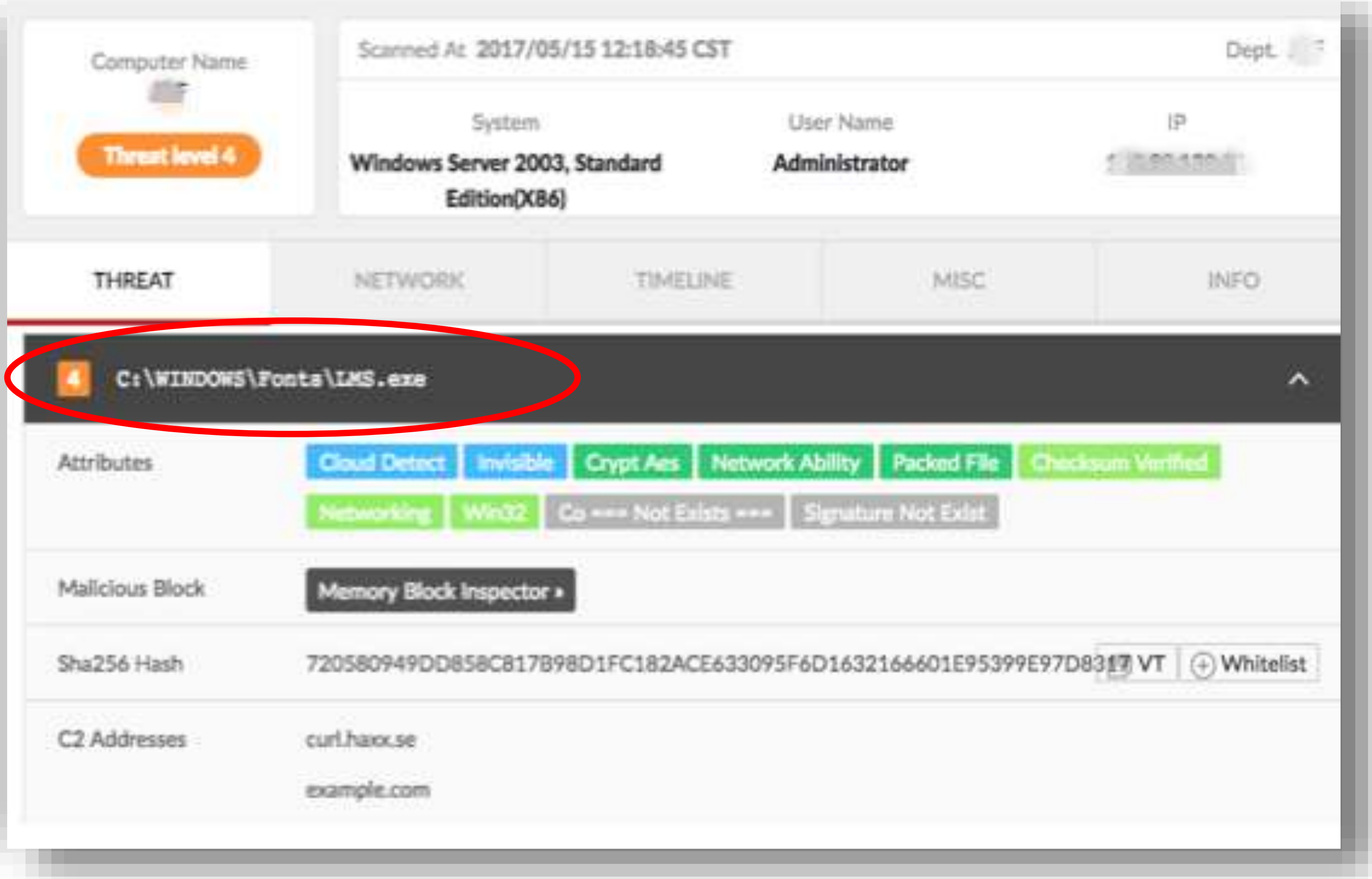
Threat Lv	🖥
4	1
3	1
2	51
1	1956

🖥 / 🖥	3	/	2004
品 / ✕	2	/	6

1 Endpoint

Dept	Computer Name
[redacted]	[redacted]

4	2017/05/15 12:18:45 CST
4	2017/05/15 02:01:52 CST
4	2017/05/15 02:01:52 CST
4	2017/05/15 02:01:52 CST
4	2017/05/15 02:01:52 CST



Computer Name [redacted]

Threat level 4

Scanned At 2017/05/15 12:18:45 CST

Dept. [redacted]

System	User Name	IP
Windows Server 2003, Standard Edition(X86)	Administrator	[redacted]

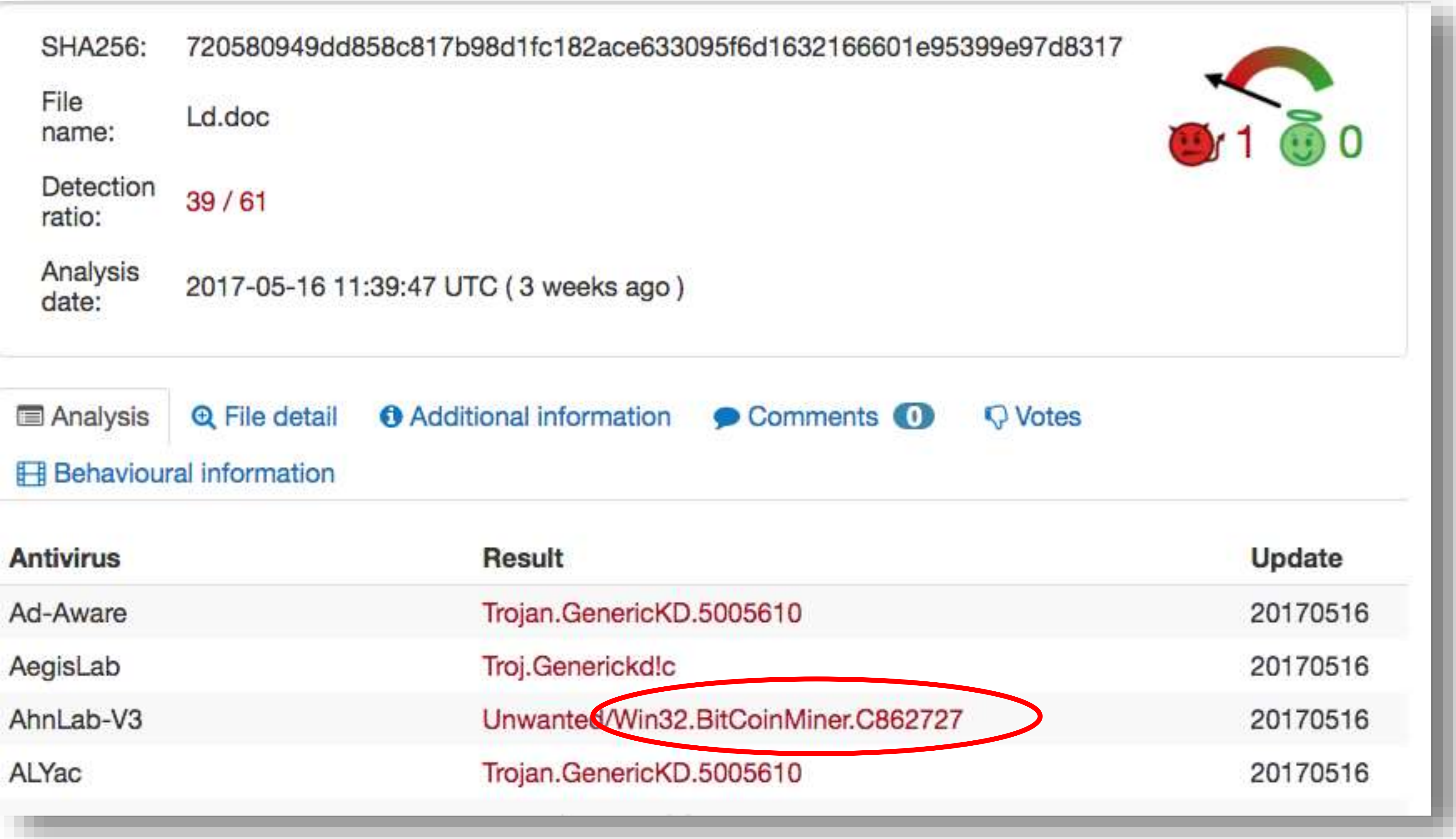
4 C:\WINDOWS\Fonts\LMS.exe

Attributes: Cloud Detect, Invisible, Crypt Aes, Network Ability, Packed File, Checksum Verified, Networking, Win32, Co === Not Exists ===, Signature Not Exist

Malicious Block: Memory Block Inspector »

Sha256 Hash: 720580949DD858C817B98D1FC182ACE633095F6D1632166601E95399E97D8317

C2 Addresses: curl.haxx.se
example.com

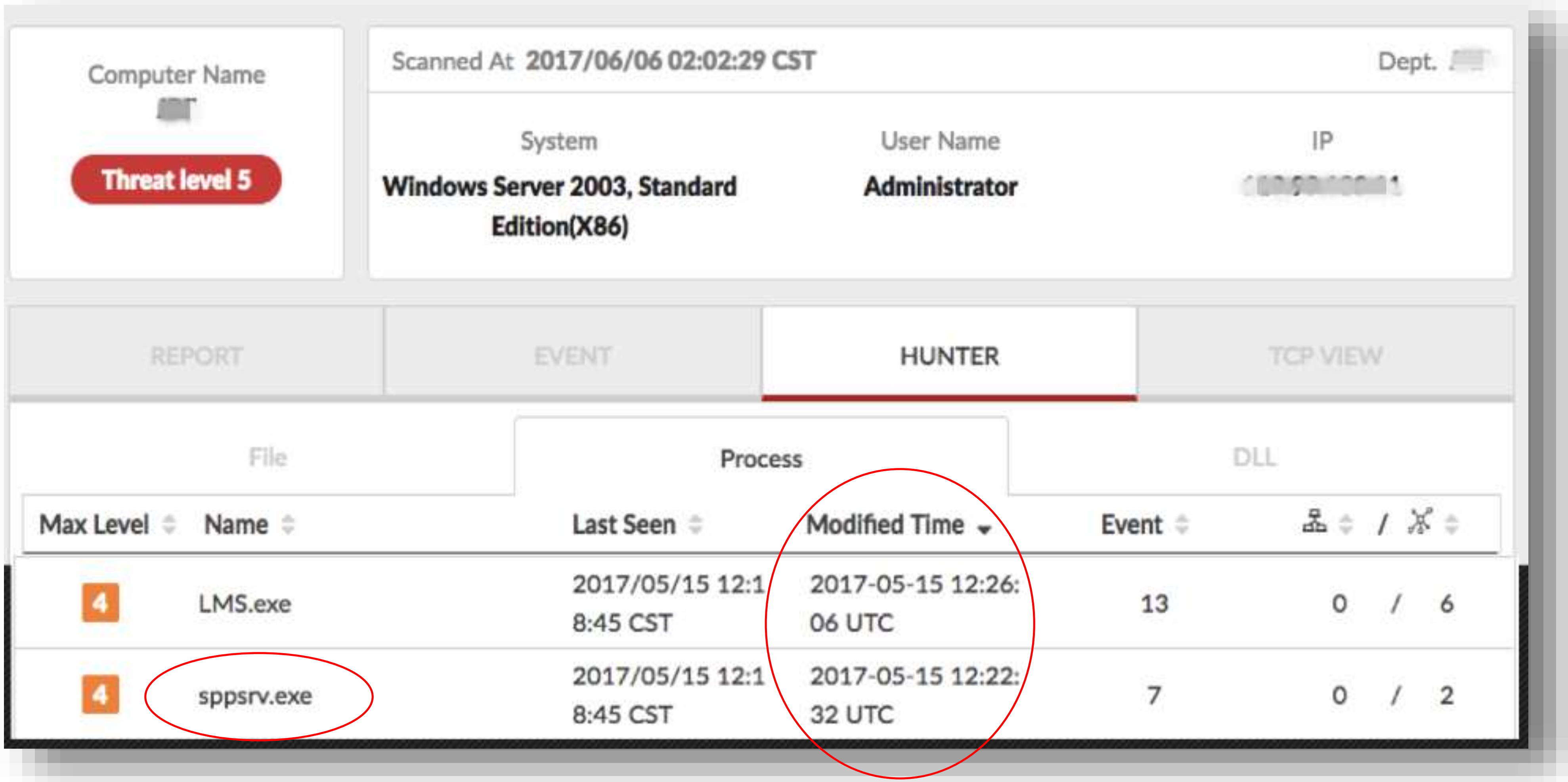


SHA256:	720580949dd858c817b98d1fc182ace633095f6d1632166601e95399e97d8317
File name:	Ld.doc
Detection ratio:	39 / 61
Analysis date:	2017-05-16 11:39:47 UTC (3 weeks ago)

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.5005610	20170516
AegisLab	Troj.Generickd!c	20170516
AhnLab-V3	Unwanted/Win32.BitCoinMiner.C862727	20170516
ALYac	Trojan.GenericKD.5005610	20170516

繼續調查…

- 透過檔案修改時間來關聯



Computer Name

[redacted]

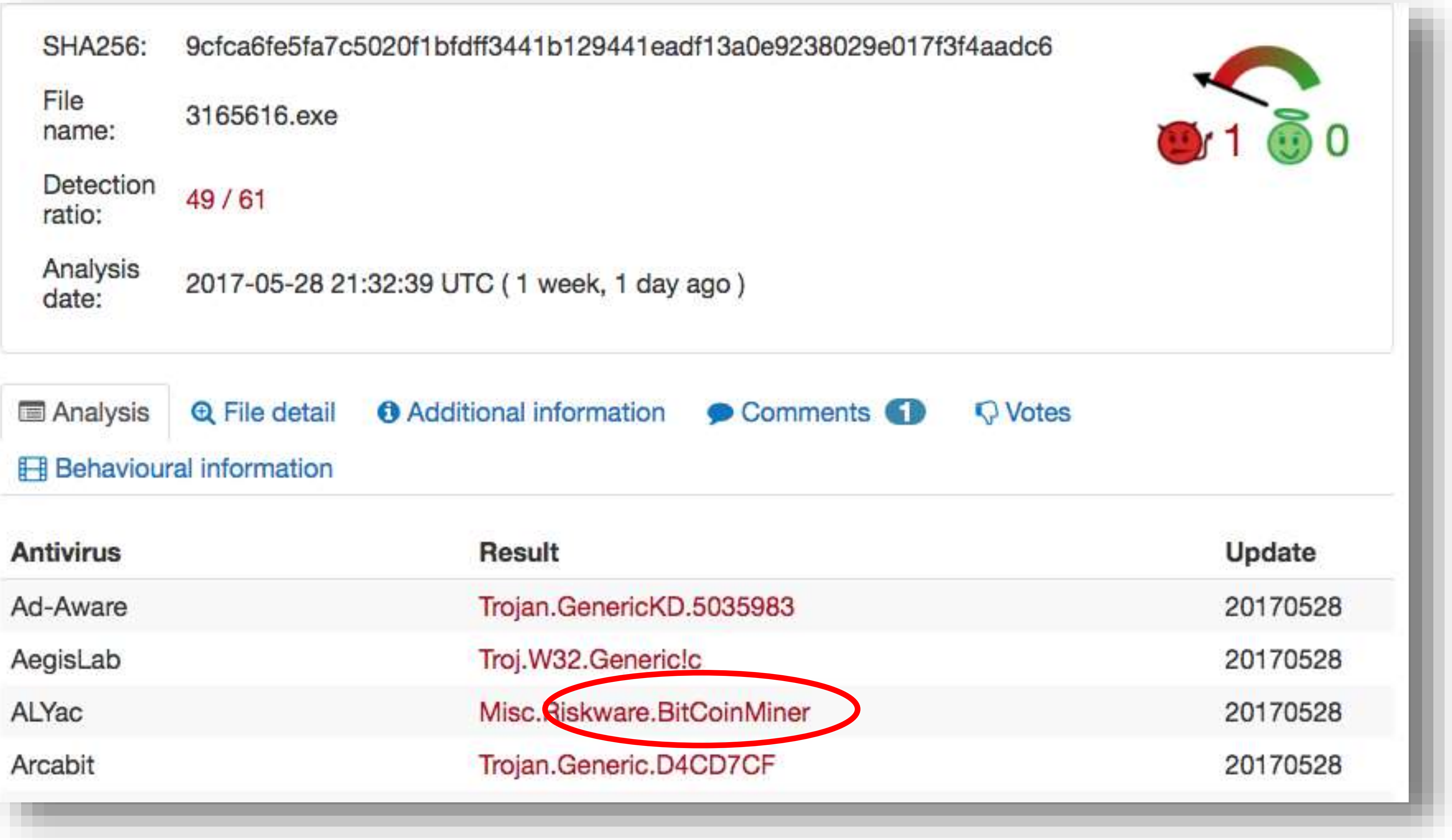
Threat level 5

Scanned At 2017/06/06 02:02:29 CST

Dept. [redacted]

System	User Name	IP
Windows Server 2003, Standard Edition(X86)	Administrator	[redacted]

Max Level	Name	Last Seen	Modified Time	Event	/
4	LMS.exe	2017/05/15 12:18:45 CST	2017-05-15 12:26:06 UTC	13	0 / 6
4	sppsrv.exe	2017/05/15 12:18:45 CST	2017-05-15 12:22:32 UTC	7	0 / 2



SHA256: 9cfca6fe5fa7c5020f1bfdff3441b129441eadf13a0e9238029e017f3f4aadc6

File name: 3165616.exe

Detection ratio: 49 / 61

Analysis date: 2017-05-28 21:32:39 UTC (1 week, 1 day ago)

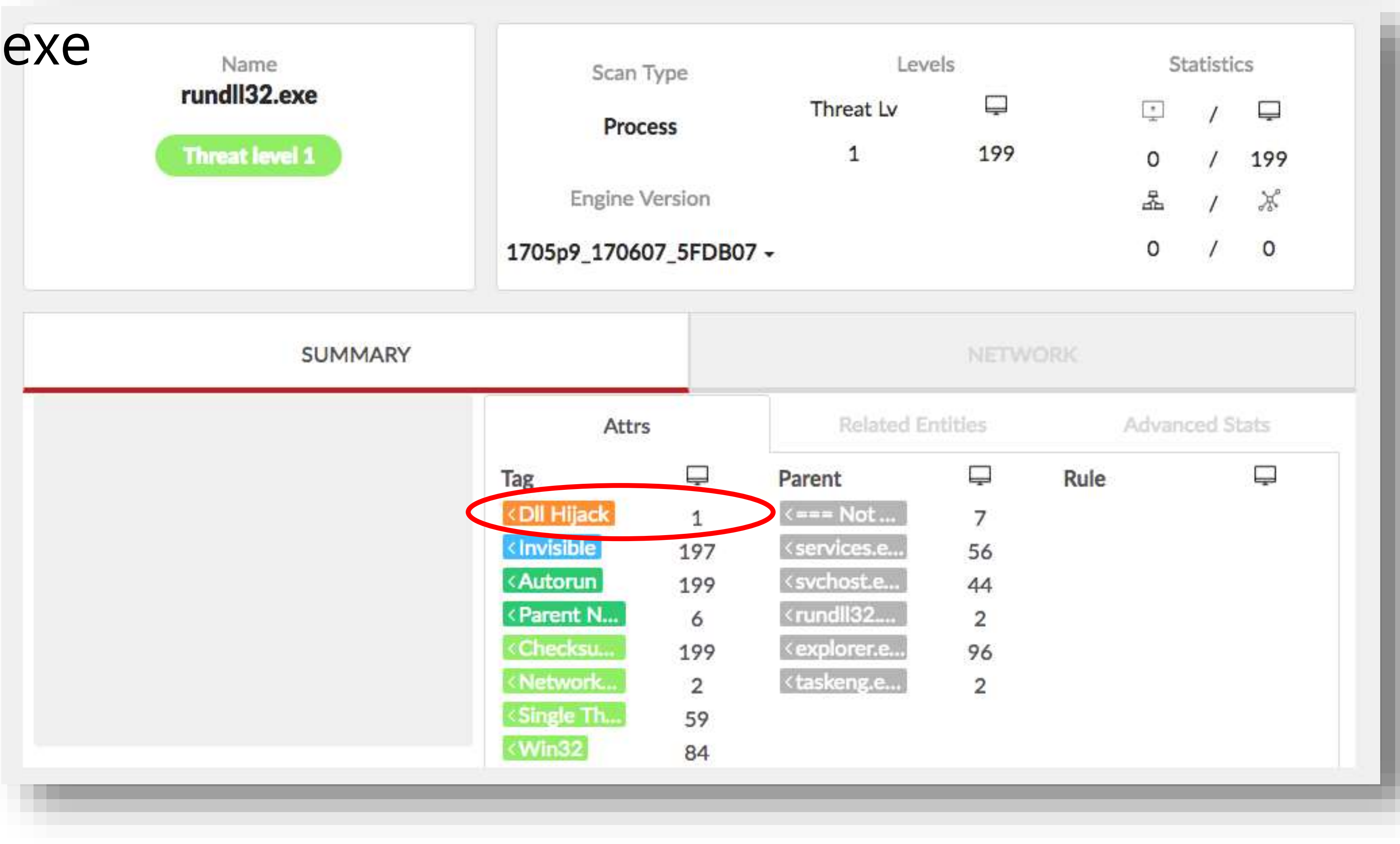
Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.5035983	20170528
AegisLab	Troj.W32.Generic!c	20170528
ALYac	Misc.Riskware.BitCoinMiner	20170528
Arcabit	Trojan.Generic.D4CD7CF	20170528

Case #2

TEAM T5
Cyber Security Research

Case #2

發現某一台主機rundll32.exe
有 DLL劫持（Dll Hijack）



Name
rundll32.exe
Threat level 1

Scan Type
Process

Engine Version
1705p9_170607_5FDB07 ▾

Levels

Threat Lv	🖥
1	199

Statistics

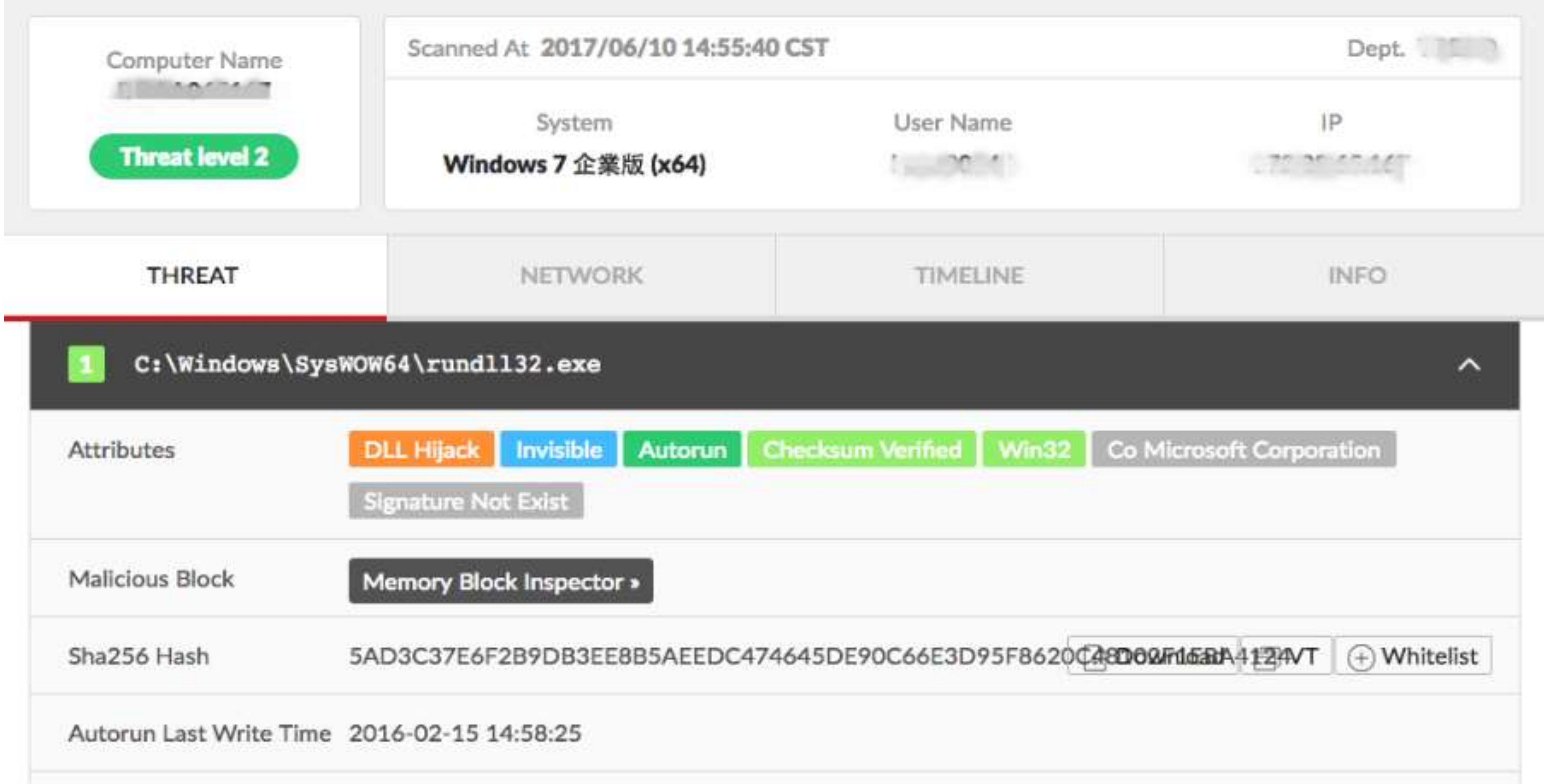
🖥	/	🖥
0	/	199
品	/	✕
0	/	0

SUMMARY | NETWORK

Attrs | Related Entities | Advanced Stats

Tag	🖥	Parent	🖥	Rule	🖥
‹Dll Hijack	1	‹=== Not ...	7		
‹Invisible	197	‹services.e...	56		
‹Autorun	199	‹svchost.e...	44		
‹Parent N...	6	‹rundll32....	2		
‹Checksu...	199	‹explorer.e...	96		
‹Network...	2	‹taskeng.e...	2		
‹Single Th...	59				
‹Win32	84				

觀察異常報告的掃描細節



Computer Name
[redacted]

Threat level 2

Scanned At 2017/06/10 14:55:40 CST

Dept. [redacted]

System
Windows 7 企業版 (x64)

User Name
[redacted]

IP
[redacted]

THREAT | NETWORK | TIMELINE | INFO

1 C:\Windows\SysWOW64\rundll32.exe

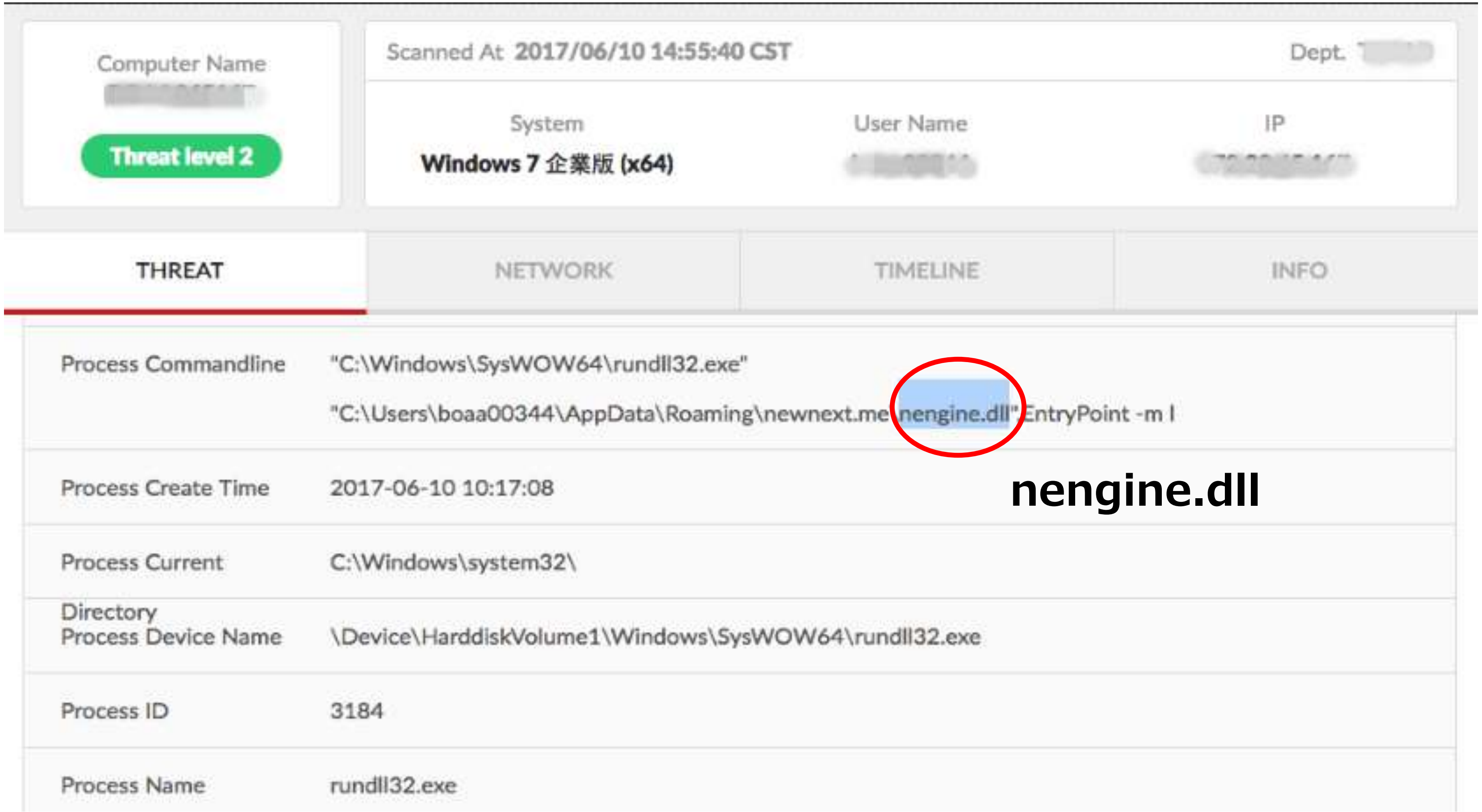
Attributes: DLL Hijack, Invisible, Autorun, Checksum Verified, Win32, Co Microsoft Corporation, Signature Not Exist

Malicious Block: Memory Block Inspector »

Sha256 Hash: 5AD3C37E6F2B9DB3EE8B5AEEDC474645DE90C66E3D95F8620C48D02F16BA4124 Download VT ⊕ Whitelist

Autorun Last Write Time: 2016-02-15 14:58:25

Command-Line



Computer Name [redacted]

Threat level 2

Scanned At 2017/06/10 14:55:40 CST

Dept. [redacted]

System	User Name	IP
Windows 7 企業版 (x64)	[redacted]	[redacted]

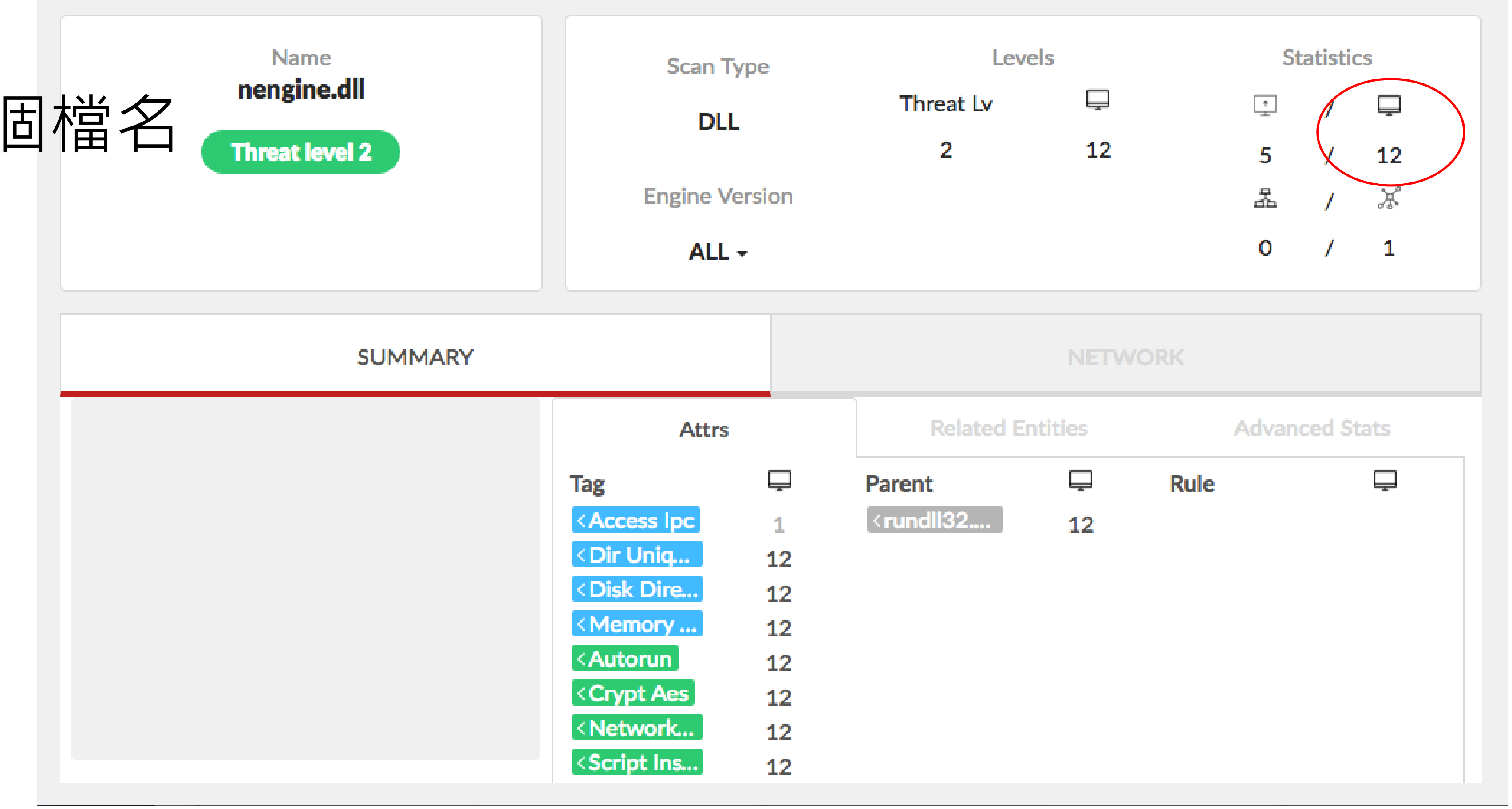
Process Commandline	"C:\Windows\SysWOW64\rundll32.exe" "C:\Users\boaa00344\AppData\Roaming\newnext.me\nengine.dll",EntryPoint -m I
Process Create Time	2017-06-10 10:17:08
Process Current Directory	C:\Windows\system32\
Process Device Name	\Device\HarddiskVolume1\Windows\SysWOW64\rundll32.exe
Process ID	3184
Process Name	rundll32.exe

nengine.dll

關聯到nengine.dll

- 過去所有掃描結果

總共12台電腦具備這個檔名



Name

nengine.dll

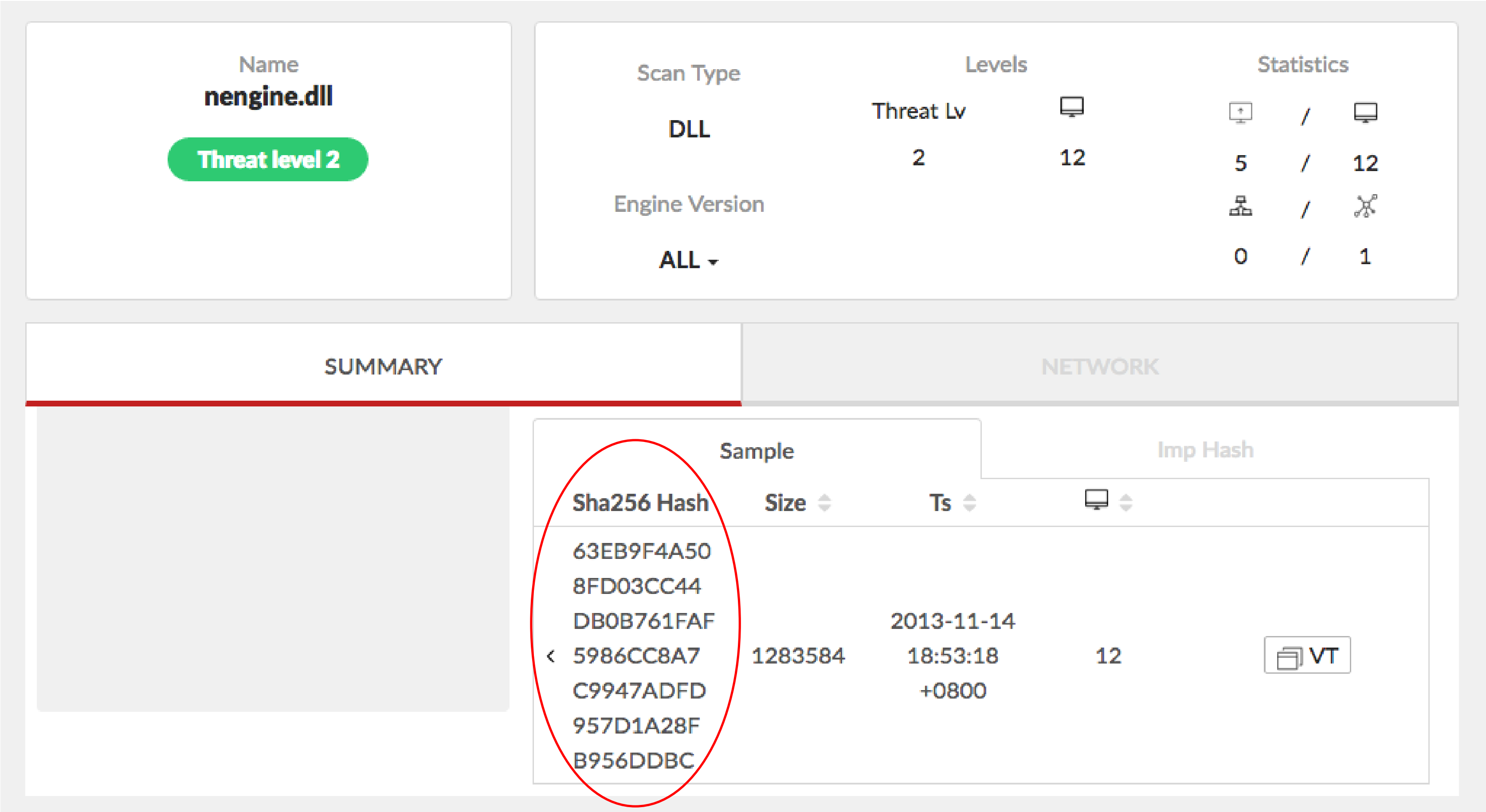
Threat level 2

Scan Type	Levels		Statistics		
	Threat Lv	🖥		/	🖥
DLL	2	12	5	/	12
Engine Version				/	
ALL ▾			0	/	1

Tag	🖥	Parent	🖥	Rule	🖥
‹Access Ipc	1	‹rundll32....	12		
‹Dir Uniq...	12				
‹Disk Dire...	12				
‹Memory ...	12				
‹Autorun	12				
‹Crypt Aes	12				
‹Network...	12				
‹Script Ins...	12				

確定是相同的檔案

- 共有12台具備相同sha256 hash



Name
nengine.dll
Threat level 2

Scan Type
DLL

Engine Version
ALL ▾

Levels

Threat Lv	🖥
2	12

Statistics

🖥	/	🖥
5	/	12
0	/	1

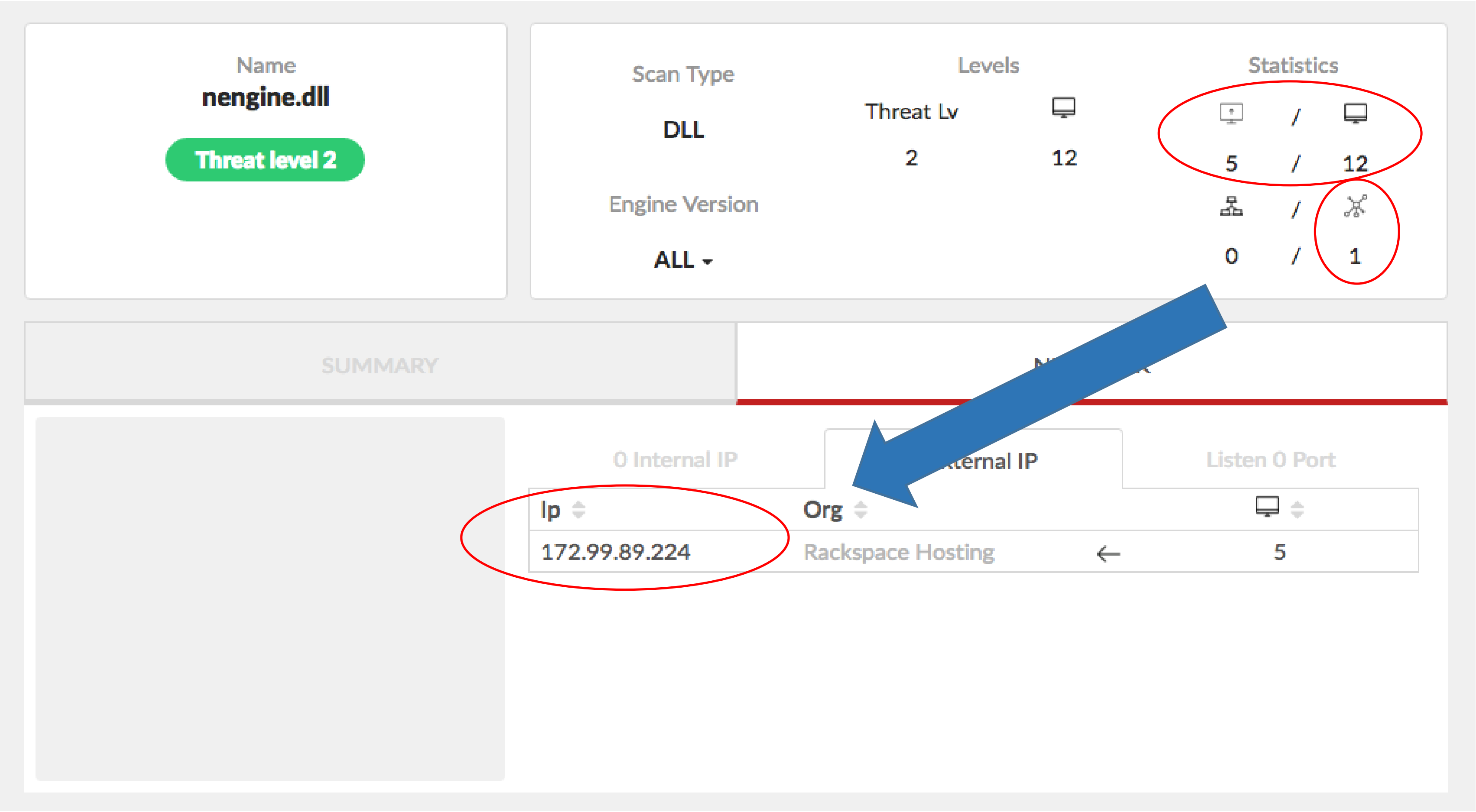
SUMMARY | NETWORK

Sample | Imp Hash

Sha256 Hash	Size	Ts	🖥	
63EB9F4A508FD03CC44DB0B761FAF5986CC8A7C9947ADFD957D1A28FB956DDBC	1283584	2013-11-14 18:53:18 +0800	12	VT

觀察連線的狀況

- 有5台當前掃描時候正在連線IP



Name
nengine.dll
Threat level 2

Scan Type
DLL

Engine Version
ALL ▾

Levels
Threat Lv 2
🖥 12

Statistics
5 / 12
0 / 1

SUMMARY

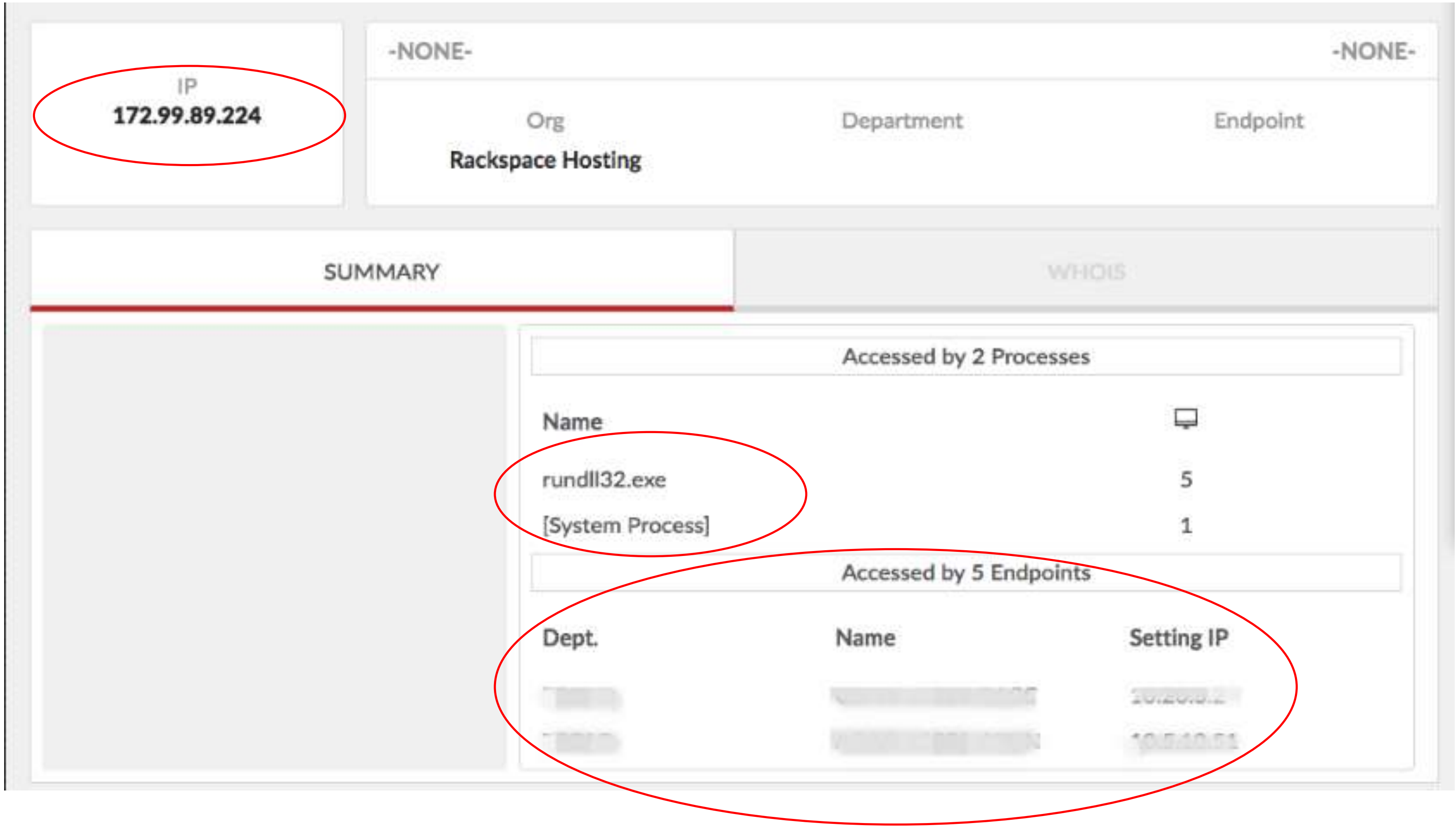
0 Internal IP

ternal IP

Listen 0 Port

Ip	Org		🖥
172.99.89.224	Rackspace Hosting	←	5

這個IP還有哪些 Process會連？



-NONE- -NONE-

IP
172.99.89.224

Org
Rackspace Hosting

Department

Endpoint

SUMMARY WHOIS

Accessed by 2 Processes

Name	🖥
rundll32.exe	5
[System Process]	1

Accessed by 5 Endpoints

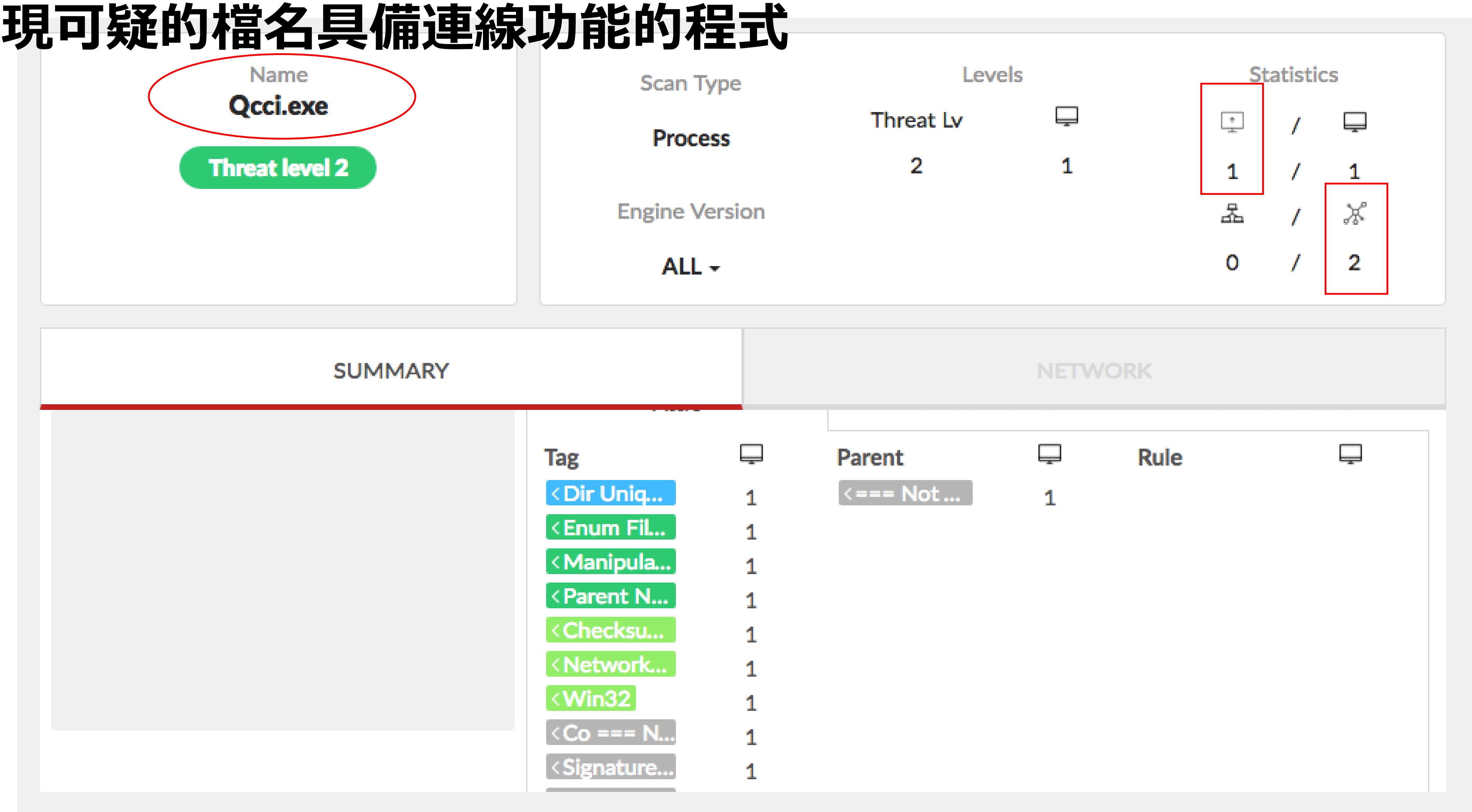
Dept.	Name	Setting IP
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Case #3

TEAM T5
Cyber Security Research

Case #3

發現可疑的檔名具備連線功能的程式



Name
Qcci.exe

Threat level 2

Scan Type
Process

Engine Version
ALL ▾

Levels

Threat Lv	🖥
2	1

Statistics

🖥	/	🖥
1	/	1
品	/	✳
0	/	2

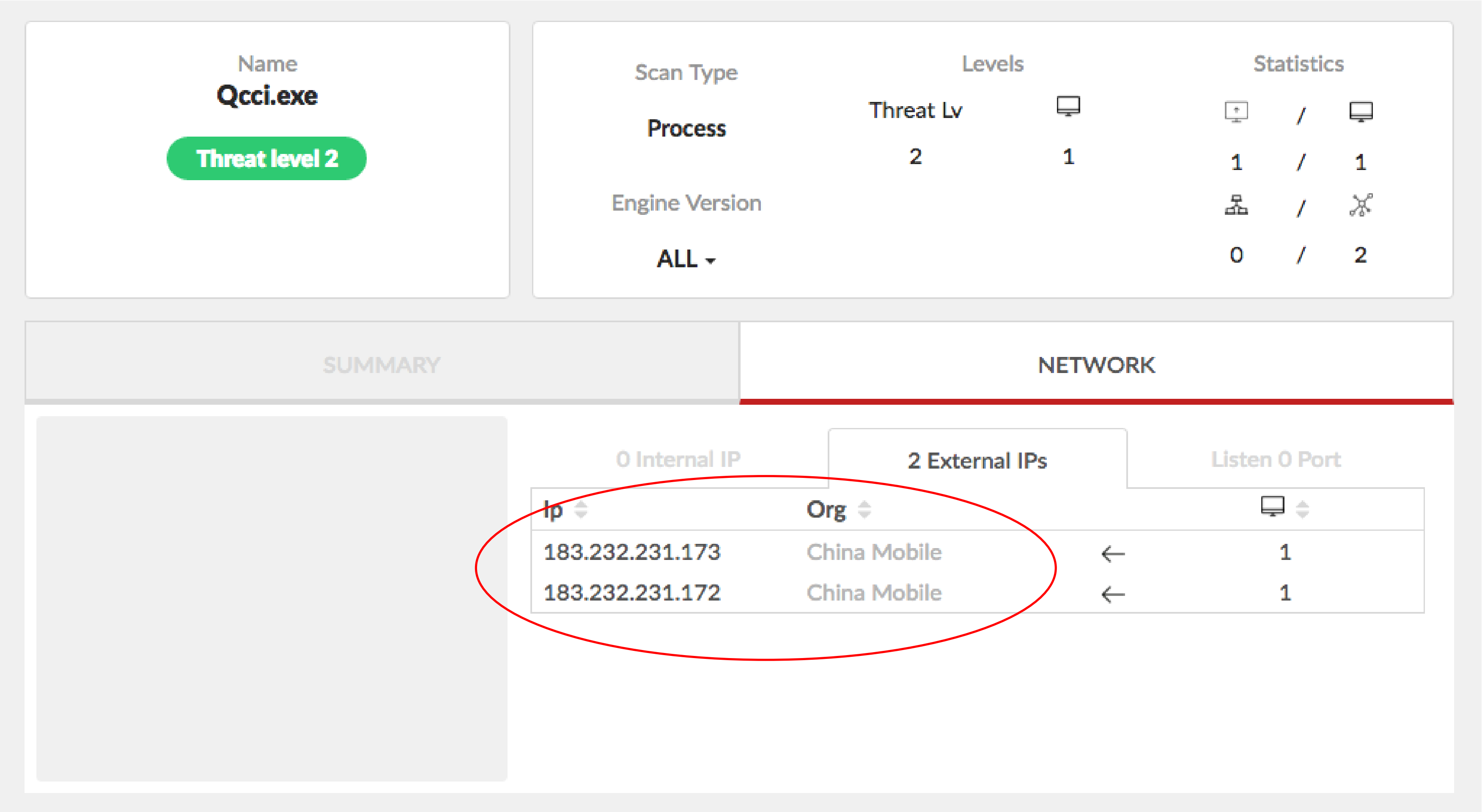
SUMMARY | NETWORK

Tag	🖥
Dir Uniq...	1
Enum Fil...	1
Manipula...	1
Parent N...	1
Checksu...	1
Network...	1
Win32	1
Co === N...	1
Signature...	1

Parent	🖥
=== Not ...	1

Rule	🖥

會連到一個特定組織的兩個IP



Name
Qcci.exe
Threat level 2

Scan Type: Process

Engine Version: ALL

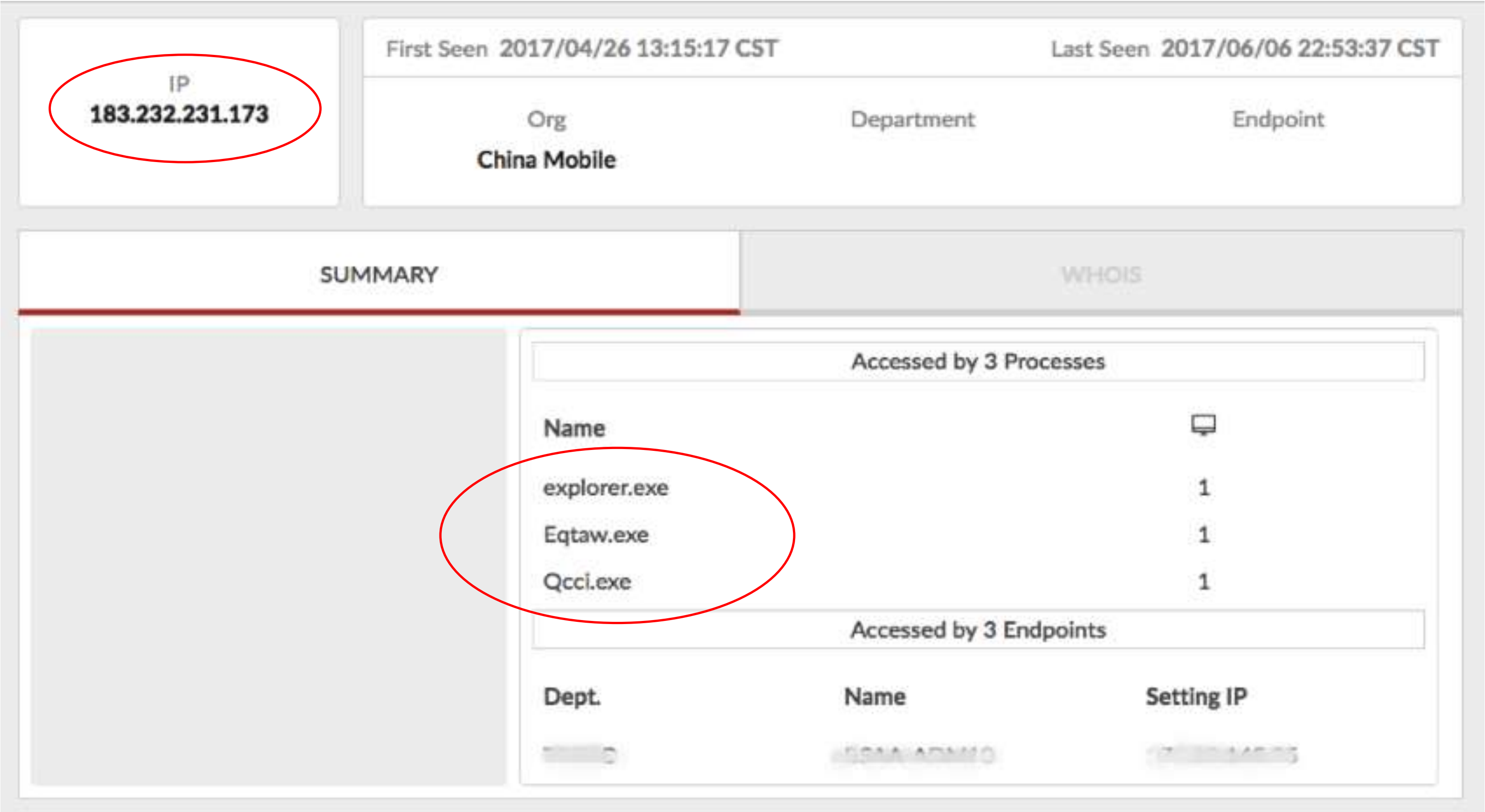
Threat Lv	🖥
2	1

Statistics: 1 / 1, 0 / 2

Ip	Org		🖥
183.232.231.173	China Mobile	←	1
183.232.231.172	China Mobile	←	1

關連IP

- 哪些主機連到這組IP
- 哪些程式連到這組IP



IP
183.232.231.173

First Seen 2017/04/26 13:15:17 CST   Last Seen 2017/06/06 22:53:37 CST

Org	Department	Endpoint
China Mobile		

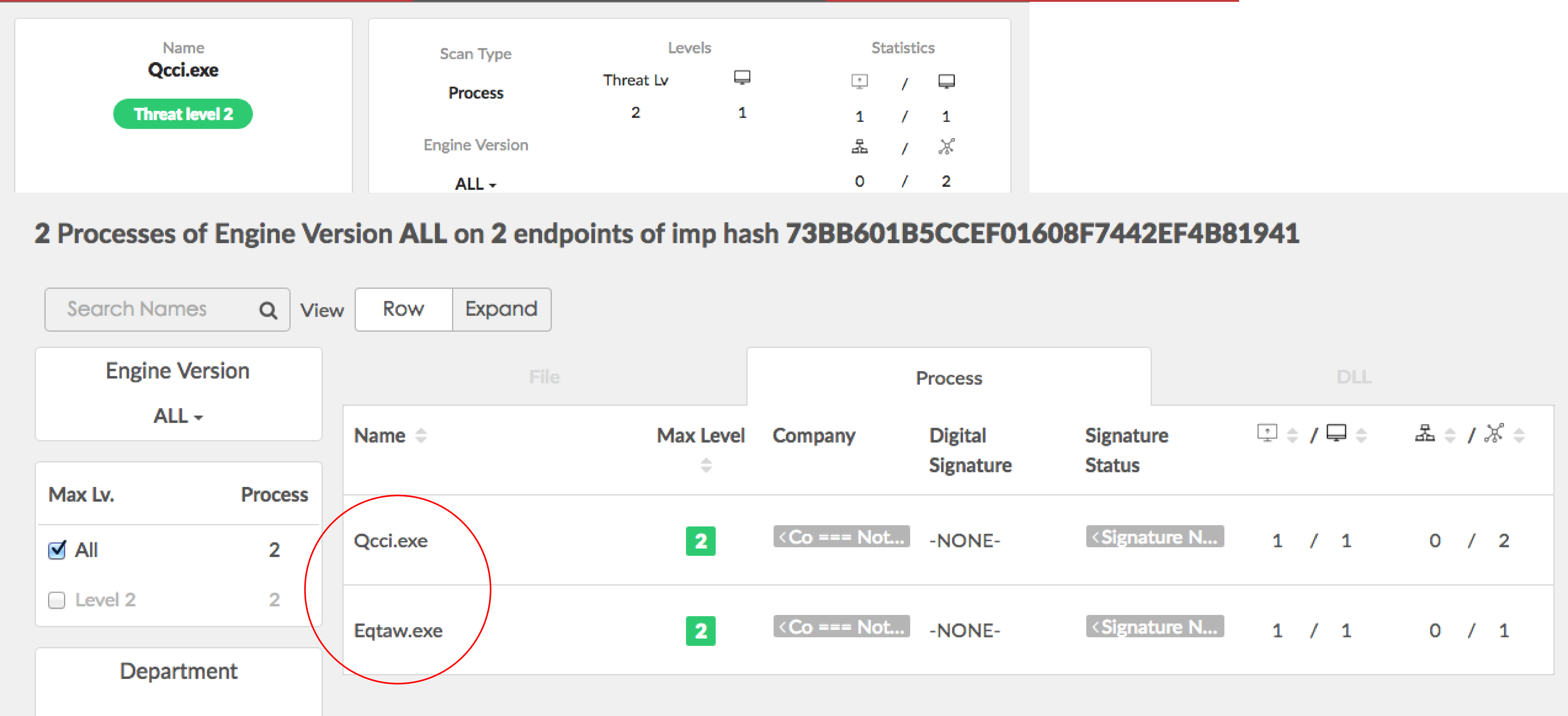
Accessed by 3 Processes

Name	🖥
explorer.exe	1
Eqtaw.exe	1
Qcci.exe	1

Accessed by 3 Endpoints

Dept.	Name	Setting IP
[redacted]	[redacted]	[redacted]

透過imphash關連是否有相似功能程式



Name
Qcci.exe
Threat level 2

Scan Type	Levels		Statistics		
Process	Threat Lv	🖥	🖥	/	🖥
	2	1	1	/	1
Engine Version			品	/	✕
ALL ▾			0	/	2

2 Processes of Engine Version ALL on 2 endpoints of imp hash 73BB601B5CCEF01608F7442EF4B81941

Engine Version
ALL ▾

Max Lv.	Process
☑ All	2
□ Level 2	2

Department

Name	Max Level	Company	Digital Signature	Signature Status	🖥 / 🖥	品 / ✕
Qcci.exe	2	‹Co === Not...	-NONE-	‹Signature N...	1 / 1	0 / 2
Eqtaw.exe	2	‹Co === Not...	-NONE-	‹Signature N...	1 / 1	0 / 1

主動式事件處理

- 要盡可能將環境中的主機相關惡意事件**一次解決**
- 只有一隻惡意程式嗎？只有一台電腦被感染嗎？
- 已知惡意程式有沒有相似功能的程式在其他主機上？
- 惡意程式連線了哪些 IP？透過哪些Process？有沒有其他的程式/主機也會連到這些 IP？

ThreatSonar

Advanced Threat Detecting Platform

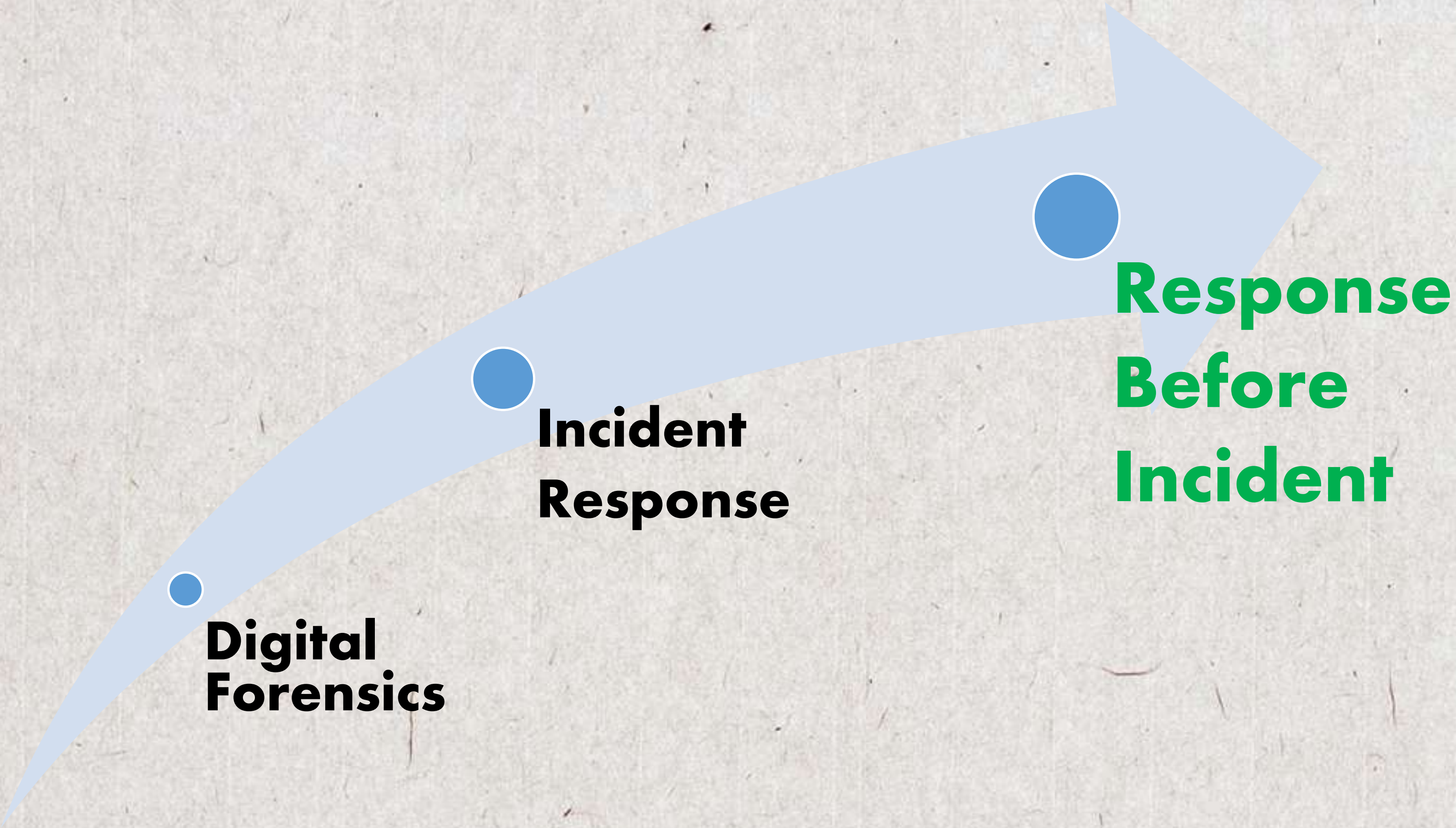
DOPPLER

Cyber Threat Solutions

TEAMT5

Cyber Security Research

慮患於未形 治亂於始發



Digital Forensics

Incident Response

Response Before Incident

制敵機先

主動式資安事件處理

杜浦數位

杜浦數位

Agenda

- Introduction
  - 流行攻擊手法 數十年來演進
  - Supply Chain Attacks 供應鏈攻擊
  - 「系統遲早會被入侵」思維
  - 資安事件處理 必須化被動為主動

- Proactive Defense How-to
  - 從視野建構 到態勢感知
  - 內部主動處理：Threat Hunting 威脅狩獵
  - 外部專家知識：Threat Intelligence 威脅情資
  - 內外兼攻防禦：Threat Fusion 威脅整合
  - 完整防禦循環、多層次威脅防禦

- Threat Hunting 心法
  - 兩種 Threat Hunting: Host, Network
  - Pivoting: 假設和證據 Ping-Pong
  - 使用威脅情資分類優先順序
  - 情資導向的 Threat Hunting Cycle
  - 如何善用內外情資 達成 Threat Fusion

- Threat Hunting 實戰案例
  - 找出異常數位簽章的程式
  - 找出異常功能屬性的程式
  - 找出異常 cmd line 的程式
  - 找出異常 IP 連線的程式

□ 歡迎對~~駭客手法~~資安有熱誠的夥伴加入我們！

□ 我們在三樓台灣資安館「威脅情資」主題區

□ 想了解我們的產品、服務，歡迎來坐☺

TEAM T5
Cyber Security Research

DOPPLER
Cyber Threat Solutions

Q & A