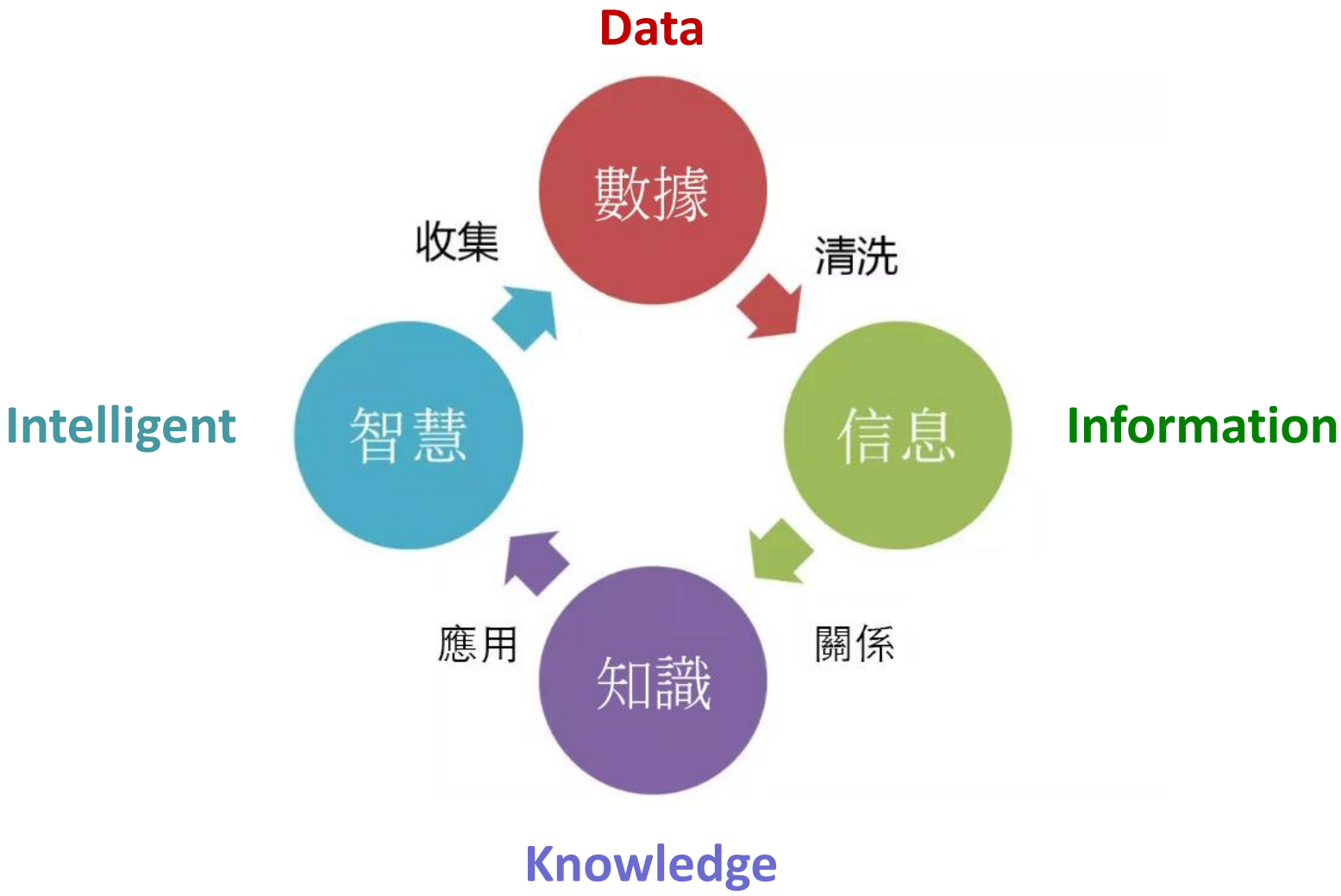
善用大數據分析技術
讓校園網路維運進入智慧化時代
與資安概論

2019/11/6 暨南大學區網中心

N-Partner
石謂龍 Robin Shih
Product Director
rshih@npartnertech.com
+886-935784086

了解這些名詞的定義與演化歷程



Beer and Diaper

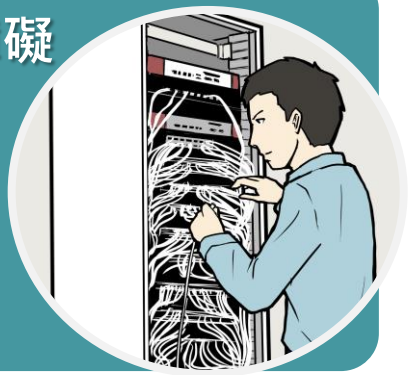
IT維運人員的工作循環

報修

蒐集Log資料

分析障礙根源

處置-消弭障礙



N-Partner

想想醫生根據數據診斷病因開立藥方的過程

收集資料 → 智慧分析 → 處置解決

N-Partner

IT維運的三大技術

- 設備健康狀態(Up/Down)
- 效能使用率(CPU/ Memory/Bandwidth)
- 資產清單

SNMP

- NetFlow/sFlow
- L3/L4 Data
- 流量使用分析
- 封包大小與Protocol監控
- 流量型DDoS分析依據
- 能了解量大量小的問題
- 可以繪製流量圖

Flow

Correlation

Auto Learning

Intelligent

Help

Syslog

安全產品,網路設備,伺服器都可以透過Syslog將事件(Event)/Audit/System Log丟出

- 事件(Event) Log記載人的使用行為
- 可以用來分析資安
- L7 (Application Layer) Data

IT Operation

Knows

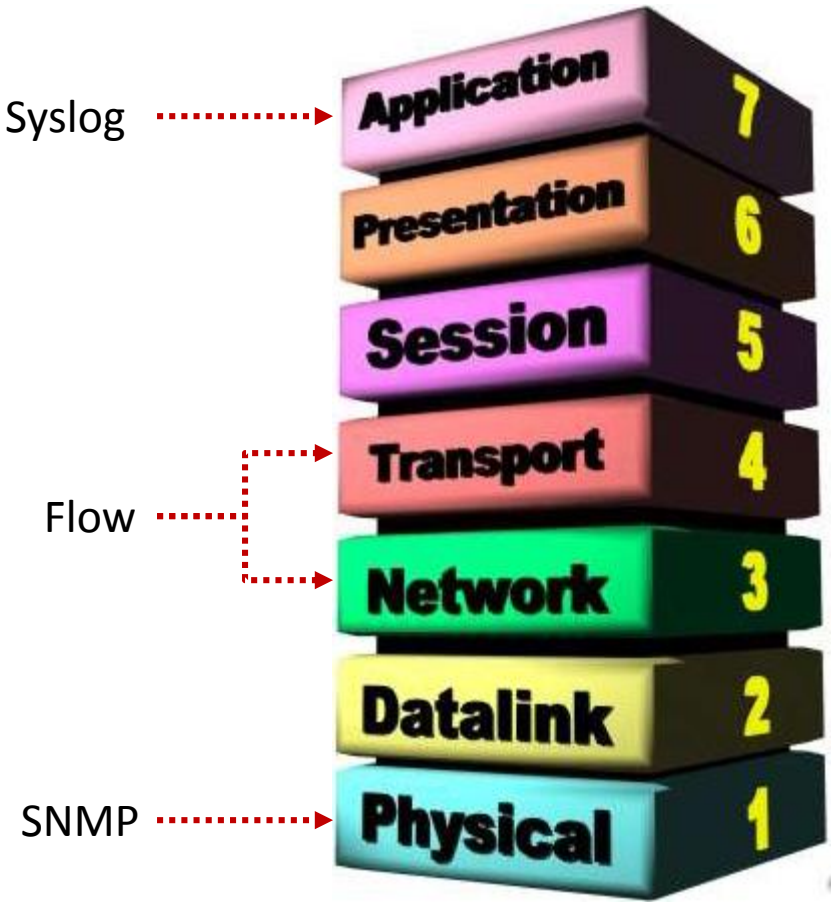
Efficiency

Control

Fix and Recover

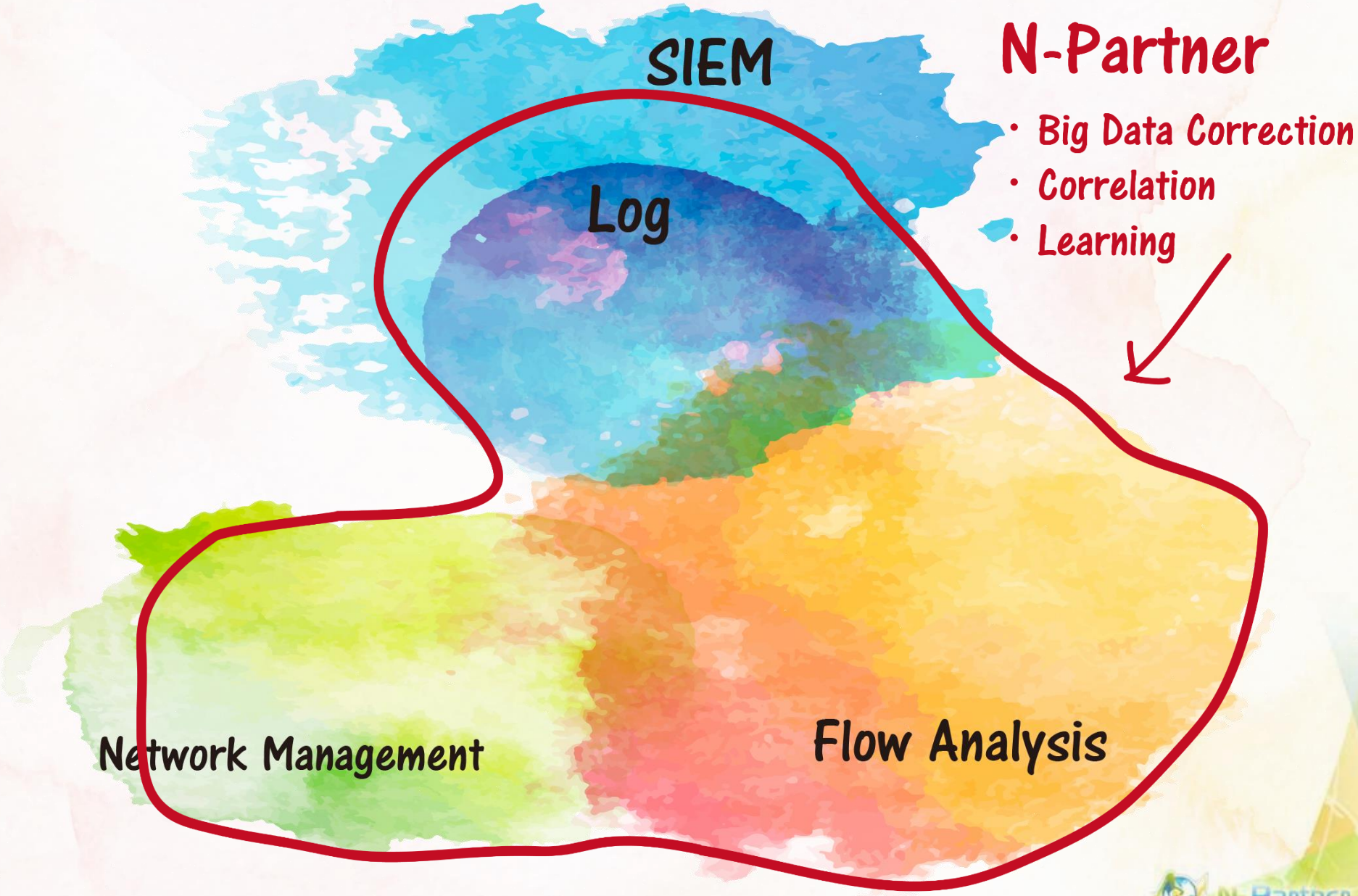
N-Partner

三大技術的OSI涵蓋領域



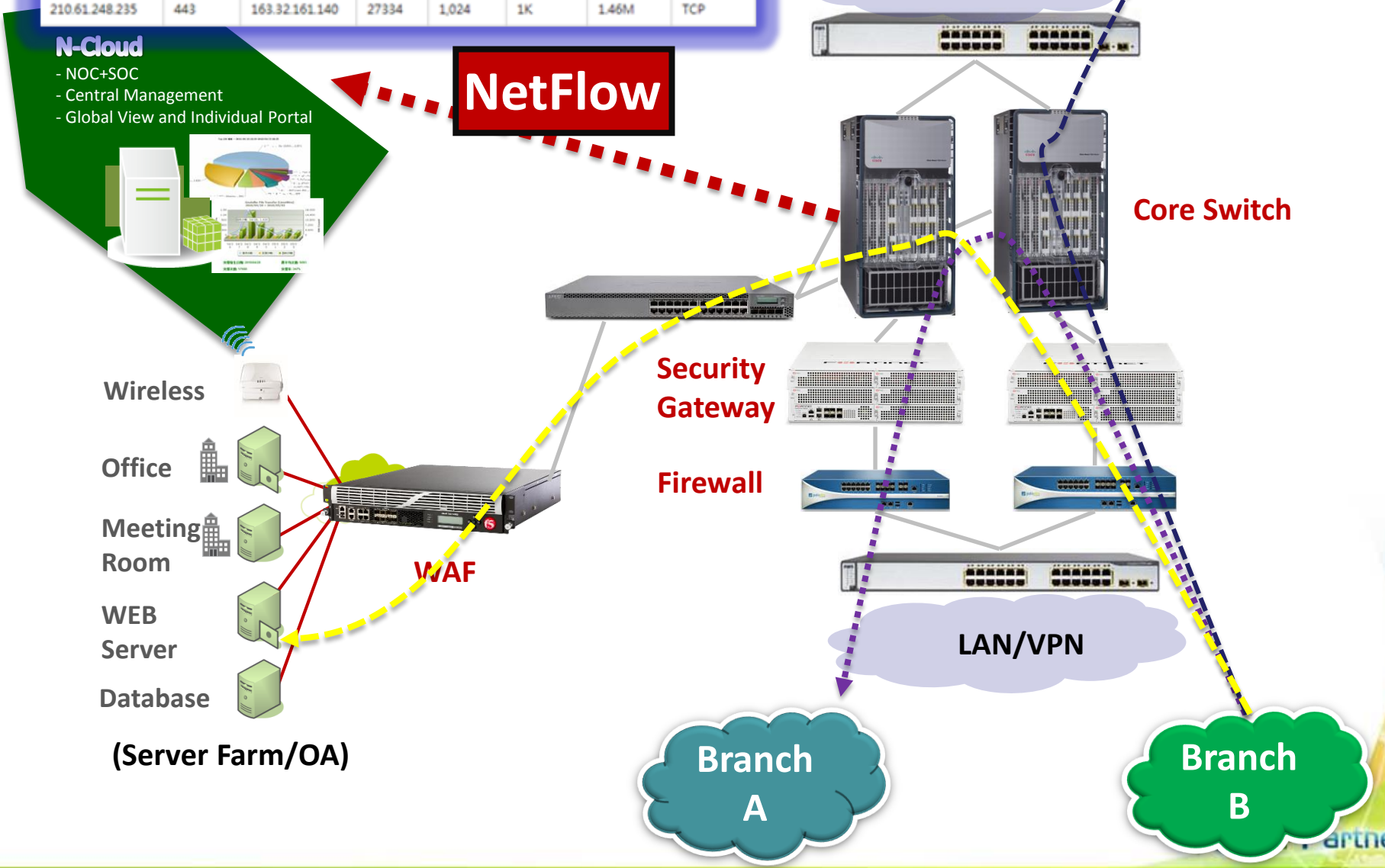
N-Partner

N-Partner Coverage

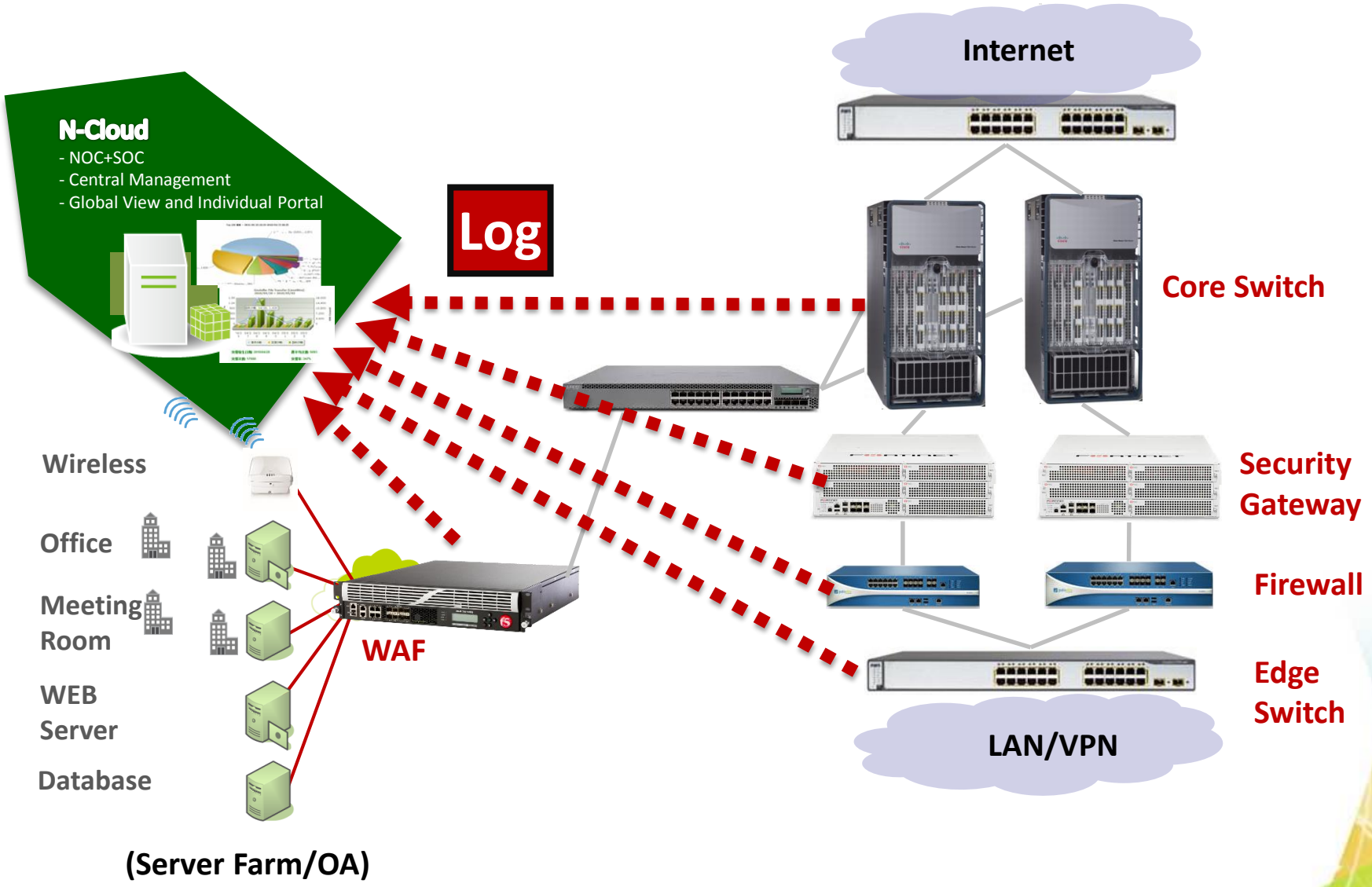


Flow(NetFlow/sFlow) data collection

Src IP	Src Port	Dst IP	Dst Port	Session	Packets	Bytes	Protocol
210.61.17.116	222	163.32.56.52	54335	1,024	1K	100K	TCP
163.28.130.14	443	163.32.78.56	1982	1,024	1K	1.41M	TCP
210.61.248.235	443	163.32.161.140	27334	1,024	1K	1.46M	TCP



Receive logs from servers/network device/security products



將各種日誌自動進行正規畫切割,才能查詢與分析

正規化前

Hostname="f5demo.bestcom.coom.tw",SlotId="0",errdefs_msgno="22282249",Entity="ACL_FORCE",AggrInterval="300",EOCTimestamp="1500459900",HitCount="1",ApplicationName="<Unassigned>",RuleName="Allow_443",ContextType="Management Port",ContextInfo="/Common/self_1",Action="Accept",VLAN="/Common/int_1",Policy="Aggregated",SourceIp="210.71.213.29",SourceIpRouteDomain="0",SourcePort="35031",DestinationIp="192.168.10.145",DestinationIpRouteDomain="0",DestinationPort="443",SaTranslationPool="Aggregated",SaTranslationType="None",SelfIp="Aggregated",SelfRouteDomain="0",ServerIp="Aggregated",ServerRemoteRouteDomain="0",SrcCountry="TW",SrcRegion="N/A",DstCountry="N/A",DstRegion="N/A",SrcUserName="Aggregated",DstUserName="No-Lookup"

正規化後

事件	來源IP	來源Port	來源名稱解析	來源區域	目的IP	目的Port	目的名稱解析
Information Leakage,HTTP Parser Attack: HTTP protocol compliance failed,Illegal method,Illegal HTTP status in response	61.60.98.238	3700		TW	74.125.31.27	80	Google
Entity="ACL_FORCE", SaTranslationType="None"	210.71.213.29	35031		TW	192.168.10.145	443	Home

目的區域	來源Port解析	目的Port解析	Audit User	目的主機名稱	路徑	參數	狀態	分類	應用服務
US					gmail-smtp-in.l.google.com		405	Network Event	HTTP
				Aggregated	/Common/self_1				Unassigned

次數	Session	Packets	Bytes	Protocol	時間	設備	事件型態	等級	Policy ID	動作
1	0	0	0	N/A	2017/07/19 22:00:59	f5 asm10.10.10.73	traffic	Critical		Permit
1	0	0	0	N/A	2017/07/19 22:00:59	F5 LTM 10.10.10.56			Allow_443	Permit

來源使用者	目的使用者	來源MAC	目的MAC	Session ID	NAT 來源IP	NAT 來源Port	NAT 目的IP	NAT 目的Port	來源IP所屬交換機/介面	目的IP所屬交換機/介

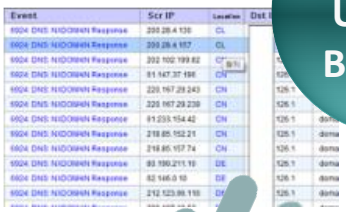
N REPORTER

智慧化維運-關聯所有訊息,節省查找時間

FW

Server/AD

Security



Event, User ID, Behavior

Geo, Reputation, AS#

Health, CPU, Interface

Event	Source IP	Destination IP	Country	Name Mapping	Packet	Byte	Username	Location
	192.168.1.222	168.95.1.1			60	4,260		
	192.168.1.33	8.8.8.8			251	203K		
	192.168.1.33	210.100.38.101			157	115K		
	192.168.2.88	210.71.213.25			19	3,822		
	192.168.2.88	121.2.15.177			4	617		

Who → Behavior → When → Where → Location

N-Partner

自動執行不同系統間的關聯性整合

Get these data from DNS

Get these data from AD

Get these data from DHCP

Query via SNMP

Event	Src IP	Src User	Source MAC	Src Host Name	SrcIP Switch/Port
nexus.officeapps.live.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CAI[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
dnl-09.geo.kaspersky.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CAI[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
content.cdn.viber.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.msftncsi.com	10.163.17.76	s[redacted]na	2C:27:D7:20:A6:40	HFO-C[redacted] hfy.local	CPF[redacted]Gi0/4, CPF1-PR...
crl.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...

全域設備一目了然

設備樹狀圖

自動更新 110

搜尋

- Global (56)
  - 中山國小 (4)
    - Tainan Juniper SRX [10.0.0.240]
    - Tainan R [10.0.0.252]
    - Tainan TP [10.0.0.251]
    - Tainan Win2k8 AD [10.0.0.2]
  - 仁愛國小 (1)
    - Bluecoat 172.16.3.171 [172.16.3.171]
  - 客庄國小 (6)
    - Flow_10.111.111.254 [10.111.111.254]
    - R 10.1.0.252 [10.1.0.252]
    - TP 10.1.0.251 [10.1.0.251]

操作	所屬領域	IP	設備名稱	設備種類	Model	資料格式	狀態	介面	建立時間	瀏覽
	中山國小	10.0.0.2	Win2k8 AD	Syslog		Windows AD (Raw)			2018/03/21 14:47	
	中山國小	10.0.0.240	Juniper SRX	Syslog		Juniper SRX			2018/03/21 14:52	
	中山國小	10.0.0.251	TP	Syslog		TippingPoi			2018/03/21 14:48	
	中山國小	10.0.0.252	R						2018/03/21	

流量圖

Device CPU (%) (SNMP)

2018/10/22 01:10 ~ 2018/10/23 01:10 (time unit: 5mins)

100 / 50 / 0 %

21:00 23. Oct

點擊查看流量

09:00 12:00 15:00 18:00 21:00 23. Oct

pps (Flow)

01:10 ~ 2018/10/23 01:10 (time unit: 5mins)

09:00 12:00 15:00 18:00 21:00 23. Oct

關閉

Top 100 Byte

2018/10/22 11:20 ~ 201

流量爆量來源

other, 49.77%

2, 3.92%
3, 3.78%
4, 3.75%
5, 2.66%
6, 2.19%
7, 2.06%
8, 1.93%
9, 1.83%
10, 1.60%

Top 100 Session

2018/10/22 11:20 ~ 2018/10/22 11:24

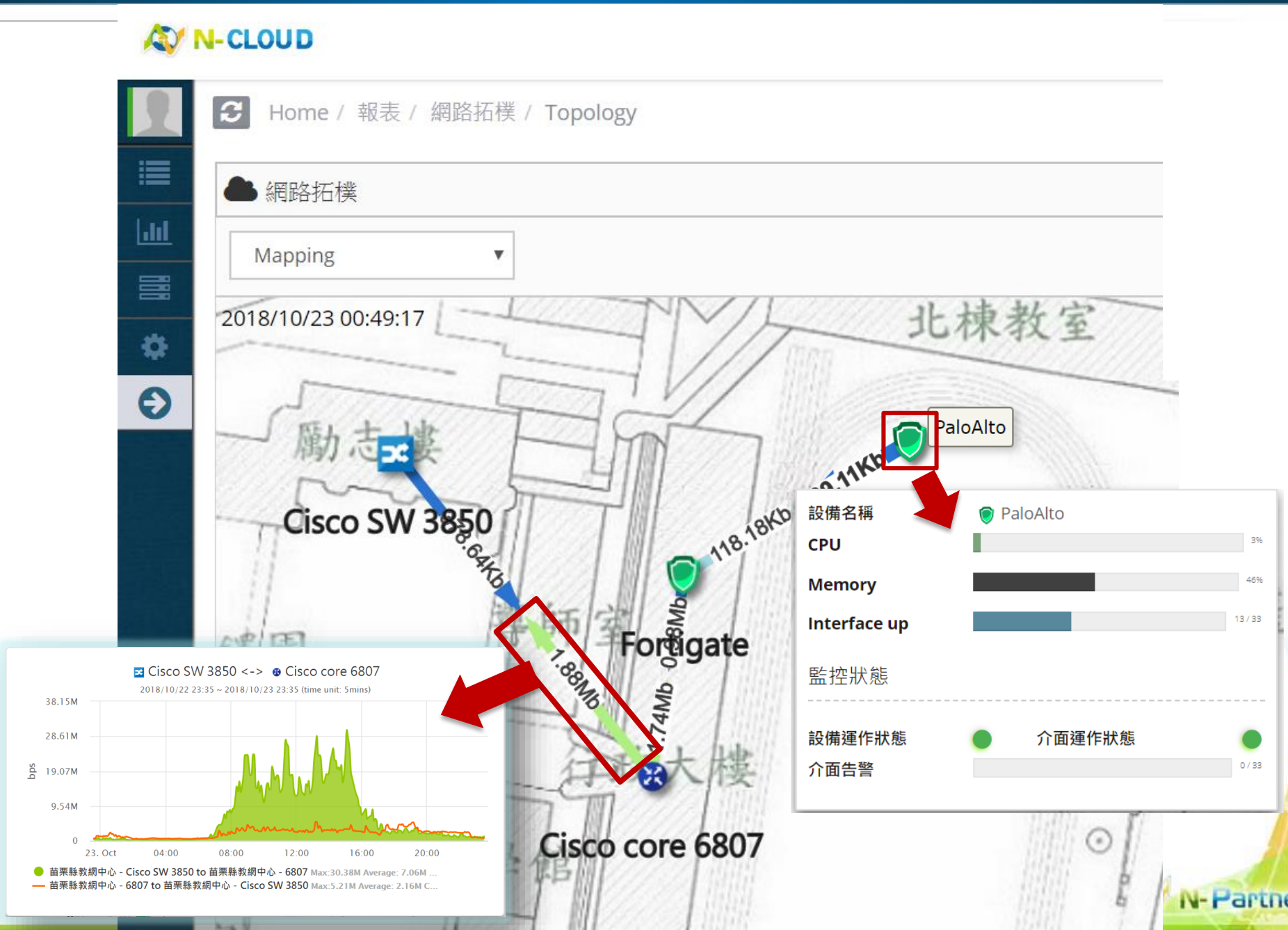
1, 0.94%
2, 0.00%
3, 0.02%
4, 0.01%
5, 0.07%
6, 0.00%
7, 0.01%
8, 0.15%
9, 0.18%
10, 0.06%

other, 98.56%

NO	來源 IP	Hit Count	Sessions	Packets	Bytes	流量圖
1	13.107.4.50	0	3.16K	17.96M	26.05G	
2	163.19.209.149	0	13	2.81M	[illegible]	
3	23.53.65.123	0	56	2.56M	3.71G	
4	163.28.224.230	0	32	2.58M	3.69G	
5	192.229.232.240	0	251	1.78M	2.61G	

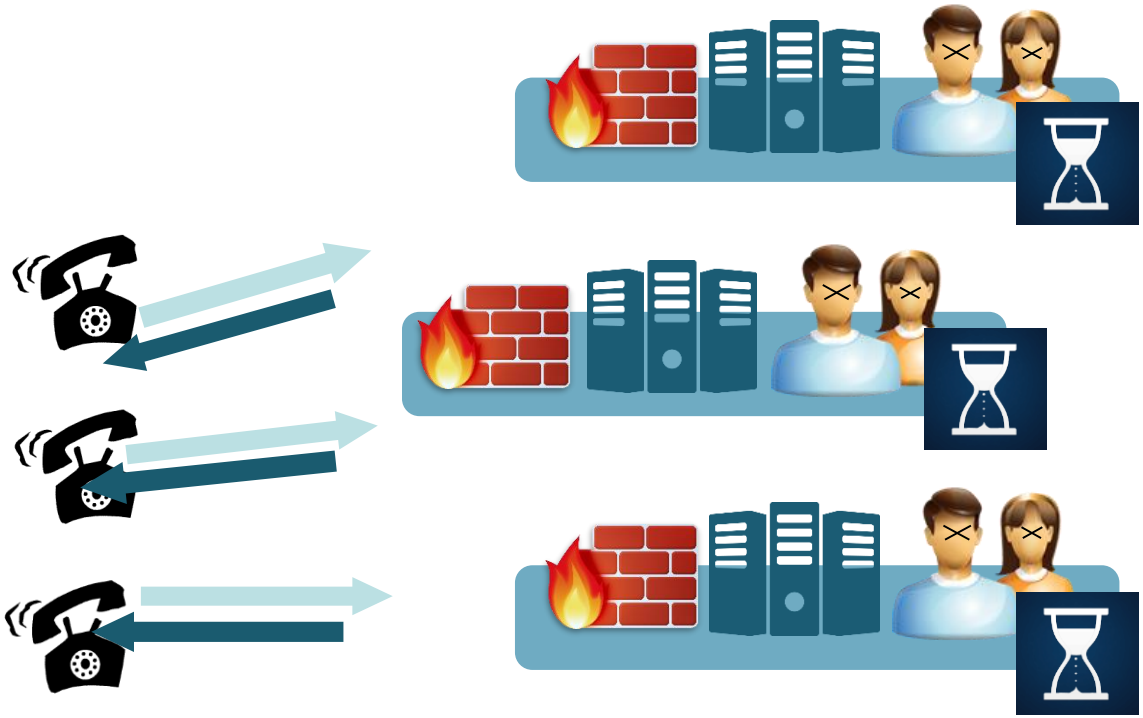
N-Partner

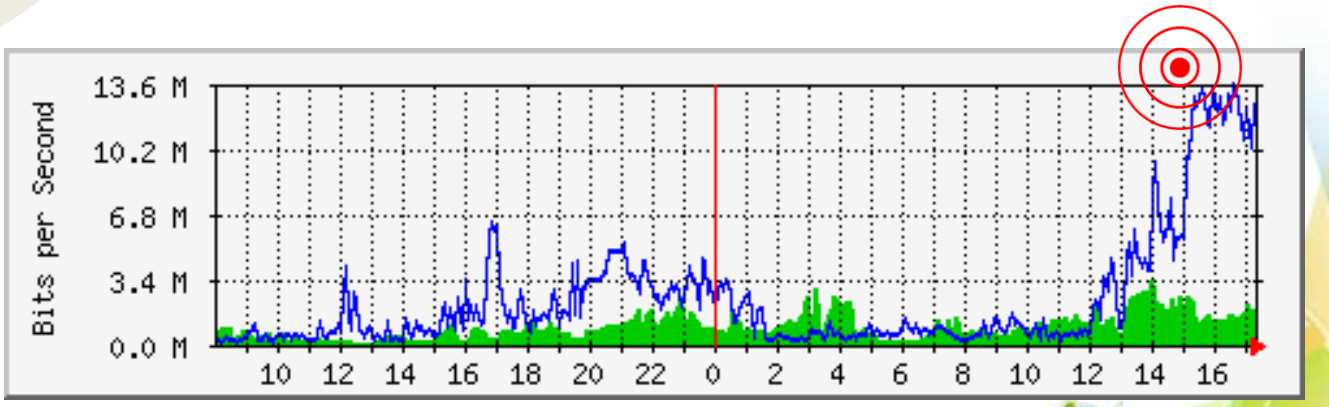
網路拓樸再進化



N-Partner

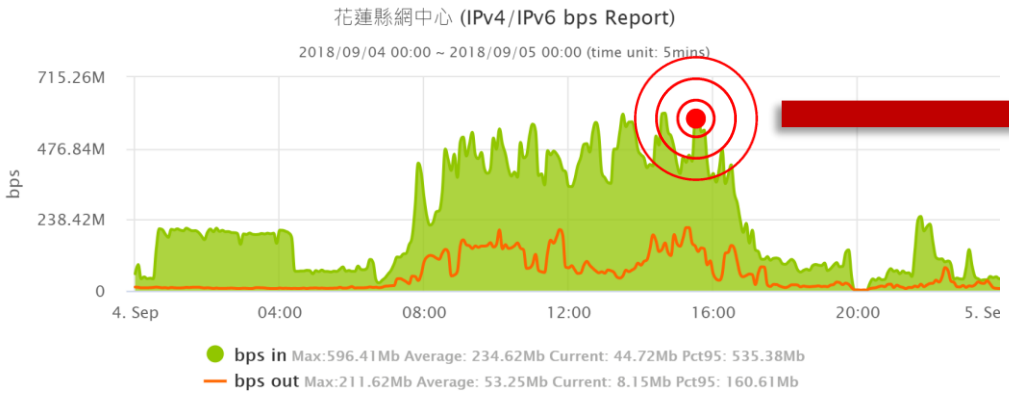
傳統用SNMP技術繪製的MRTG無法除錯

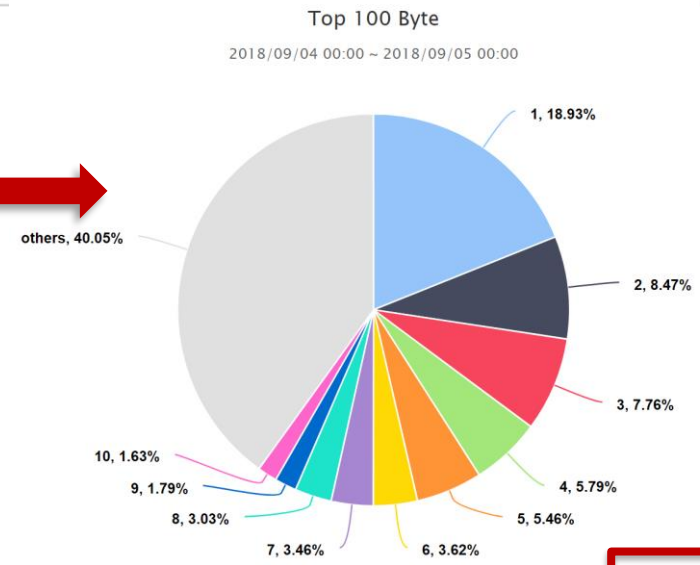




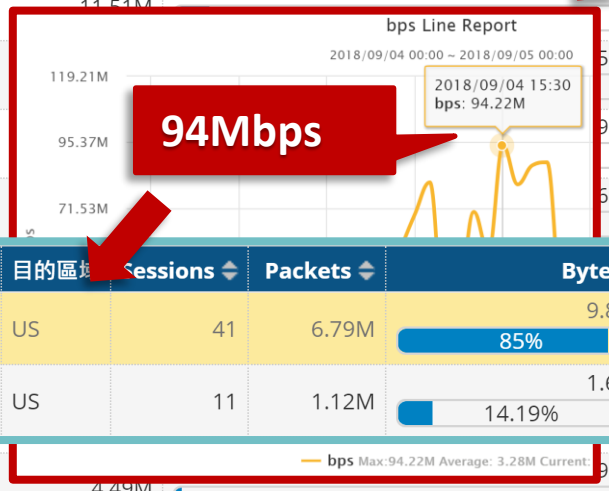
N-Partner

揮別MRTG-頻寬資源佔據分析,掌握異常用量





NO	來源 IP 名稱解析	Sessions	Packets	Bytes	流量圖
1	太昌國小	161.48K	28.89M	34.64G 18.93%	
2	新城國中	132.75K	14.15M	15.49G 8.47%	
3	壽豐國小	96.13K	11.51M	1[illegible]0G	
4	北昌國小	140.63K	[illegible]	[illegible]58G	
5	春日國小	162.25K	[illegible]	[illegible]99G	
6	豐濱國小	80.16K	[illegible]	[illegible]63G	
10	志學國小	393.37K	4.49M	[illegible]98G 1.63%	

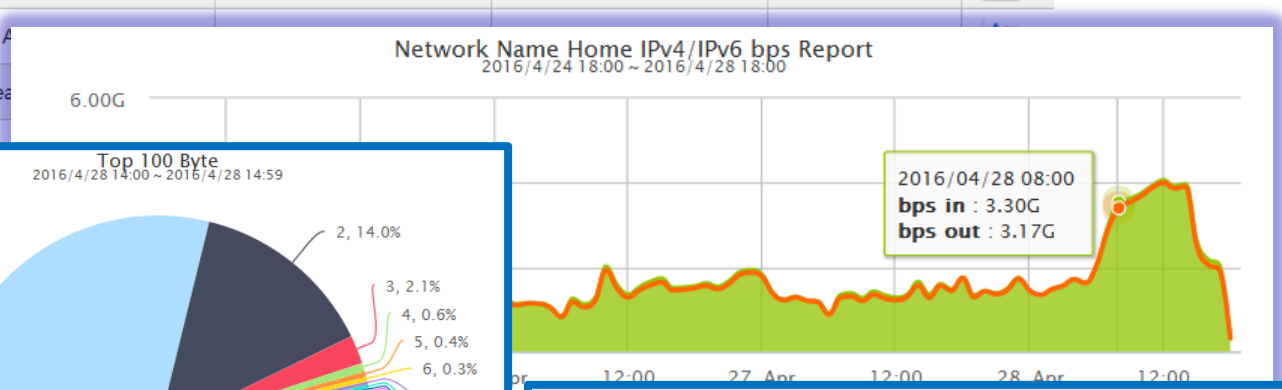


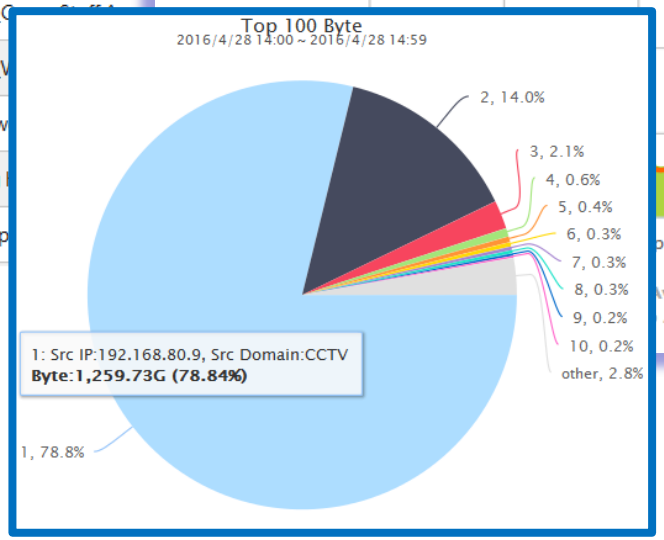
NO	來源 IP	目的 IP	目的 Port	目的 IP 名稱解析	目的區域	Sessions	Packets	Bytes
1	10.100.157.26	172.217.24.10	TCP:443	Google	US	41	6.79M	9.86G 85%
2	10.100.157.26	172.217.160.106	TCP:443	Google	US	11	1.12M	1.65G 14.19%

CCTV佔據內網傳輸頻寬

Total Number: 122

Network Name	Volume of traffic in			
	Sessions	Packets	Bytes	
Home	2.75G	19.81G	19,546.44G	
Iraq_Camp_Manager Office Area	69.29K	1.03M	937.36M	
Iraq_Camp Manager A				
Iraq_Camp Office Area				
Iraq_C				
Iraq_V				
Huaw				
Qing				
Camp				

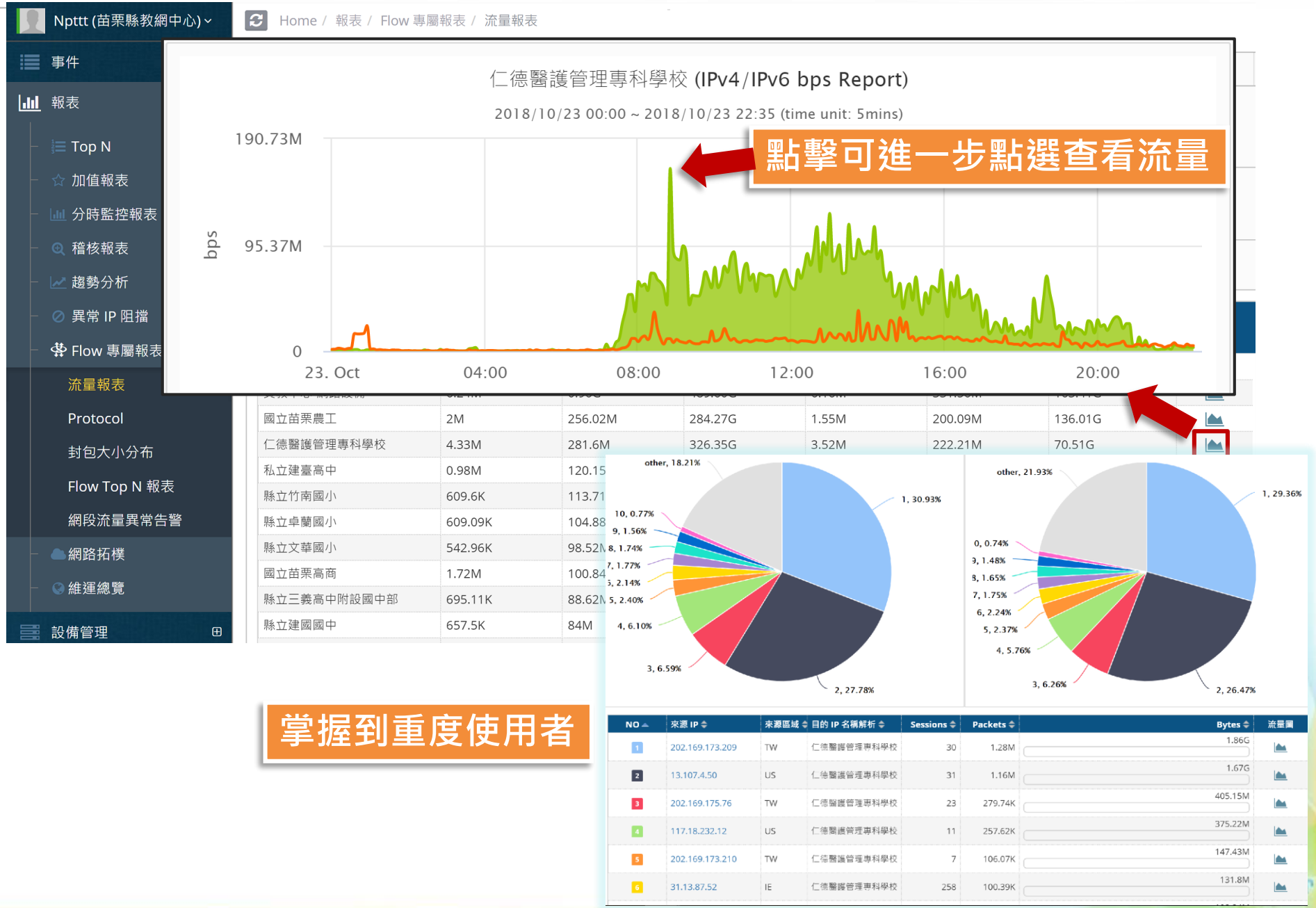




NO.	Src IP	Src Domain	Sessions	Packets	Bytes
1	192.168.80.9	CCTV	99.03M	926.37M	1,259.73G
2	10.163.176.48	Iraq_OCC_Server Virtualization System	1.53K	154.07M	223.48G
3	10.163.177.248	OCC Phase II Server Virtualization	1.14M	24.47M	34.24G
4	10.163.15.154	Iraq_OCC_Mail Server	550.11K	7.55M	10.15G

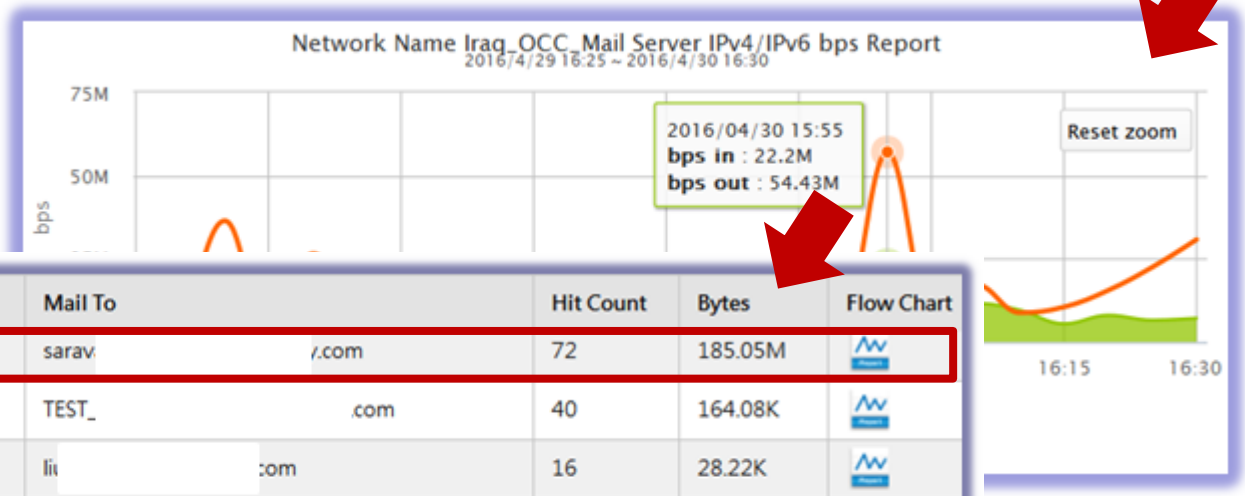
N-Partner

改用Flow繪製可以清楚掌握各單位的網路流量



自動學習的案例- 異常巨量郵件寄送即時告警

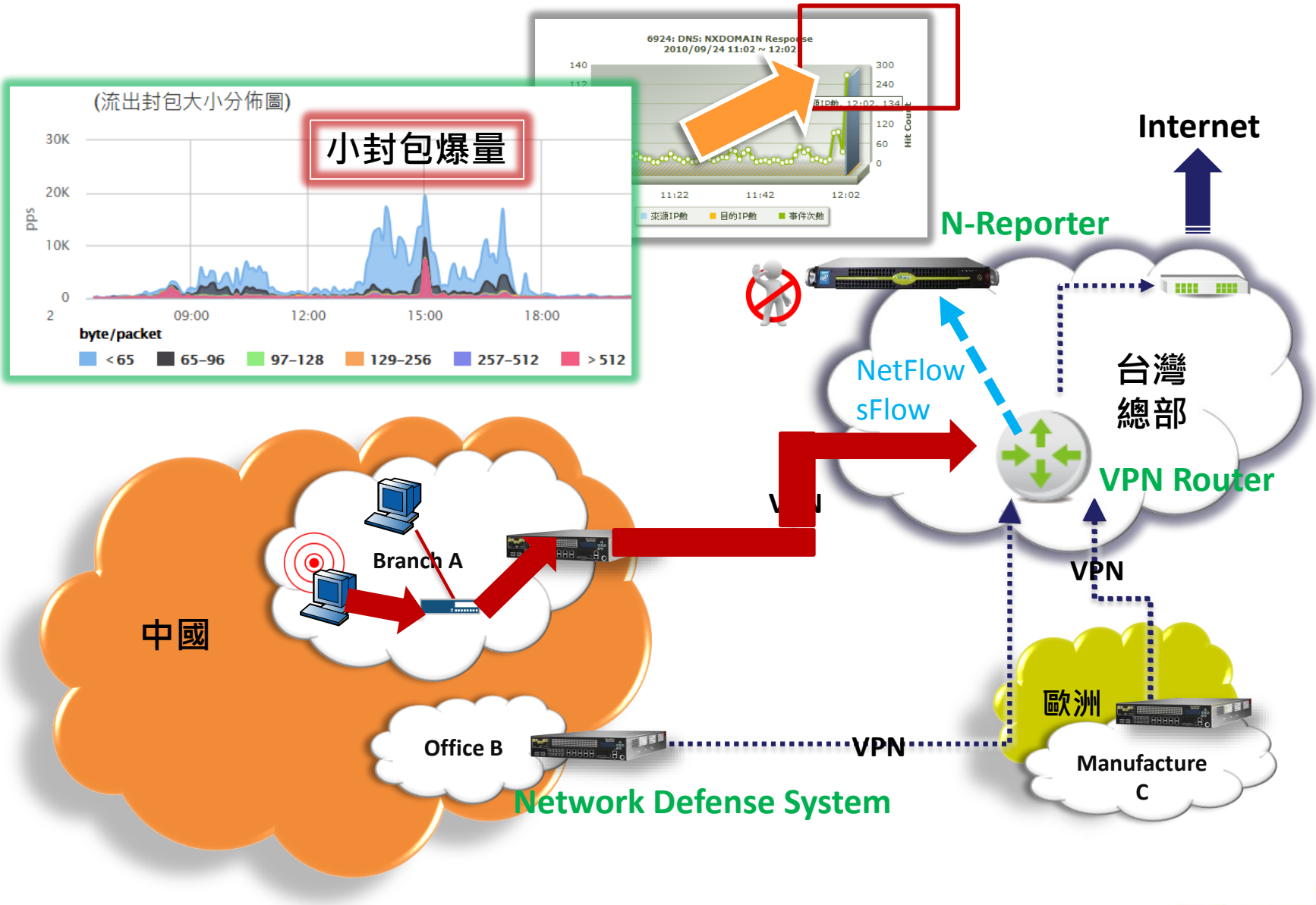
Mapping Name	Volume of traffic in			Volume of traffic out			Alert Time	Flow C
	Session/sec	pps	bps	Session/sec	pps	bps		
in_Controller	206.07	5.28K	3.59M	207.36	7.15K	77.93M	2016/04/30 15:55:00	
Mail Server	1.38K	5.64K	22.2M	1.92K	5.42K	54.43M	2016/04/30 15:55:00	
I_DNS Server	28.39	4.67K	2.22M	19.15	6.39K	73.34M	2016/04/30 15:55:00	
ouse Office Area	7.39							
fireless	0.35							
office area	18.92							
Wireless System Guest	1.38K							
Office Network System	25.22K							
Room308	3.65							



NO.	Mail From	Mail To	Hit Count	Bytes	Flow Chart
2	mai com	sarav .com	72	185.05M	
3	mo .com	TEST_ .com	40	164.08K	
4	liuli com	li com	16	28.22K	
5	gac om	g .com	16	39.13K	
6	hait fy.com	A y.com	12	182.01M	
7	fc.d y.com	jc com	10	93.83K	
8	selv om	s .com	10	2.35M	
9	joh .com	mus .com	8	1.88M	
10	ps_ .com	tri .com	8	8.33M	

N-Partner

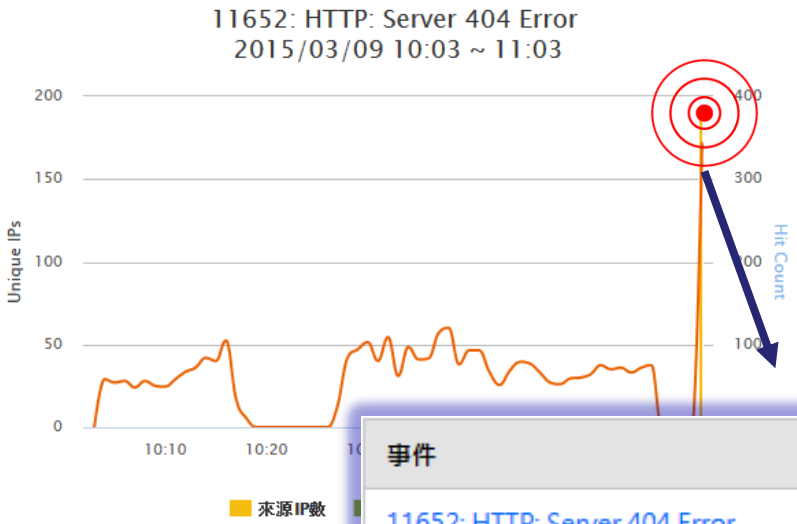
自我療癒VPN網路運作流程



封包大小異常分析- 掌握服務遭受攻擊的細節

事件	來源IP	來源Port	來源區域	目的IP	目的Port	目的IP名稱解析	次數
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	4885	CN	223.	443	旅行社	85
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	4885	CN	223.	443	旅行社	79
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	4706	CN 中華人民共和國		443	旅行社	36
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	4706	CN	223.	443	旅行社	36
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5003	CN	223.	443	旅行社	11
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5003	CN	223.	443	旅行社	11
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5221	CN	223.	443	旅行社	3
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5221	CN	223.	443	旅行社	3
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5112	CN	223.	443	旅行社	2
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5112	CN	223.	443	旅行社	2

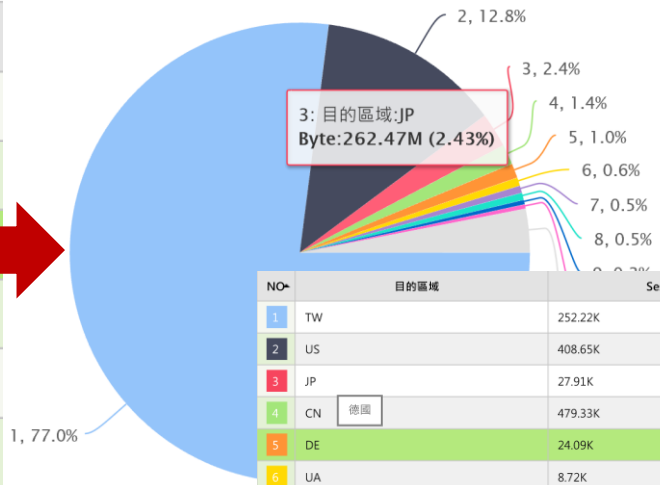
3/9 11:03- 出現爆量Server 404 Error



事件	來源IP	來源區域	目的IP	目的IP名稱解析	次數
11652: HTTP: Server 404 Error	61.220.141.217	TW	223.26.68.83	五福旅行社	291
11652: HTTP: Server 404 Error	118.163.159.210	TW	223.26.68.83	五福旅行社	112
11652: HTTP: Server 404 Error	118.163.240.108	TW	223.26.68.83	五福旅行社	38
11652: HTTP: Server 404 Error	220.132.130.176	TW	223.26.68.27	五福旅行社	35
11652: HTTP: Server 404 Error	114.33.36.179	TW	223.26.68.83	五福旅行社	31
11652: HTTP: Server 404 Error	122.116.208.32	TW	223.26.68.83	五福旅行社	31
11652: HTTP: Server 404 Error	61.220.141.217	TW	223.26.68.27	五福旅行社	26
11652: HTTP: Server 404 Error	61.222.59.107	TW	223.26.68.83	五福旅行社	26
11652: HTTP: Server 404 Error	61.220.141.217	TW	223.26.68.38	五福旅行社	24
11652: HTTP: Server 404 Error	125.227.123.223	TW	223.26.68.83	五福旅行社	23

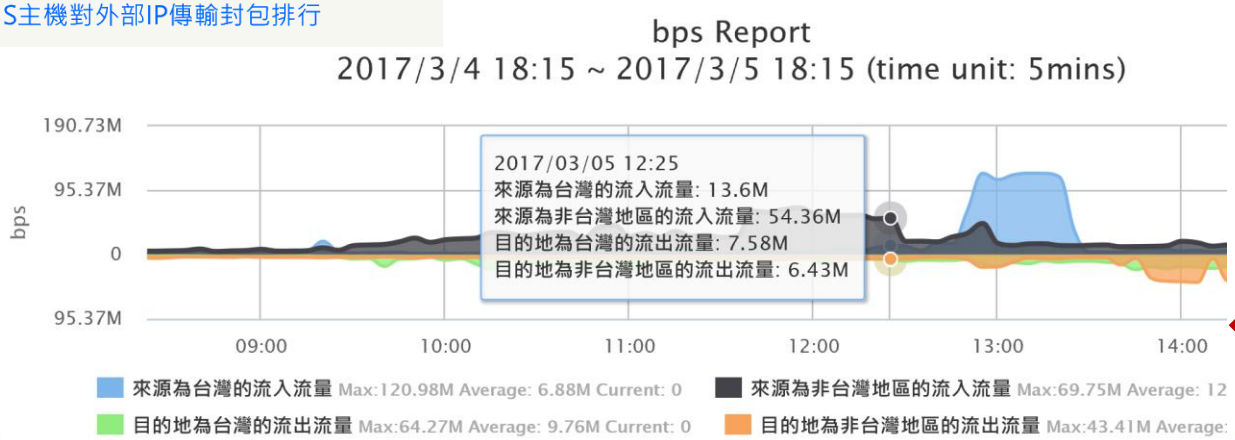
根據國家流量排行與非臺灣流量時圖

報表名稱
防火牆阻擋事件報表
流出流量排行By組織單位
流出流量排行By國家
流入流量排行By組織單位
流入流量排行By國家
外部連線至內部服務Port盤點
外部IP對內部重要服務流量排行
內部連外部流量排行
內部流出大量封包排行by IP
來自中國大陸的流量排行
DNS主機對外部IP傳輸封包排行



NO.	目的區域	Sessions	Packets	Bytes	
1	TW	252.22K	7.08M	77.01%	8.13G
2	US	408.65K	1.76M	12.83%	1.35G
3	JP	27.91K	232.53K	2.43%	262.47M
4	CN 德國	479.33K	773.47K	1.42%	153.24M
5	DE	24.09K	101.69K	1.03%	111M
6	UA	8.72K	51.14K	0.59%	63.55M
7	NL	21.01K	58.87K	0.51%	55.04M
8	FR	16.03K	49.77K	0.5%	54.37M

報表名稱
DNS流量監控
RDP流量監控
SSH流量監控
http與https流量監控
來自外部查詢DNS流量監控
台灣與非台灣流量監控



N-Partner

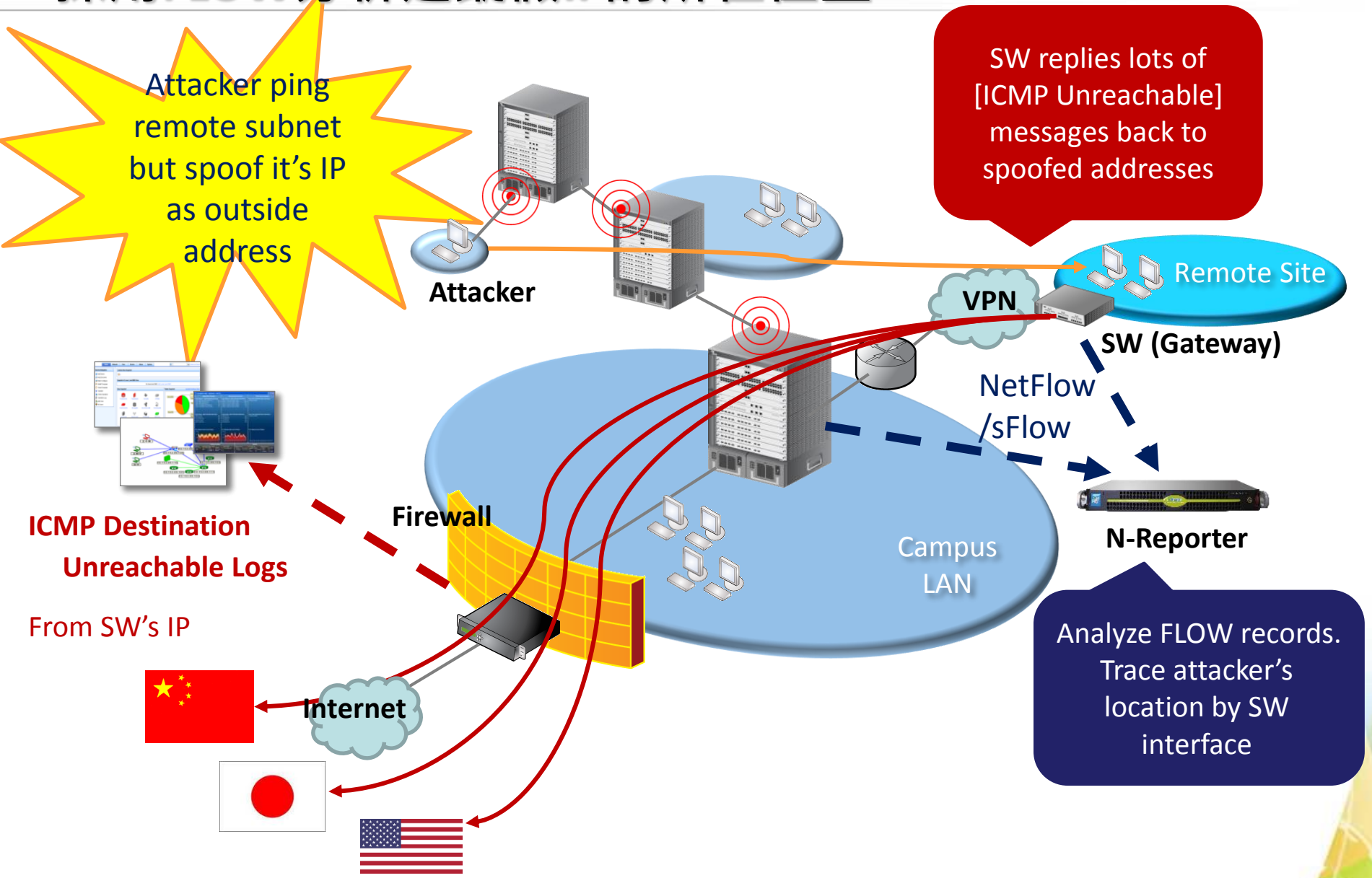
知名服務流量分時圖

直接在圖形上點擊可以查詢知名服務的詳細內容,能夠充分瞭解網路資源被使用的情況

時間	來源IP	來源IP名稱解析	來源區域	來源Port解析	目的IP	Session	Packets	Bytes
2017/03/07 09:04:59	2404:6800:4008:c03::64	Google	AU	https	8:84be:1:cd49:b54	1,024	1K	1.37M
2017/03/07 09:04:59	74.125.10.137	Google	US	https	141.1	1,024	1K	1.44M
2017/03/07 09:04:59	2607:f8b0:4017:26::b	Google	US	https	8:8268:4:3df0:4aa	1,024	1K	1.37M
2017/03/07 09:04:59	172.217.27.142	Google	US	https	20.198	1,024	1K	1.44M
2017/03/07 09:04:59	172.217.24.10	Google	US	https	3.3.87	1,024	1K	1.44M
2017/03/07 09:04:59	172.217.24.1	Google	US	https	25.144	1,024	1K	1.44M
2017/03/07 09:04:59	216.58.200.238	Google	US	https	74.111	1,024	1K	1.35M
2017/03/07 09:04:59	216.58.200.238	Google	US	https	85.195	1,024	1K	1.35M
2017/03/07 09:04:59	2404:6800:4008:c06::65	Google	AU	https	8:84c4:2:10cb:436	1,024	1K	81K

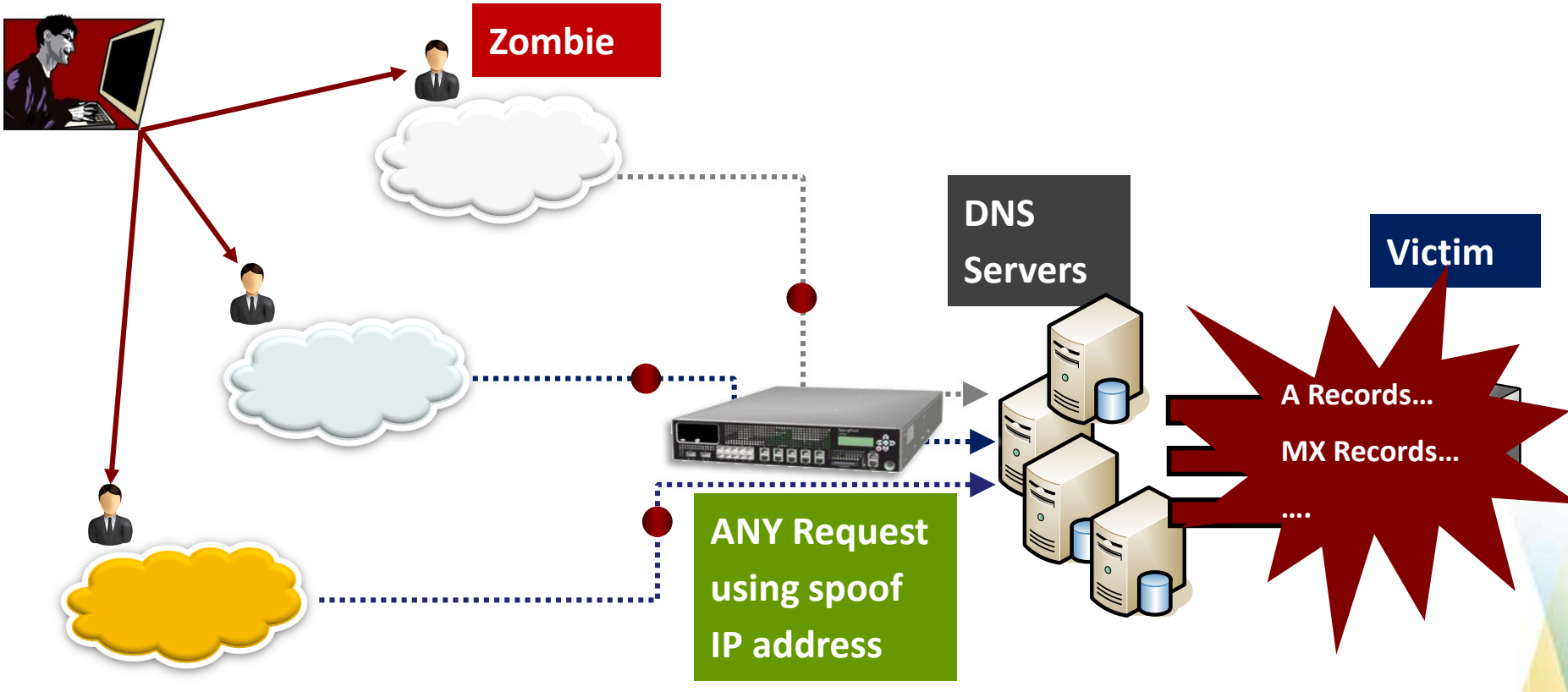
N-Partner

採用FLOW分析追蹤假IP的所在位置

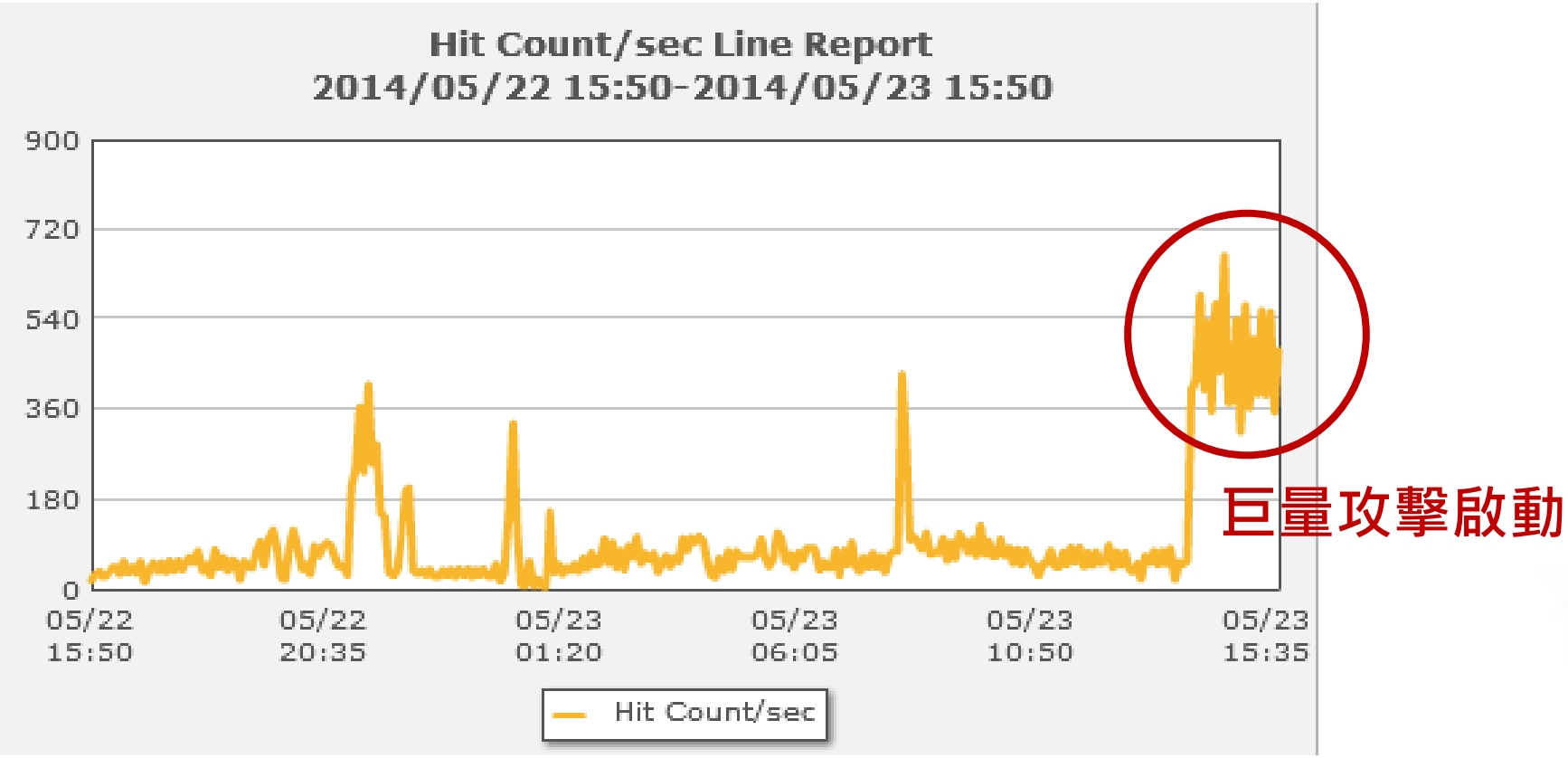


DNS Amplify – 可以放大28-40倍數的流量

- *主要目的- 消耗頻寬資源*



DNS Amplify攻擊案例



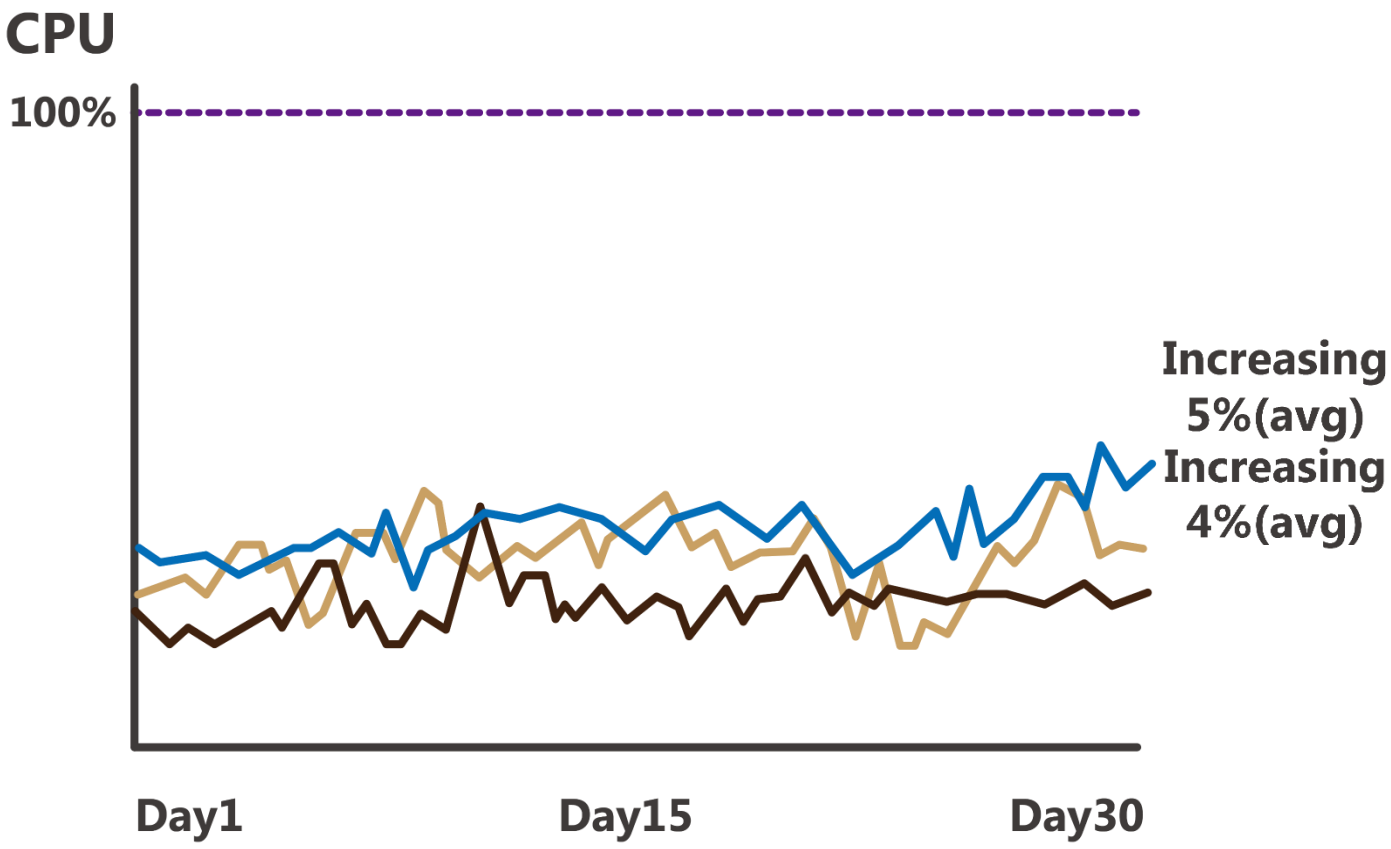
DNS Amplify TOP 10攻擊來源案例

這些並不是用戶的IP地址- 駭客使用IP偽造 (Spoofed IP address)-通常這些IP是駭客意圖要灌流量的IP

NO.	事件	來源IP	來源區域	目的IP	目的區域	Hit Count
1	13019: DNS: DNS ANY Response	21.38	TW	92.201	TW	773.46K
2	13019: DNS: DNS ANY Response	94.123.247.2	TR	92.190	TW	397.11K
3	13019: DNS: DNS ANY Response	245.116	TW	92.201	TW	353.73K
4	13019: DNS: DNS ANY Response	72.200.121.163	US	92.201	TW	299.8K
5	13019: DNS: DNS ANY Response	4.203	TW	92.201	TW	181.84K
6	13019: DNS: DNS ANY Response	8.161	TW	92.201	TW	169.3K
7	13019: DNS: DNS ANY Response	31.244	TW	92.201	TW	155K
8	13019: DNS: DNS ANY Response	244.111	TW	92.201	TW	141.08K
9	13019: DNS: DNS ANY Response	4.181	TW	92.201	TW	134.99K
10	13019: DNS: DNS ANY Response	87.210.50.215	NL	92.192	TW	134.23K

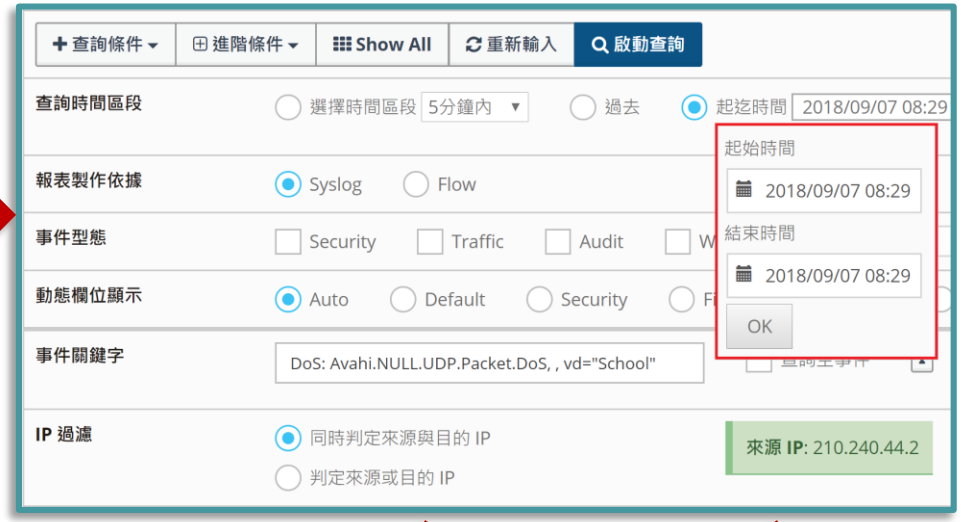
N-Partner

運用人工智慧-圖形比對出細微差異變化



N-Partner

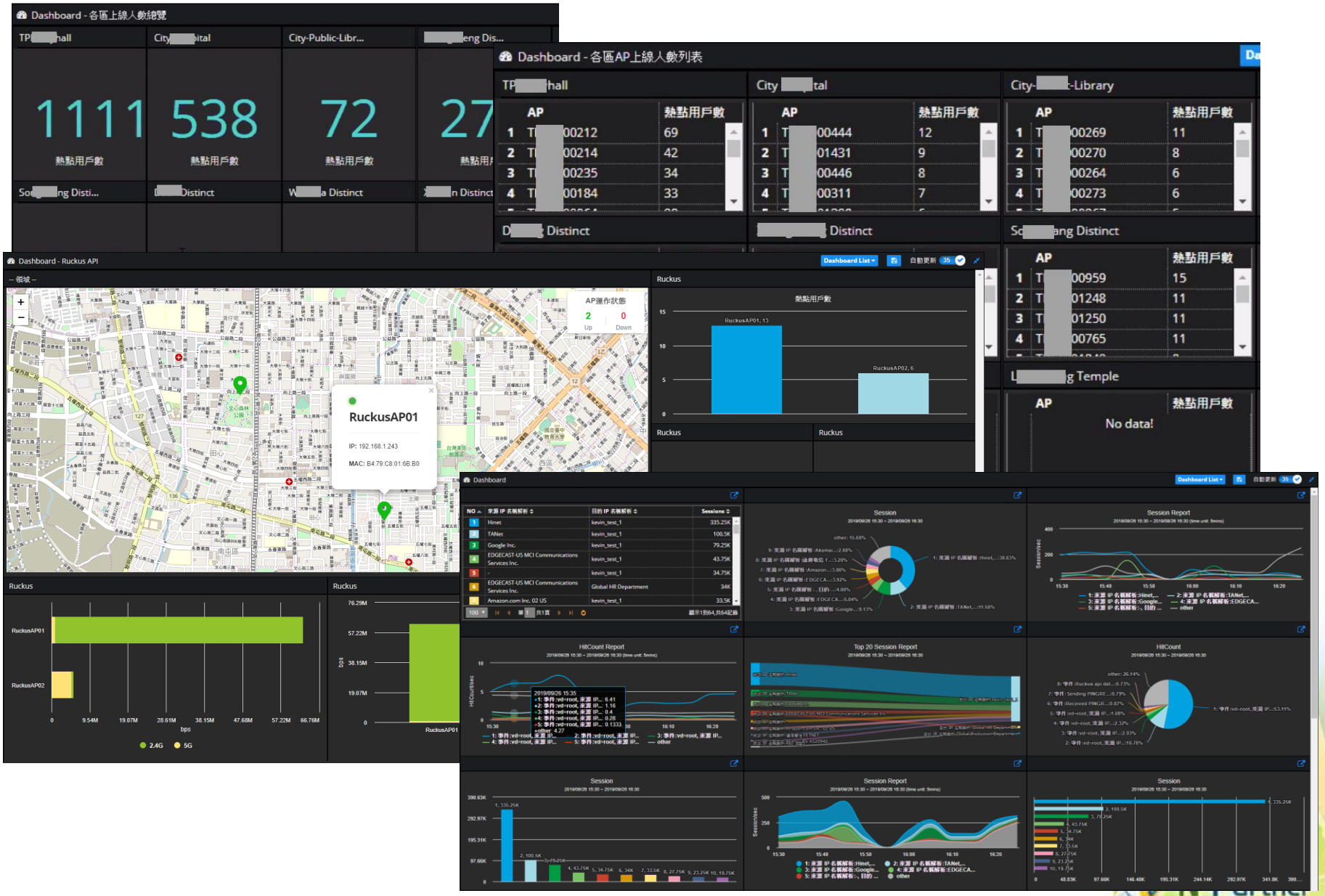
智慧校園維運-根據教育部資安通報,查找內部IP與位置



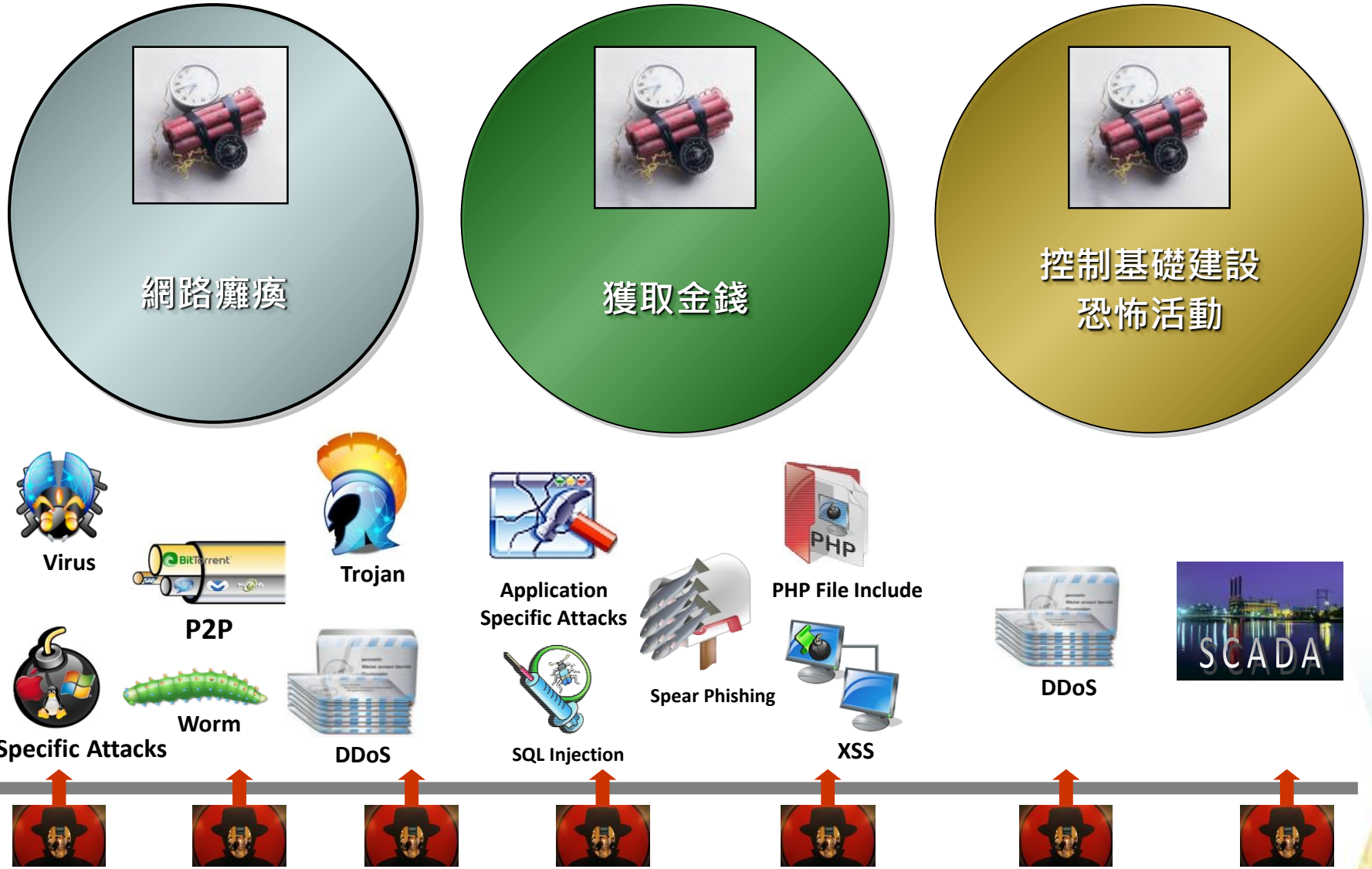
事件行為	來源 IP	目的 IP	學校	時間	NAT內部IP	使用者	所在位置
DNS: hacker.com	210.240.44.2	168.95.1.1	中正	3/9 15:02	192.168.1.33	王曉明	教室1-GE1/0/1
HTTPS: Google Gmail Access	210.240.44.2	8.8.8.8	中正	3/9 15:05	192.168.1.33	王曉明	教室1-GE1/0/1
BitTorrent: Peer-to-Peer Communications	210.240.44.2	210.100.38.101	中正	3/9 15:11	192.168.1.33	王曉明	教室1-GE1/0/1
MS-RPC: Microsoft Server Service Buffer Overflow	210.240.44.2	210.71.213.25	中正	3/9 15:14	192.168.1.33	王曉明	教室1-GE1/0/1
	210.240.44.2	121.2.15.177	中正	3/9 15:15	192.168.1.33	王曉明	教室1-GE1/0/1

N-Partner

維運用監控Dashboard



攻擊分類與目的



N-Partner

大敵當前

Original Motion Picture Soundtrack
ENEMY AT THE GATES
Music Composed and Conducted by
JAMES HORNER

俄羅斯駭客發動網軍癱瘓愛沙尼亞政府網路

許多來自台灣的電腦參予了這次的攻擊

InfoWorld

Back to article Print this

Russian gov't not behind Estonia DDOS attacks

Analysis throws doubt on whether a single agency alone was involved

By Jeremy Kirk, IDG News Service

June 01, 2007

From alleged poisonings to organized crime, Russia has been getting a lot of bad press lately. But this time the country -- or at least, the government -- may be in the clear.

The string of crippling DDOS (distributed denial-of-service) attacks against Estonia didn't appear to be a coordinated attack by one entit ssia, wrote Jose Nazario, senior security engineer with Arbor Networks, in a commentary.

Estonia, a former satellite of the Soviet Union with a population of 1.3 million, came under inte mmercial and government Web sites. The attacks came as Estonia moved a World War II memorial of a statue of a Soviet

Although Russia was quickly accused, Russian g re suspicions than facts.

But further analysis throws do io wrote.

While it is possible to spoof the to Tallin," Estonia's capital, Nazario wrote.

While the Russian government r ussian-speaking computer gurus may have joined in.

Several Russian-language Web f allow others to rig their computers to join in a DDOS attack, which involves sending massive streams of data to a Web site, causing it to crash. omputer to send data to a Web site.

"We see signs of Russian nationalism at work here, but no Russian government connection," Nazario wrote.

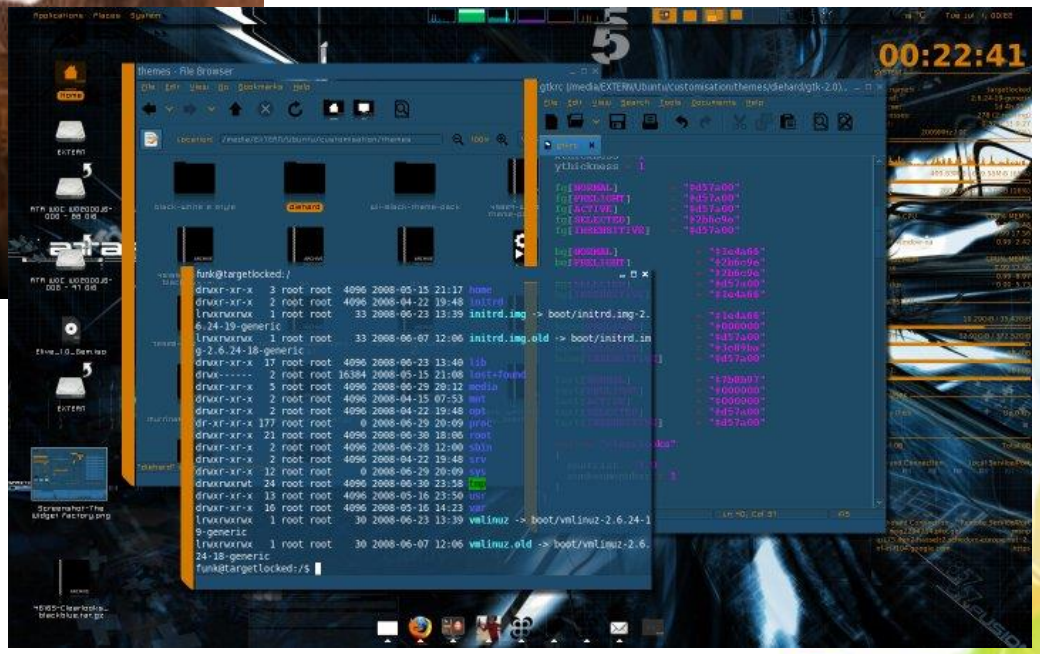
This week has been fairly quiet, said Hillar Aarelaid, chief security officer for Estonia's Computer Emergency Response Team.

"We have seen some attacks, but they are quite easy to handle," Aarelaid said, adding the DDOS attacks remain under investigation.

"Estonia... came under intense electronic attacks on April 27, jamming up commercial and government Web sites. – DDOS Attacks"

Critical Infrastructure Attacks

終極警探4 -描述駭客透過網路控制交通設施等基礎建設



公路電子看板遭駭客入侵--前有活屍

速報>> MLB／吉拉迪承受重返榮耀壓力　洋基球迷：沒冠軍就下台 (12:47)

國際新聞

轉寄新聞　友善列印　我要投稿　字級：大 中 小

前面有活屍？　美國交通電子看板經常被駭客惡搞(2009/02/05 16:08)

德州奧斯汀市一條公路旁邊的電子看板上寫著：「小心！前面有活屍」。(圖／美聯社)

記者朱錦華／綜合報導

美國公路的交通電子看板經常遭到駭客惡搞，例如他們會把「前面有落石」竄改成「前面有活屍」（zombies），或「前面有迅猛龍」等。公路安全單位非但一點也不覺得有趣，反而覺得不勝其擾。

最近的一次惡搞，周二(3日)發生在伊利諾州柯林維爾附近的255號州際公路。一面電子看板出現了：「活屍出現，前面道路封閉」的字樣。

類似的惡作劇還出現在印第安納波里斯、德州的奧斯汀等地。

伊利諾州的通輸主管部門位非常擔心，這種惡作劇會對用路人造成困擾或分心，釀成意外。在伊利諾州，惡整交通電子看板，最高可罰250美元。

殭屍電腦(Botnet)的用途

- Botnet是有組織性的犯罪工具,主要用途包括:
  - 發送垃圾郵件
  - 執行網路釣魚誘騙
  - 增加廣告點閱次數(click fraud)
  - 發動DDoS攻擊

- **要防止DDoS,企圖用異常流量演算來阻擋是不得已的下策:**
  - 異常流量演算一定有時間上的延誤與誤差值問題
  - 做好漏洞防護工作,避免電腦成為Botnet
  - 對IRC管控

任何人都可以輕鬆租Botnet

- Home
- Price
- Stats
- Sign Up

Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив

Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет палености , если файл палится более чем 30% из тестируемых 11 антивирусов , то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

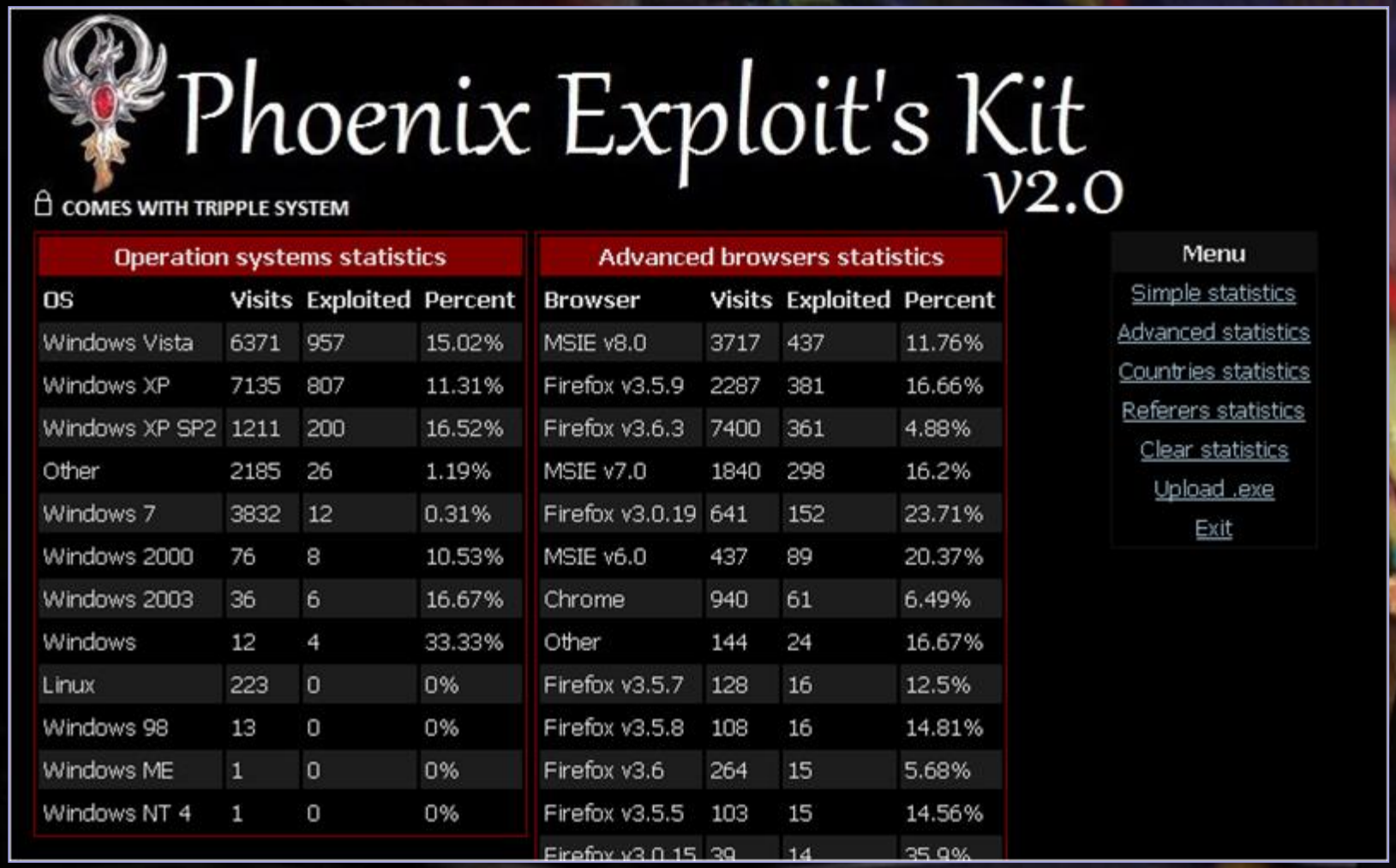
Октябрь 16/2007
Налетай не скупись покупай ж иеоЙЙсь] а точнее микс и юсу

Август 30/2007

Цены

Country	Price for 1k	
AU	300$	Order now
DE	220$	Order now
GB	210$	Order now
IT	200$	Order now
NZ	200$	Order now
ES	200$	Order now
US	110$	Order now
BG	100$	Order now
DK	100$	Order now
FR	100$	Order now
PT	100$	Order now
NL	100$	Order now
CA	80$	Order now
JP	80$	Order now
SE	70$	Order now
BR	60$	Order now
TR	60$	Order now
NO	50$	Order now

Effectiveness of Exploit Toolkits



Phoenix Exploit's Kit v2.0

COMES WITH TRIPPLE SYSTEM

Operation systems statistics

OS	Visits	Exploited	Percent
Windows Vista	6371	957	15.02%
Windows XP	7135	807	11.31%
Windows XP SP2	1211	200	16.52%
Other	2185	26	1.19%
Windows 7	3832	12	0.31%
Windows 2000	76	8	10.53%
Windows 2003	36	6	16.67%
Windows	12	4	33.33%
Linux	223	0	0%
Windows 98	13	0	0%
Windows ME	1	0	0%
Windows NT 4	1	0	0%

Advanced browsers statistics

Browser	Visits	Exploited	Percent
MSIE v8.0	3717	437	11.76%
Firefox v3.5.9	2287	381	16.66%
Firefox v3.6.3	7400	361	4.88%
MSIE v7.0	1840	298	16.2%
Firefox v3.0.19	641	152	23.71%
MSIE v6.0	437	89	20.37%
Chrome	940	61	6.49%
Other	144	24	16.67%
Firefox v3.5.7	128	16	12.5%
Firefox v3.5.8	108	16	14.81%
Firefox v3.6	264	15	5.68%
Firefox v3.5.5	103	15	14.56%
Firefox v3.0.15	39	14	35.9%

Menu

Simple statistics
Advanced statistics
Countries statistics
Referers statistics
Clear statistics
Upload .exe
Exit

Botnet活動-- Real Case

Czech Republic

Multiple inside devices communicate with a malicious IP in midnight

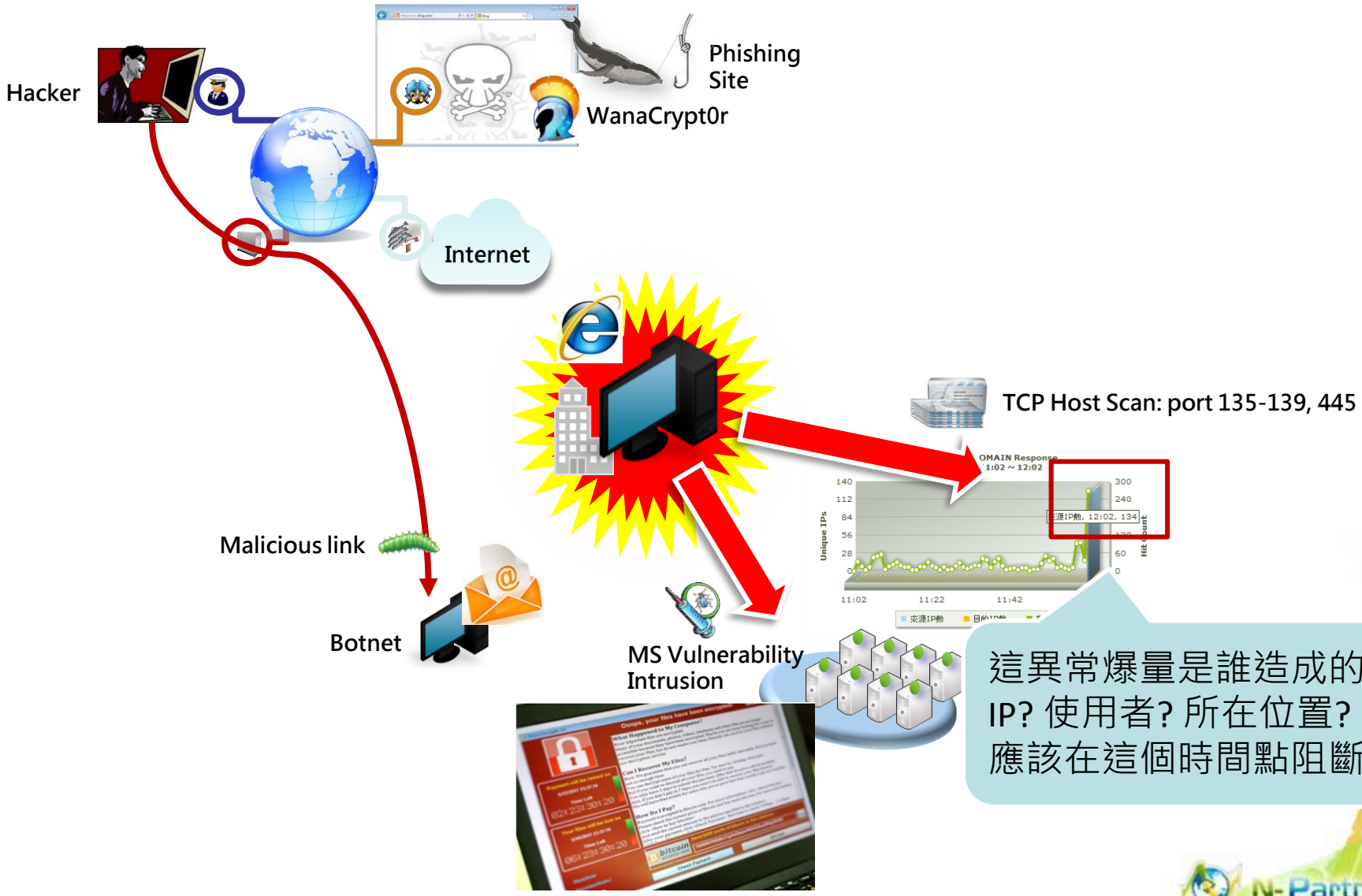
事件	來源IP	目的IP	目的Port	目的區域	次數	時間
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:59:31
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:58:35
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:58:25
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:57:21
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	捷克共和國	1	2013/04/03 00:57:11
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:56:19
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:55:59
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:55:09
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:54:49
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:53:55

勒索軟體(Ransomware)

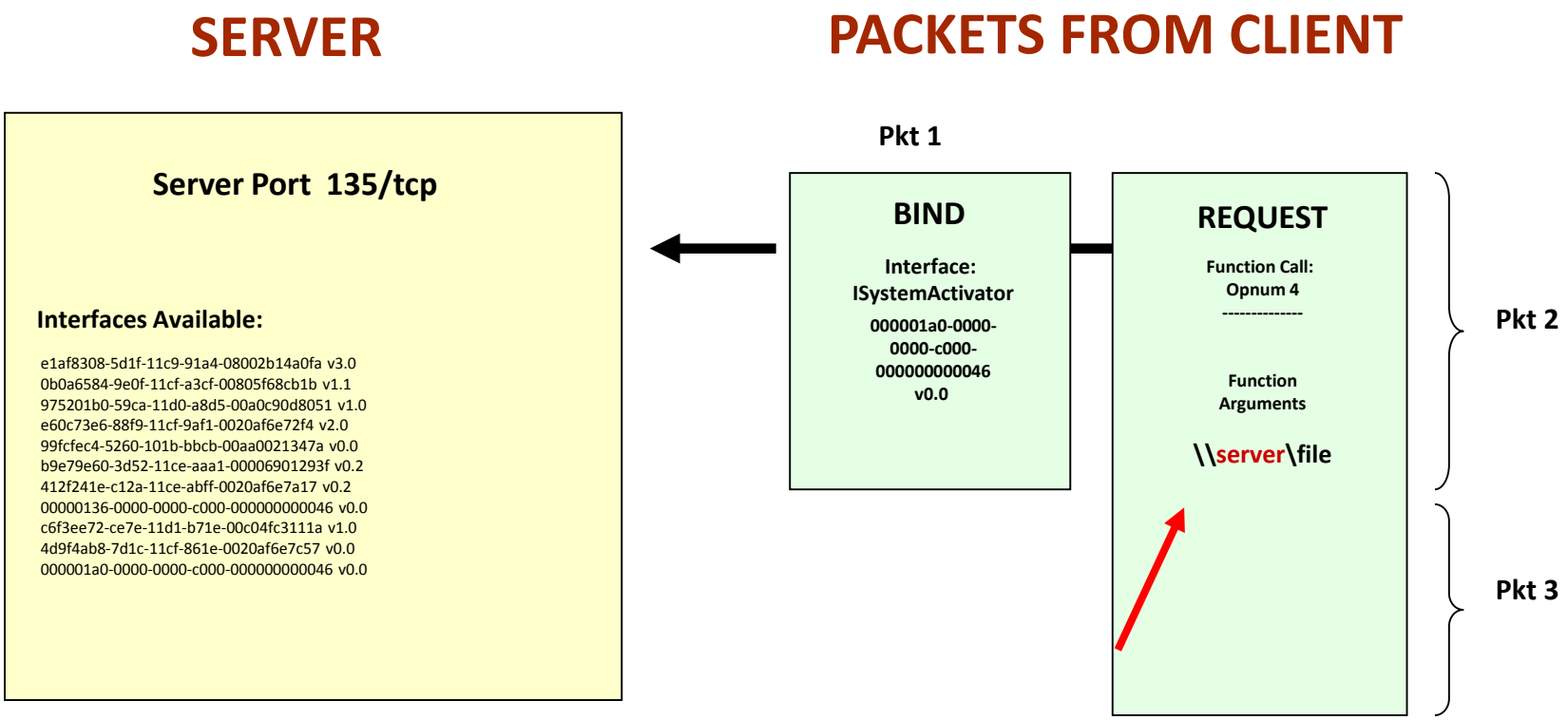
Ransomware

Ransomware is an emerging form of malware that locks the user out of their files or their device, then demands an anonymous online payment to restore access.

規畫防禦作為前先瞭解該安全事件擴散方式

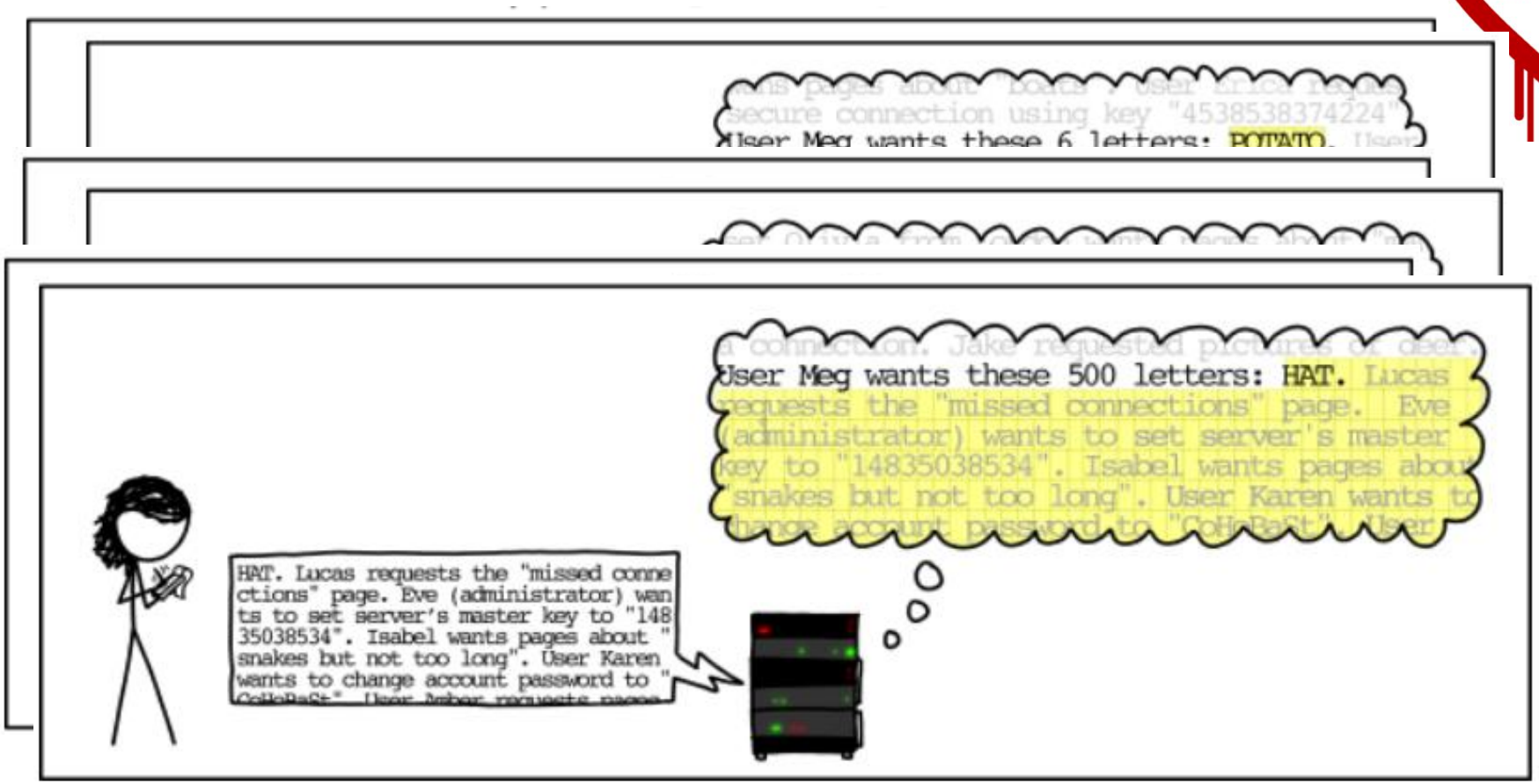


漏洞(Vulnerability)入侵



Function Call 4, contains a heap-based buffer overflow in the server parameter.

如何入侵? Heartbleed Vulnerability in OpenSSL (心臟爆血)



*Source:http://xkcd.com/1354

Vulnerability Filters

In EVERY attack, the following must be true to exploit the buffer overflow

\\server\filename

becomes
\\...44+ character buffer...\filename

A vulnerability filter detects that the following exploitation conditions are satisfied.

- ✓ TCP session established to appropriate port (135)
- ✓ BIND to the appropriate RPC interface
- ✓ REQUEST the appropriate function call (opnum=4)
- ✓ Validate that ***servername*** is not longer than 44 characters

優點：
高精準度、攻擊無法無法閃躲

缺點：
需要強大的硬體資源與快速的掃描引擎

Exploit-Specific Filters

In the posted exploits
\\server\filename

becomes
\\...long buffer with shellcode...\filename

An exploit-specific filter detects the shellcode used in a particular exploit. High false negatives.

優點
簡易的字串比對, 容易設計與部署, 適合於較弱的掃描引擎與硬體。

缺點:
高誤判率, 當攻擊手法改變就無法發揮效用

Example: The following hex string can be used to detect HD Moore's exploit and the MS Blaster worm. These are machine instructions that are passed directly to the victim processor once the buffer overflow is successful.

EB 19 5E 31 C9 81 E9 89 FF FF FF 81 36 80 BF 32 94 81 EE FC
FF FF FF E2 F2 EB 05 E8 E2 FF FF FF 03 53 06 1F 74 57 75 95
80 BF BB 92 7F 89 5A 1A CE B1 DE 7C E1 BE 32

WannaCry news appeared on 2017/5/12

Internet ▾ All news ▾ March 1, 2017-May 12, 2017 ▾ Stored by relevance ▾ Clear

WannaCry Ransomware Attack Hits Victims With Microsoft SMB Exploit
eWeek - May 12, 2017
Ransomware is no longer just a nuisance. Now it's quite literally a matter of life and death. A massive ransomware attack being labeled as "WannaCry" has been ...

A 'kill switch' is slowing the spread of WannaCry ransomware
PCWorld - May 12, 2017
The ransomware, called Wana Decryptor or WannaCry, has been found infecting machines across the globe. It works by exploiting a Windows vulnerability that ...

An NSA Cyber Weapon Might Be Behind A Massive Global ...
Forbes - May 12, 2017
According to the MalwareHunterTeam, which said WannaCry was "spreading like hell," Russia has been the hardest hit, but Spain also seems to be under ...

NSA-created cyber tool spawns global attacks — and victims include ...
Most highly cited - Politico - May 12, 2017

中石油的災情

勒索病毒侵袭全球 中石油2万座加油站断网

纽约时间： 2017-05-16 06:11 AM

勒索病毒 | 中石油 | 加油站

WannaCry勒索病毒蔓延全球，中石油所属的加油站，超过2万座断网。资料图片（pixabay.com）

【新唐人2017年05月16日讯】自12日以来，**WannaCry勒索病毒**蔓延全球，感染了150个国家的30多万台计算机。中国**中石油**公司超过2万座**加油站**也受到攻击，在**断网**约36小时左右才慢慢恢复。

N-Partner

Auto Learning: No need for threshold setting by manual

Report ▸ Traffic Abnormal Report Refresh

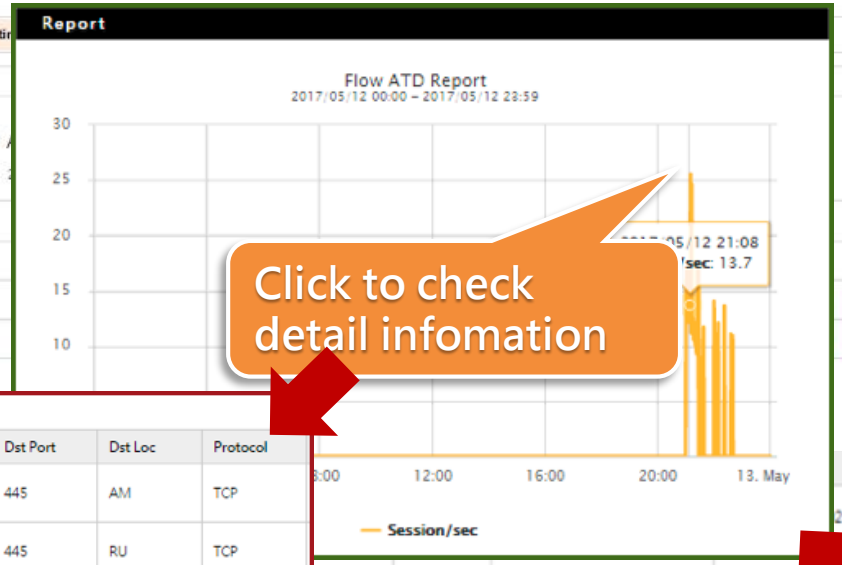
Time Query ▸ Select period in 1 Hour ▾ Last 1 Month Start Time Start Query

Enquery Scope ▸ Global

Query Abnormal item ▸ TCP SYN Host Scan

Keyword Search ▸ Query by Source IP or Destin

Realtime Trend Distribution



Click to check detail infomation

Click to view chart

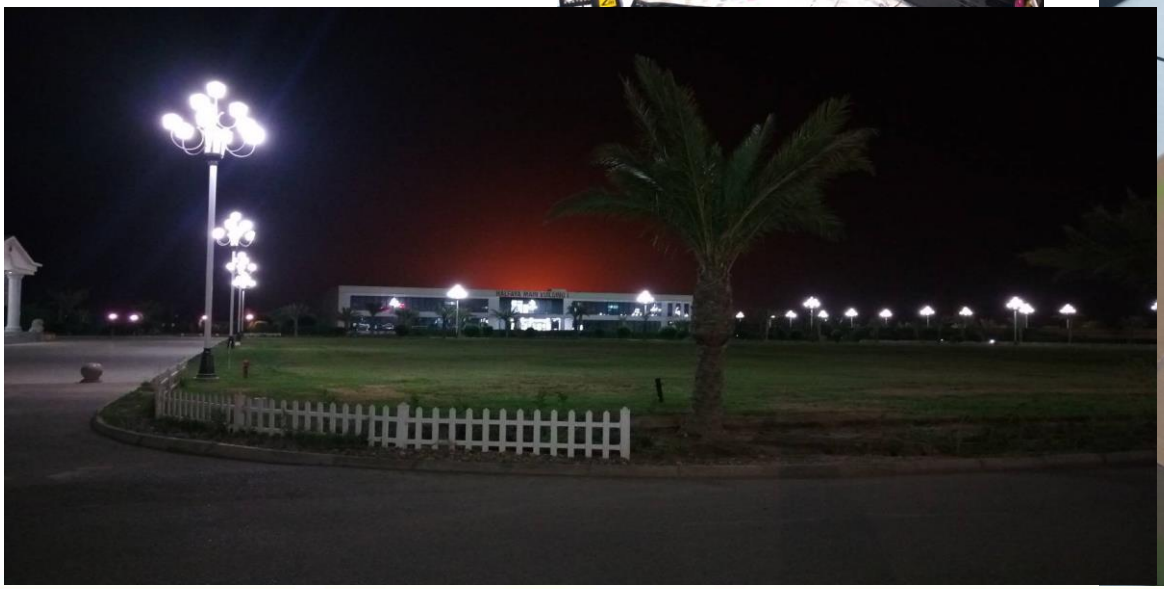
Data Time Range: 2017/05/13 14:01:00 ~ 2017/05/13 14:02:59 Total Number: 9386

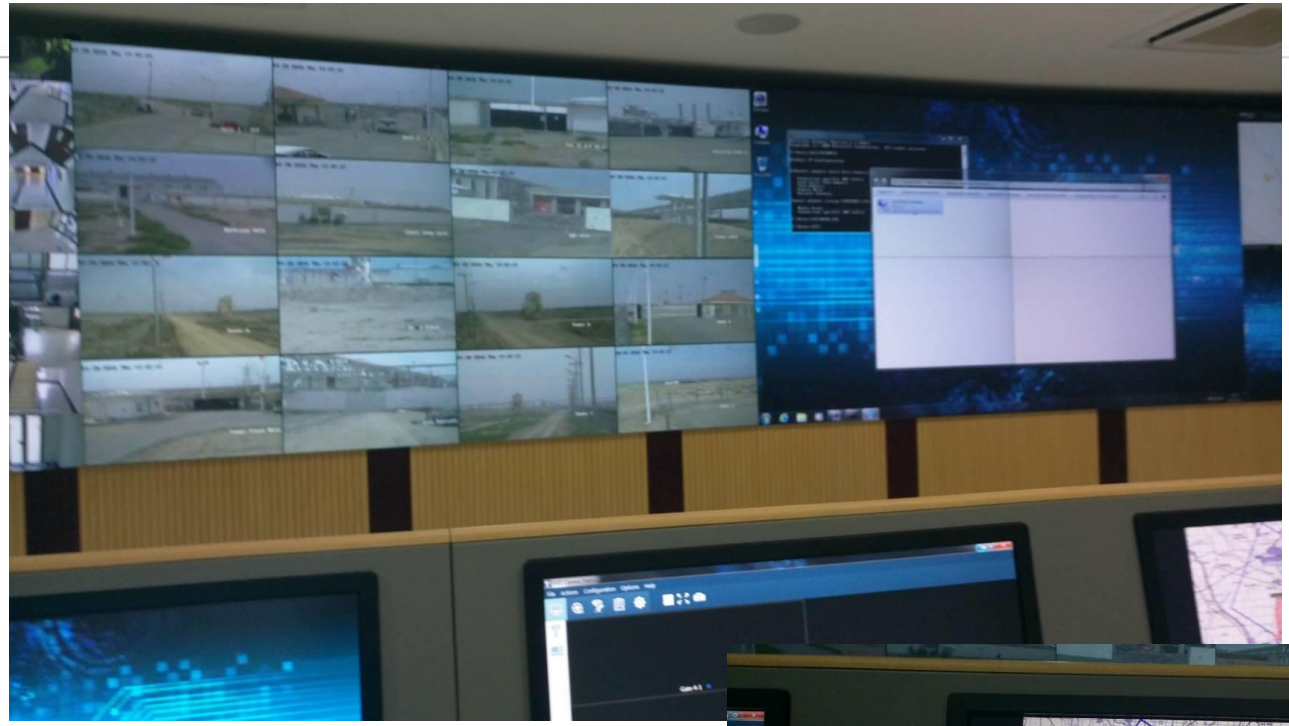
Time	Src IP	Src Port	Dst IP	Dst Port	Dst Loc	Protocol
2017/05/13 14:02:57	10.163.176.40	51385	46.130.56.167	445	AM	TCP
2017/05/13 14:02:57	10.163.176.40	51386	85.140.126.29	445	RU	TCP
2017/05/13 14:02:57	10.163.176.40	51386	85.140.126.29	445	RU	TCP
2017/05/13 14:02:57	10.163.176.40	51387	123.114.58.90	445	CN	TCP
2017/05/13 14:02:57	10.163.176.40	51387	123.114.58.90	445	CN	TCP
2017/05/13 14:02:57	10.163.176.40	51388	48.234.145.197	445	US	TCP
2017/05/13 14:02:57	10.163.176.40	51388	48.234.145.197	445	US	TCP
2017/05/13 14:02:57	10.163.176.40	51389	58.80.216.133	445	JP	TCP

Domain	Abr									View
Global	TCP Sca									
Global	TCP Sca					9K	410.62K	2017/05/13 12:53:00	2017/05/1	
Global	TCP Sca					08K	264.01K	2017/05/13 1		
Global	TCP Sca					K	104.2K	2017/05/13 12:52:00		
Global	TCP Sca					14K	59.2K	2017/05/12 21:16:00	2017/05/12 21:48:00	
Global	TCP Sca					8.7K	952.2K	2017/05/12 21:11:00	2017/05/12 22:36:00	
Global	TCP Sca	MONITOR)				1.08K	1.55M	2017/05/12 20:59:00	2017/05/12 22:39:00	
Global	TCP SYN Host Scan	10.163.15.170 (Irac_ Server)		TCP	445	1.8K	1.8K	93.79K	2017/05/12 20:28:00	2017/05/12 21:05:00	
Global	TCP SYN Host Scan	10.163.176.39 (Irac_(_ _ ir HFO DMS)		TCP	445	798	860	43.69K	2017/05/12 19:21:00	2017/05/12 19:21:00	
Global	TCP SYN Host Scan	10.163.22.2 (Home)		TCP	445	35.78K	51.33K	2.41M	2017/05/12 00:07:00	2017/05/12 11:44:00	

來去伊拉克

SYRIA
IRAQ
Baghdad
Al Mayadin
Abū Kamal
Al Qa'im
Al Hadithah
Tadmur
Qaryatayn
Sab' Abar
At Tanf
Trebil
Ar Ruṭbah
Jabal Unayzah
Ka'id
Nukhayb
Wadi Hawran
Wadi Ratnah
Wadi ar Rummah
Razzaza L.
Ar Ramadi
Al Musayyib
Karbala
Babylon
Al Hillah
Al Kifl
Al Kūfah
An Najaf
Ash Shinafiyah
Ad Diwaniyah
Al Kūt
Al Hayy
Al 'Amarah
Badrah
Mandali
Ba'qubah
Samarra'
Tikrit
Mosul
Kirkuk
Yarmanshah
Dezful
Ash Shatrah
Al 'Uzayr
Al Qurnah
As Samawah
An Nasiriyah
As Salman
Makhfar al Buqayyah
As Sikr
Ash Shabakah
Al Ma'aniyah
Badanah
Al 'Uwayqilah
Ad Duwayd
Al Jumaymah
Sabra al Hijarah
Hawr al Hammar
Az Zubayr
Rumaila
Ras al Khafji
Al Jahrah
Al Ahmadi
Al Fahahil
Al Fanar
Al Ḥawrah
Ar Ruqayyah
Al Ḥadr
Ash Sharqat
Ash Shirqat
Ba'j
Tikrit
Ar Rawah
'Anah
Al Qa'im
Al Mayadin
Al Kawm
Ar Raqqah
Ar Sukhnah
Al Ḥawrah
Ar Ramadi
Al Fallujah
Al Musayyib
Karbala
Babylon
Al Hillah
Al Kifl
Al Kūfah
An Najaf
Ash Shinafiyah
Ad Diwaniyah
Al Kūt
Al Hayy
Al 'Amarah
Badrah
Mandali
Ba'qubah
Samarra'
Tikrit
Mosul
Kirkuk
Yarmanshah
Dezful
Ash Shatrah
Al 'Uzayr
Al Qurnah
As Samawah
An Nasiriyah
As Salman
Makhfar al Buqayyah
As Sikr
Ash Shabakah
Al Ma'aniyah
Badanah
Al 'Uwayqilah
Ad Duwayd
Al Jumaymah
Sabra al Hijarah
Hawr al Hammar
Az Zubayr
Rumaila
Ras al Khafji
Al Jahrah
Al Ahmadi
Al Fahahil
Al Fanar
Al Ḥawrah
Ar Ruqayyah
Al Ḥadr
Ash Sharqat
Ash Shirqat
Ba'j





N-Partner

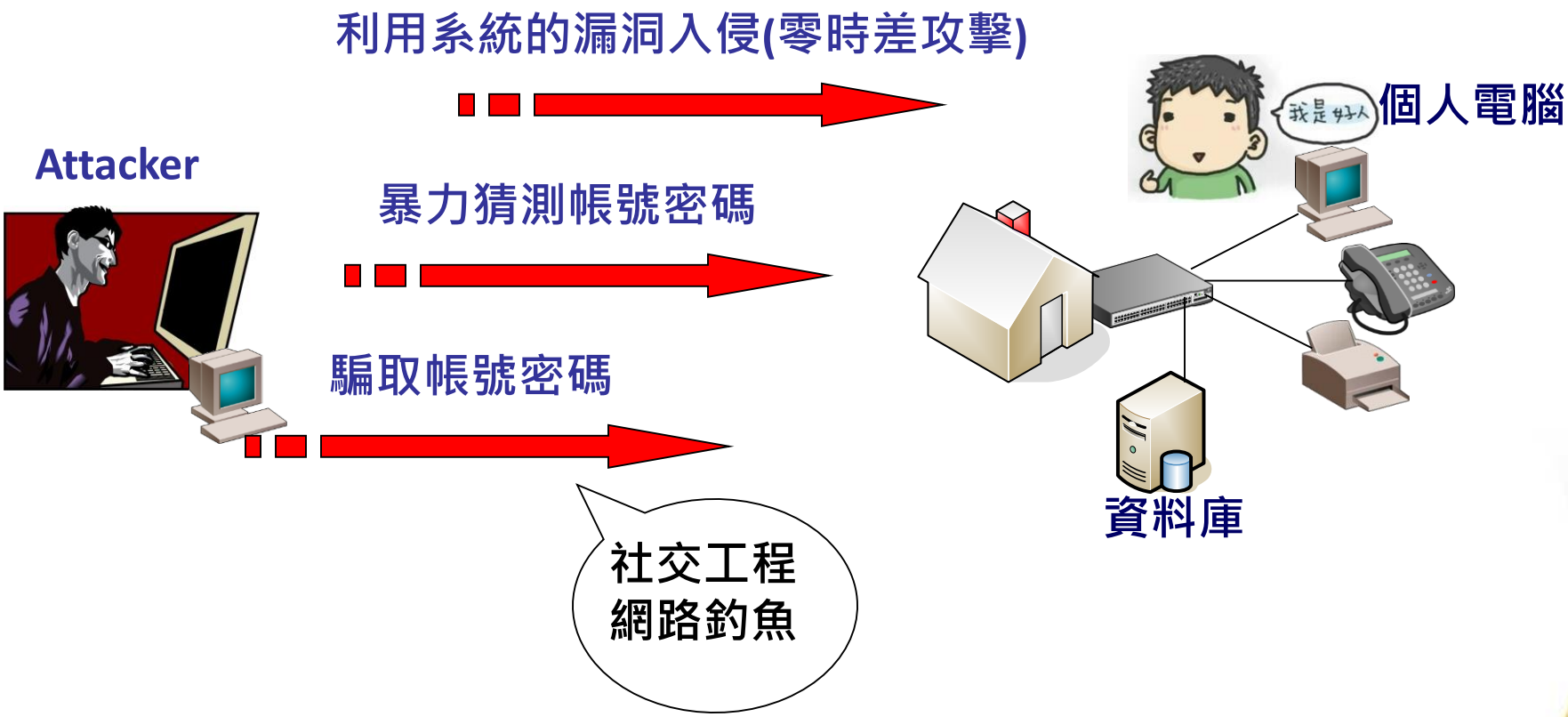
APT(Advanced Persistent Threat)

攻擊階段 → 控制階段 → 活動與擴散階段

根據美國資訊網路公司 Mandiant 在2013年所提出的 調查報告(英文) 中可將 APT 攻擊歸類成以下的生命週期來進行：

1) 初步的入侵：利用一些釣魚網站或電子郵件來做為入侵的媒介。
2) 建立立足點：植入 Rootkit 等惡意程式以掌握使用者系統。
3) 取得管理者權限：利用破解密碼等方式取得該電腦管理者權限。
4) 內部偵查與平行擴散：找尋該主機附近的其他主機或伺服器，並伺機取得其內部資料庫儲存之機密資料。
5) 持續監控並完成任務：持續掌控資料庫伺服器或是主機，並將資料匯出達到竊取機密的目的。

駭客入侵電腦系統常用的三種方式



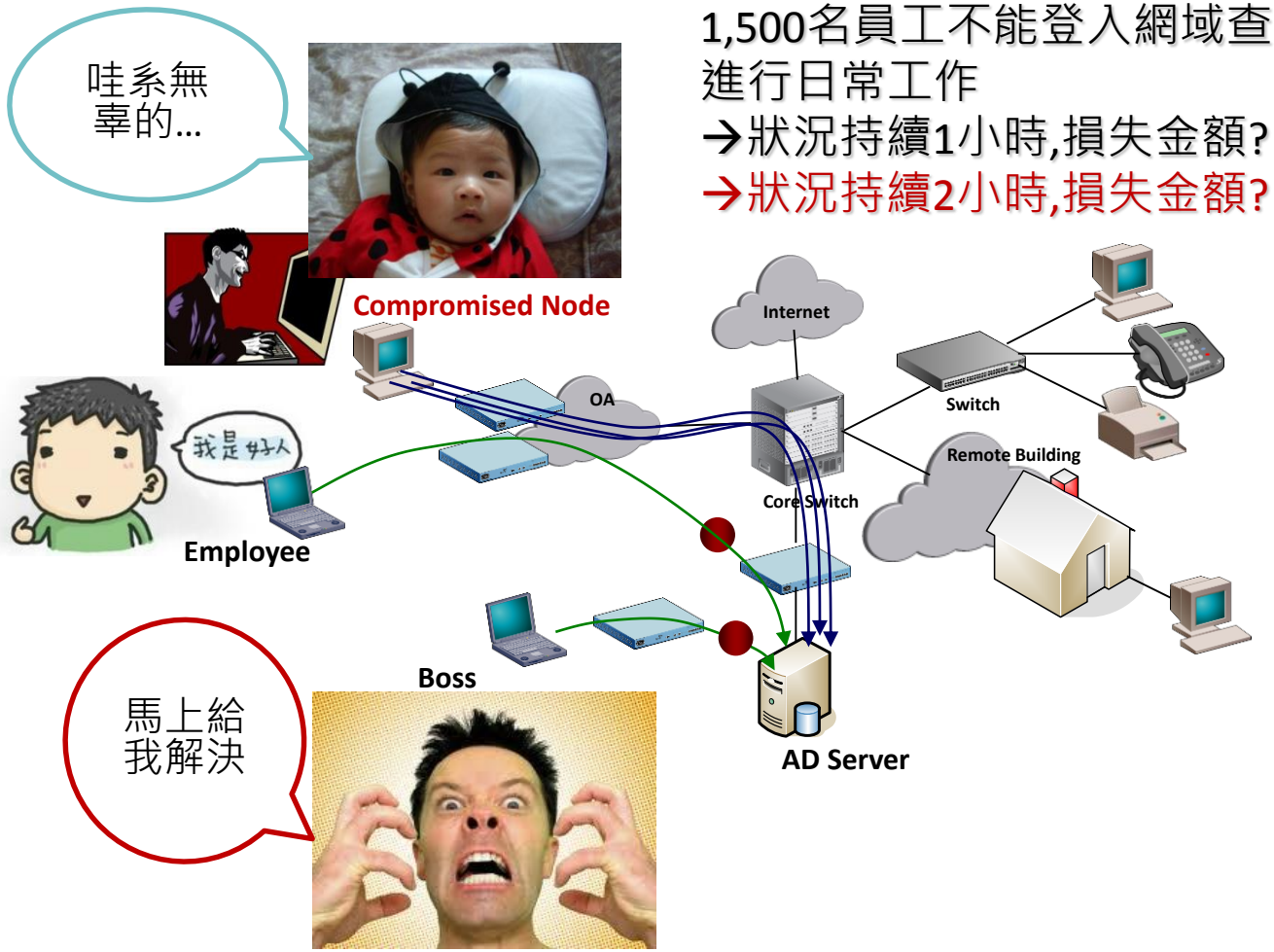
REAL CASE STUDY (無法登入網域)

來自內部的AD密碼暴力猜測攻擊→多數員工AD帳號遭Lock

1,500名員工不能登入網域查閱資料與進行日常工作

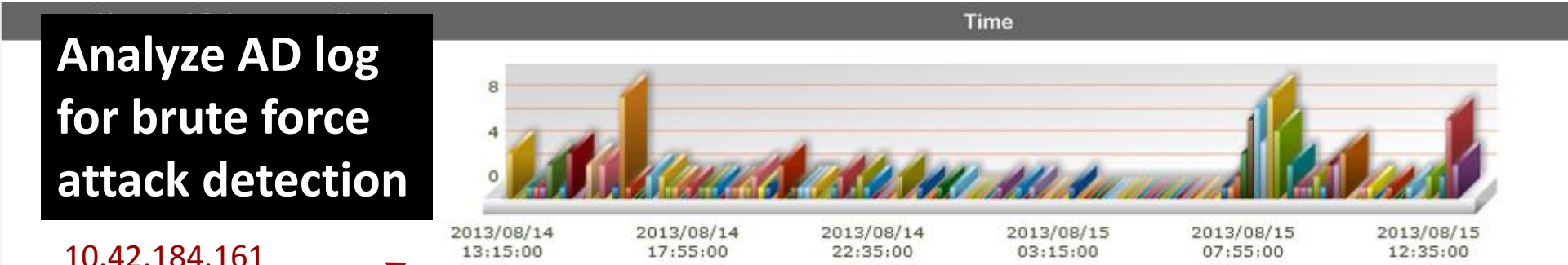
→狀況持續1小時,損失金額?

→狀況持續2小時,損失金額?



Auto learning use case: AD brute force

Analyze AD log for brute force attack detection



10.42.184.161
Is doing brute force attacks

Event	Src IP	Audit User	Time	Devices
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02

Event	Src IP	Audit User	Time
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:14
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:14
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:09
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:09

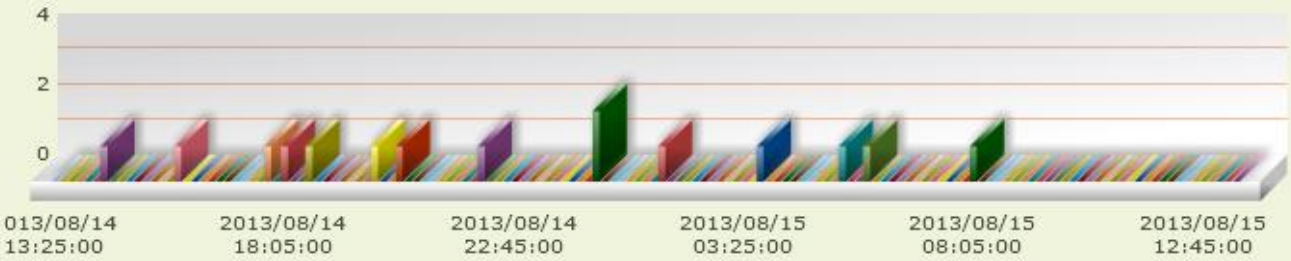
Event	Src IP	Audit User	Time
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11

N-Partner

Auto learning use case: AD brute force

Abnormal Category	Number	Time

Analyze AD log for brute force attack detection



This IP got the correct password for login purpose

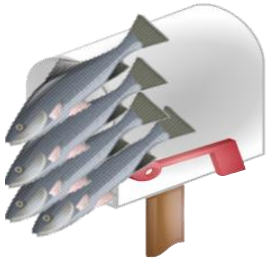
Event	Src IP	Audit User	Time	Devices
Logon Success (Security: 673)	10.42.201.2	K000477	2013/08/15 00:20:01	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/15 00:18:46	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/15 00:18:46	OA AD02
Login Failure (Security: 675)	10.42.201.2	K1102366	2013/08/14 23:52:49	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:46:23	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:46:23	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:45:33	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:39:37	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:37:12	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:37:12	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:33:56	OA AD02

APT通常伴隨社交工程與釣魚詐騙技術

何謂「社交工程」?

社交工程，英文為Social Engineering，是一種利用人性弱點，並**結合心理學知識如欺騙、偽裝、恐嚇、說服、恭維等**來獲取(騙取)有用資訊的一種駭客攻擊手法。

何謂「網路釣魚」?

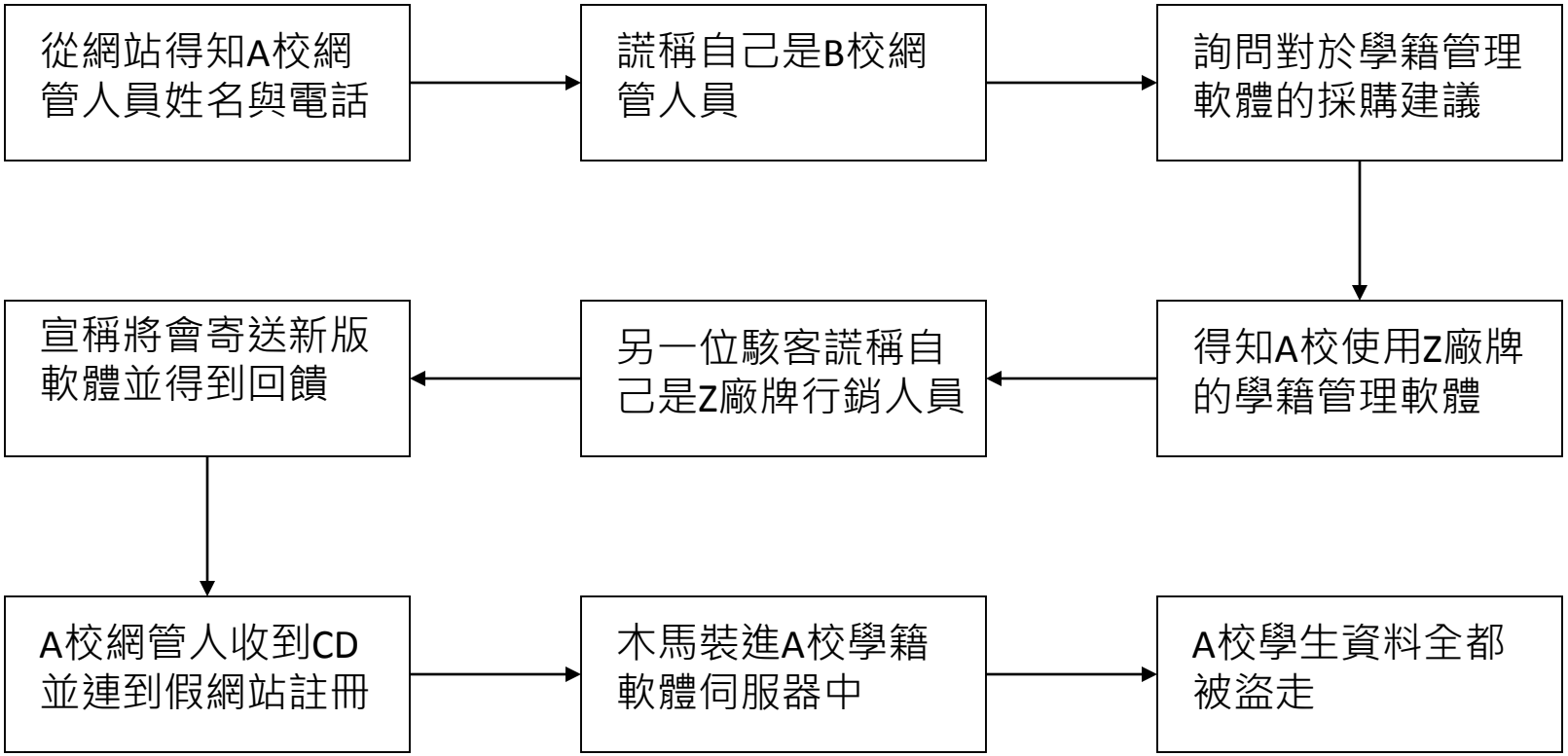


「網路釣魚」，英文為Phishing，根據反網路釣魚工作小組（APWG）所做的定義，「網路釣魚」是利用**偽造電子郵件**與**幾可亂真的仿冒網站**作為誘餌，愚弄使用者洩漏如銀行帳戶密碼、信用卡號碼等個人機密資料的一種駭客手法。

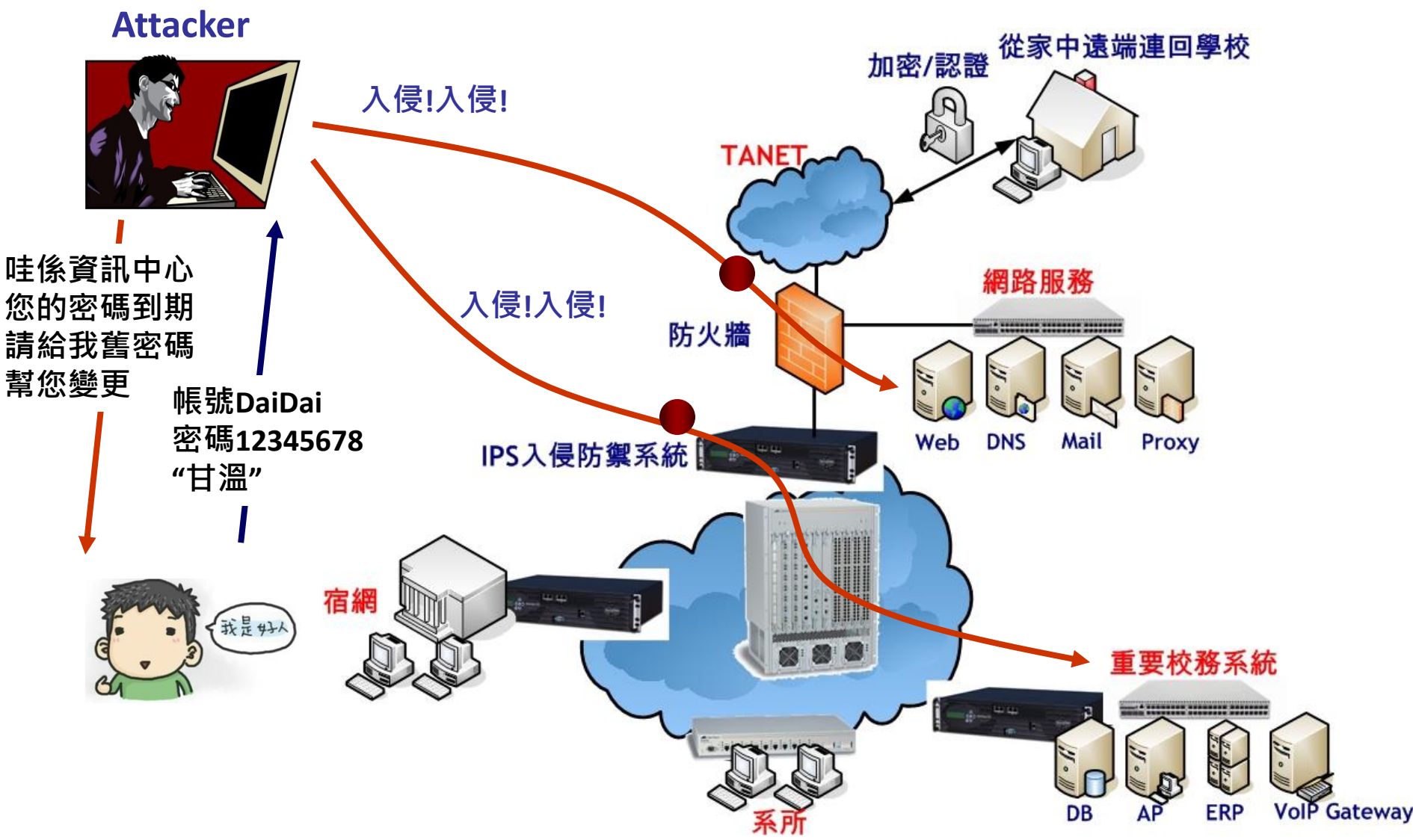
根據調查: 利用知名品牌所建立的信賴感，讓此類詐騙行為成功機率達5%

訪談詐騙社交工程實例流程圖--偽裝與恭維

目的:試圖了解A校用的學籍管理軟體,並入侵系統後取得學生資料

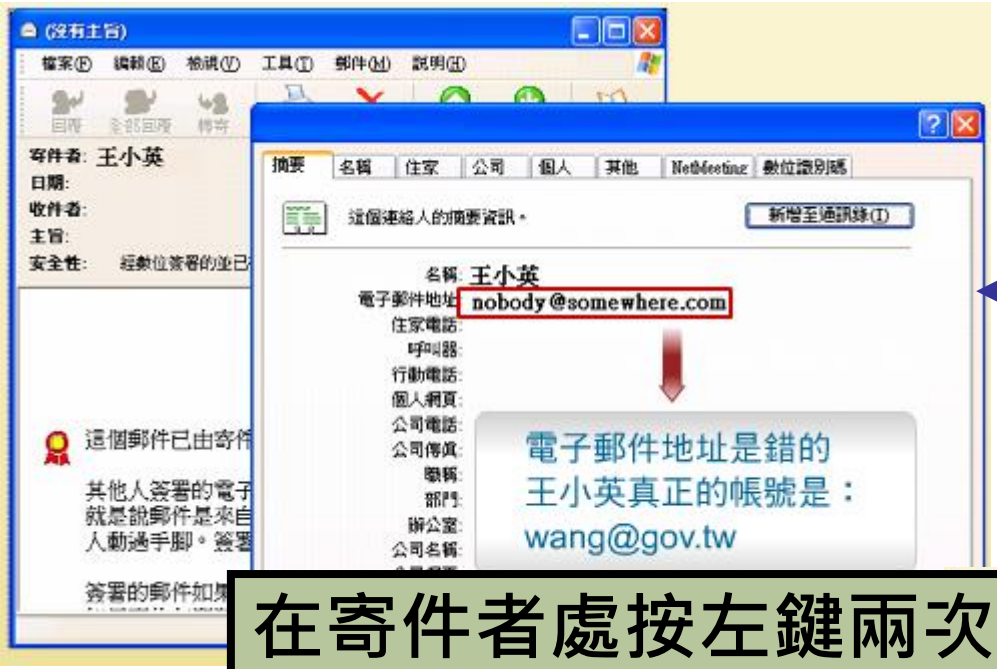


高手入侵?用騙的比較快


Attacker
入侵!入侵!
入侵!入侵!
哇係資訊中心
您的密碼到期
請給我舊密碼
幫您變更
帳號DaiDai
密碼12345678
“甘溫”
我是好人
加密/認證
從家中遠端連回學校
TANET
網路服務
防火牆
Web
DNS
Mail
Proxy
IPS入侵防禦系統
宿網
重要校務系統
系所
DB
AP
ERP
VoIP Gateway

電子郵件社交工程

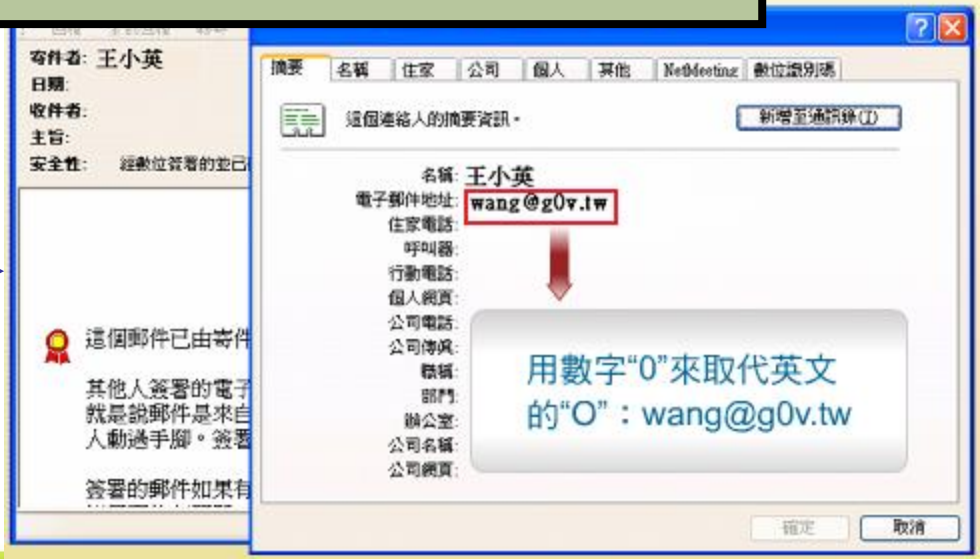
假冒的寄件者與電子郵件地址



使用相同的顯示名稱:王小英

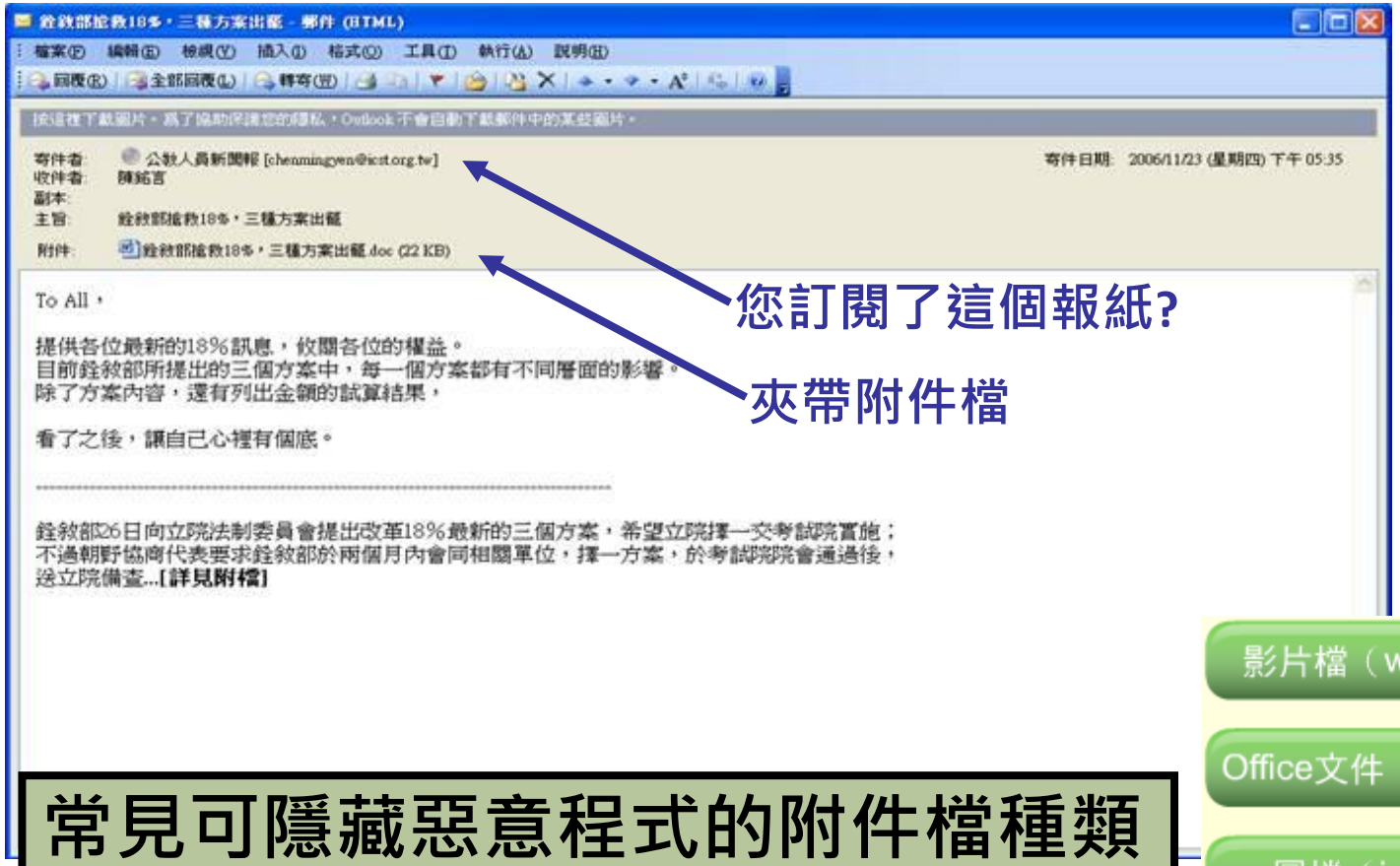
在寄件者處按左鍵兩次查看詳細寄件者資訊

申請類似的郵件地址



電子郵件社交工程

令人感興趣的郵件主旨(公文?權益?)



您訂閱了這個報紙?

夾帶附件檔

常見可隱藏惡意程式的附件檔種類

- 影片檔（wmv）
- Office文件（doc）
- 圖檔（jpg）
- 壓縮檔（zip）

Worms

Trojans

Viruses

Spyware

電子郵件社交工程

令人感興趣的郵件內容(情色,八卦,旅遊好康...)

您認識寄件者?常聯絡嗎?

夾帶附件檔

您曾經收到類似的信件嗎?

Hotmail

新增 | 刪除 垃圾郵件 | 標示為 ▾ 置於資料夾 ▾ |

rockflow@hotmail.com

收件匣 (39)
垃圾郵件
草稿 (1)
寄件備份
刪除的郵件 (40)
3Com
Account
Business
Order
Sad
Security
管理資料夾

相關網站
今日焦點
連絡人清單
行事曆

回覆 全部回覆 轉寄 |

Windows Live服務系統更新緊急通知

寄件者： 石 謂龍 (rockflow@hotmail.com)
寄件日期： 2009年4月11日 下午 03:14:08
收件者： 石 謂龍 (rockflow@hotmail.com)

親愛的Windows Live用戶

我們誠摯的感謝您使用Windows Live服務!

為了提供您更好的服務品質,我們將於2009/4/1進行系統更新作業,在此要煩請您做好Windows Live資料備份的工作,以確保您在MSN與Hotmail中的連絡人資料以及信件內容不會因為這次的系統更新而意外漏失!

您必須於2009/3/30前完成新系統的登入動作,完成後我們將為您把存放於舊系統的Windows Live資料轉移到新系統上!

欲執行新系統登入動作請點選下列連結,並輸入您的Windows Live帳號與密碼
http://www.microsoft.com/passport/login.asp@333865994/login.asp

謝謝您的使用!

Bob Smith
Director of Windows Live Service
Microsoft
http://www.microsoft.com
Windows Live™

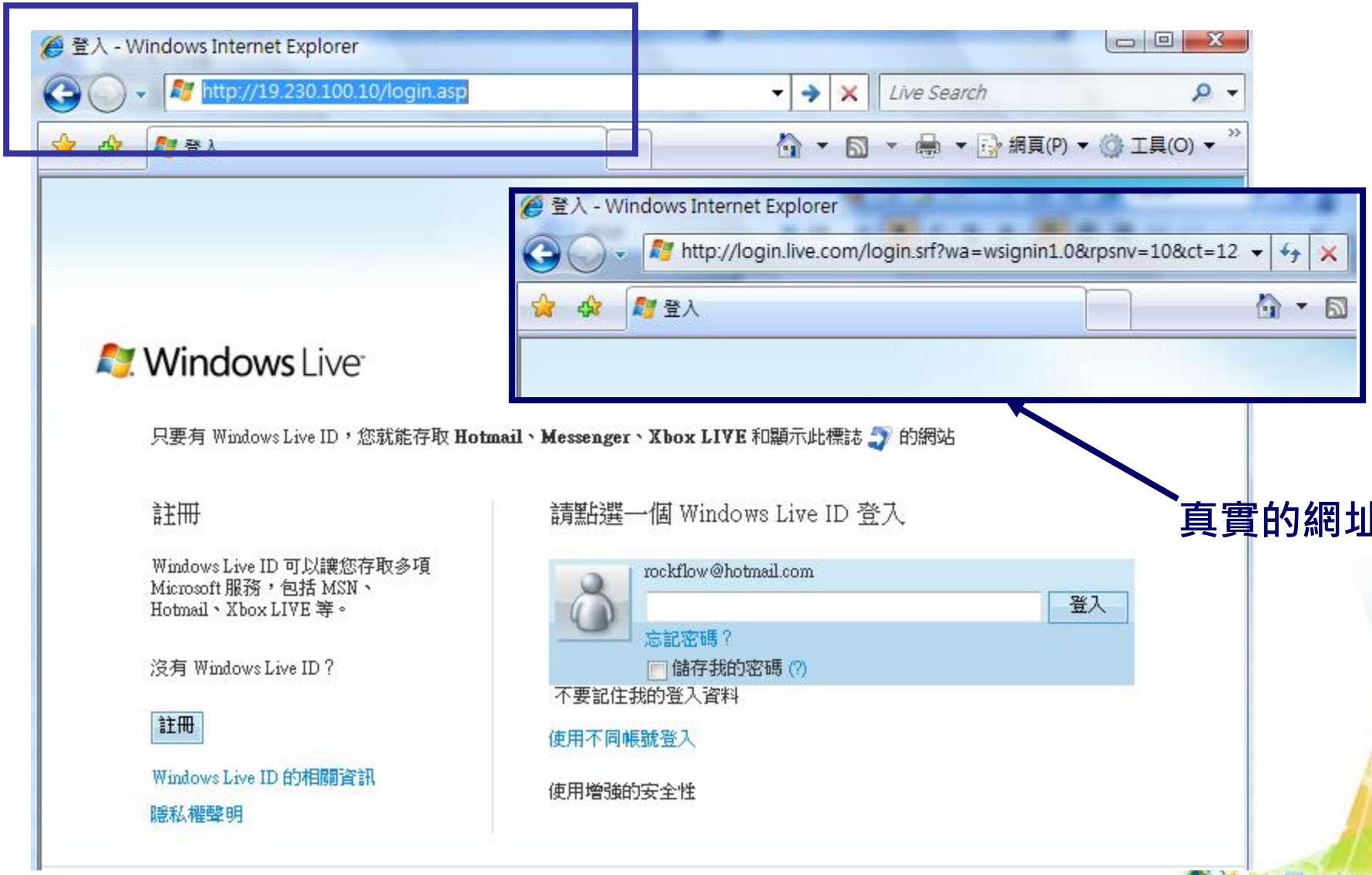
@前面的敘述都將被忽略

署名的部份煞有其事,還有Logo

N-Partner

網址列用IP來呈現?

登入畫面幾可亂真



結合Google關鍵字廣告的釣魚網址

透過Google查詢「拍賣」

竟看到假的Yahoo拍賣網站
tw.bids-yahoo.com

N-Partner

結合Google關鍵字廣告的釣魚網址(續)

真的Yahoo拍賣

假的Yahoo拍賣

TAIWAN CYBER SECURITY LANDSCAPE VERSION ALPHA6

2018 DEC

iThome

Endpoint Prevention

AhnLab, Carbon Black, Check Point, CROWDSTRIKE, CYBERARK, ERICOM, ESET, F-Secure 芬安全, FineArt 精品科技, forceshield, ForeScout, FORTINET, IBM, ivanti, KASPERSKY 卡巴斯基, Malwarebytes, McAfee, Menlo Security, MICRO FOCUS, Microsoft, NARD SECURITY, OPSWAT, paloalto, SentinelOne, ST Engineering, SOPHOS, Symantec, TREND MICRO 趨勢科技, tripwire, vmware, VOTIRO

Endpoint Detection & Response

AhnLab, Carbon Black, Check Point, cisco, CounterTack, CROWDSTRIKE, CYBERARK, CYBERBIT, Deloitte. 勤業眾信, DigiCert, DigiPPLER 數聯資安, Dragon Soft, FireEye, FORCEPOINT, F-Secure 芬安全, Fidelis, IBM, KASPERSKY 卡巴斯基, Malwarebytes, McAfee, Microsoft, paloalto, SentinelOne, SOPHOS, Symantec, TREND MICRO 趨勢科技, VERINT, WatchGuard

Network Firewall

A10, AhnLab, Barracuda, Check Point, cisco, FORCEPOINT, FORTINET, LIONIC, f5 Networks, NETWORK BOX, paloalto, SharpTech, SONICWALL, SOPHOS, STORMSHIELD, WatchGuard, zscaler, ZYXEL 合勤科技

DDoS Protection

A10, AhnLab, Akamai, CDNetworks, aws, Check Point, DigiCert, 中華電信 Chunghwa Telecom, citrix, CLOUDFLARE, 網銘數位 Digicentre, f5, FORTINET, HIERON, Imperva, Infoblox, Microsoft, NETSCOUT | Arbor, NEXUSGUARD, NETWORK BOX, N-Partner, NSFOCUS, radware, 台灣大哥大

Network Analysis & Forensics

ARCRAN, aruba, 中華資安國際 CHT Security, cisco, DARKTRACE, Deloitte. 勤業眾信, Extreme, Fidelis, FireEye, Fortinet, Gigamon, IBM, ixia, N-Partner, PacketX, paloalto, radware, SONICWALL, Symantec, UGuard, vARMOUR, VERINT, vmware

Advanced Threat Protection

AhnLab, BOX, Check Point, Cellopoint, 中華電信 Chunghwa Telecom, 中華資安國際 CHT Security, cisco, 中華數碼 Cyber Link, 中信國際電訊股份有限公司 CITIC TELECOM CPC, CDNetworks, DARKTRACE, DigiPPLER 數聯資安, Dragon Soft, F-Secure 芬安全, Fidelis, FireEye, FORCEPOINT, ForeScout, FORTINET, juniper, KASPERSKY 卡巴斯基, lastline, McAfee, NETWORK BOX, MICRO FOCUS, Microsoft, Openfind, OPSWAT, paloalto, proofpoint, REDSOCKS, Softnext 中華數位科技, SONICWALL, SOPHOS, Symantec, TREND MICRO 趨勢科技, vARMOUR, VERINT, WatchGuard, ZYXEL 合勤科技, zscaler

Web Security

A10, Akamai, Barracuda, Check Point, cisco, ERICOM, f5, FORCEPOINT, FORTINET, f5 Networks, McAfee, NETWORK BOX, SOPHOS, Symantec, TREND MICRO 趨勢科技

Risk Assessment & Visibility

acunetix, AMSECURE, aws, 中華資安國際 CHT Security, 中信國際電訊股份有限公司 CITIC TELECOM CPC, CDNetworks, Deloitte. 勤業眾信, DEVCORE, Dragon Soft, IBM, IPANSEC 中為國際資安顧問股份有限公司, 數聯資安, kiuwan, Microsoft, observeit, Qualys, Radiant Tech, RAPID7, RISKIQ, Symantec, tenable, Ware Valley, WhiteSource

WAF & Application Security

A10, Akamai, ARXAN, aws, Barracuda, ca technologies, citrix, CLOUDFLARE, f5, forceshield, FORTINET, IBM, IMPERVA, Microsoft, NETWORK BOX, Qualys, radware, riverbed, SONICWALL, Symantec, TREND MICRO 趨勢科技, WhiteSource

Application Security Testing

ca technologies, CHECKMARX, 中華資安國際 CHT Security, 網銘數位 Digicentre, IBM, 數聯資安, MICRO FOCUS, Qualys, tenable, WhiteSource

iThome

臺灣資安市場地圖

TAIWAN CYBER SECURITY LANDSCAPE VERSION ALPHA6

Managed Security Service

ACEI 資訊科技, Akamai, AVIOT, BCCF 資訊科技, Check Point, 中華資安國際 CHT Security, CyberSource, 網銘數位 Digicentre, f5, FireEye, IBM, 數聯資安, Microsoft, NETWORK BOX, SentinelOne, ST Engineering, Symantec, 睿貿網路, TREND MICRO 趨勢科技, VERINT, zscaler

Security Awareness & Training

AMSECURE, Deloitte. 勤業眾信, GSS 叡揚資訊, proofpoint, SOPHOS, ST Engineering, Symantec, TREND MICRO 趨勢科技

Encryption

aws, CERTES NETWORKS, CHANGING 全新科技, FineArt 精品科技, FUDO SECURITY, gemalto, I•X, KUNGFUNET, proofpoint, MICRO FOCUS, Microsoft, SOPHOS, ST Engineering, Symantec, THALES, TrustView, utimaco, Ware Valley

Data Leak Prevention

ca technologies, Check Point, CLOUDFLARE, cobrasoftc, DIGITAL GUARDIAN, Fidelis, FineArt 精品科技, FORCEPOINT, GTT Technologies, McAfee, Microsoft, NETWORK BOX, proofpoint, Symantec, VARONIS, Ware Valley, zscaler

Mobile Security

ARXAN, BlackBerry, Check Point, citrix, f5, iSecurity, IBM, Microsoft, MobileIron, Symantec, vmware, XCome

Penetration Testing

ACEI 資訊科技, BCCF 資訊科技, 中華資安國際 CHT Security, 中信國際電訊股份有限公司 CITIC TELECOM CPC, Deloitte. 勤業眾信, DEVCORE, 網銘數位 Digicentre, 數聯資安, NARD SECURITY, RAPID7, 睿貿網路

Container Security

McAfee, Qualys, tenable, TREND MICRO 趨勢科技, vARMOUR, WhiteSource

Cloud Security

aws, Check Point, cisco, FORCEPOINT, HDE, IBM, McAfee, Microsoft, NETWORK BOX, paloalto, Symantec, TREND MICRO 趨勢科技, zscaler

GCB

SOFT 軟體世界, Dragon Soft, 雷擎先進, Radiant Tech, RAPIXUS, Symantec

Incident Response

ALIEN VAULT, BCCF 資訊科技, Check Point, 中華資安國際 CHT Security, CYBERBIT, CDNetworks, Deloitte. 勤業眾信, Fidelis, IBM, 數聯資安, Microsoft, MICRO FOCUS, NETWORK BOX, paloalto, Softnext 中華數位科技, ST Engineering, Symantec, 睿貿網路, VERINT

NAC

aruba, Check Point, cisco, SOFT 軟體世界, Extreme, ForeScout, FORTINET, Infoblox, IPguard, Microsoft, NETWORK BOX, PMS 飛泓科技, paloalto, UPAS

Firewall Management

algosec, FIREMON, tufin

Secure File Sharing

axway, citrix, FINALCODE, FineArt 精品科技, IBM, ipswitch, Microsoft, Openfind, QNAP, RICOH, Synology, TrustView, vmware

Authentication

aws, ca technologies, Centrify, CHANGING 全新科技, 中華電信 Chunghwa Telecom, datablink, FUDO SECURITY, FORTINET, FUJITSU, gemalto, ID-Trust, IBM, I•X, LDAP, Microsoft, ONE IDENTITY, Symantec, thycotic, vmware

Privileged Access Management

ANCHOR, Avecto, aws, ca technologies, Centrify, cobrasoftc, CYBERARK, FUDO SECURITY, Krontech, observeit, ONE IDENTITY, thycotic, VARONIS

Identity Governance

ca technologies, Centrify, CYBERARK, f5, IBM, MICRO FOCUS, Microsoft, ONE IDENTITY, SailPoint, vmware

IDaaS

aws, Centrify, CYBERARK, gemalto, IBM, Microsoft, ONE IDENTITY, vmware

Messaging Security

Barracuda, BOX, Cellopoint, Check Point, cisco, f5, FireEye, FORCEPOINT, FORTINET, McAfee, Microsoft, Openfind, proofpoint, ShareTech, Softnext 中華數位科技, SONICWALL, SOPHOS, Symantec, TREND MICRO 趨勢科技

Security Information and Event Management

ALIEN VAULT, AMIYA, Billows, Check Point, CORRELOG, FORTINET, IBM, IPANSEC 中為國際資安顧問股份有限公司, 數聯資安, LogRhythm, McAfee, MICRO FOCUS, Microsoft, NETWORK BOX, N-Partner, SecuLegal, splunk>, tripwire

Security Analytics

aws, 中華電信 Chunghwa Telecom, 中信國際電訊股份有限公司 CITIC TELECOM CPC, CDNetworks, DARKTRACE, Deloitte. 勤業眾信, FORCEPOINT, GTT Technologies, IBM, 數聯資安, Microsoft, paloalto, observeit, RAPID7, RISKIQ, Symantec, VERINT

Threat Intelligence

ALIEN VAULT, Check Point, cisco, CROWDSTRIKE, CDNetworks, DigiPPLER 數聯資安, FireEye, IBM, ixia, lastline, McAfee, NETWORK BOX, paloalto, proofpoint, Qualys, RISKIQ, Symantec, VERINT

ICS & IoT

Check Point, CYBERBIT, Deloitte. 勤業眾信, NETWORK BOX, paloalto, ST Engineering, Symantec, tenable, TREND MICRO 趨勢科技

DNS Security

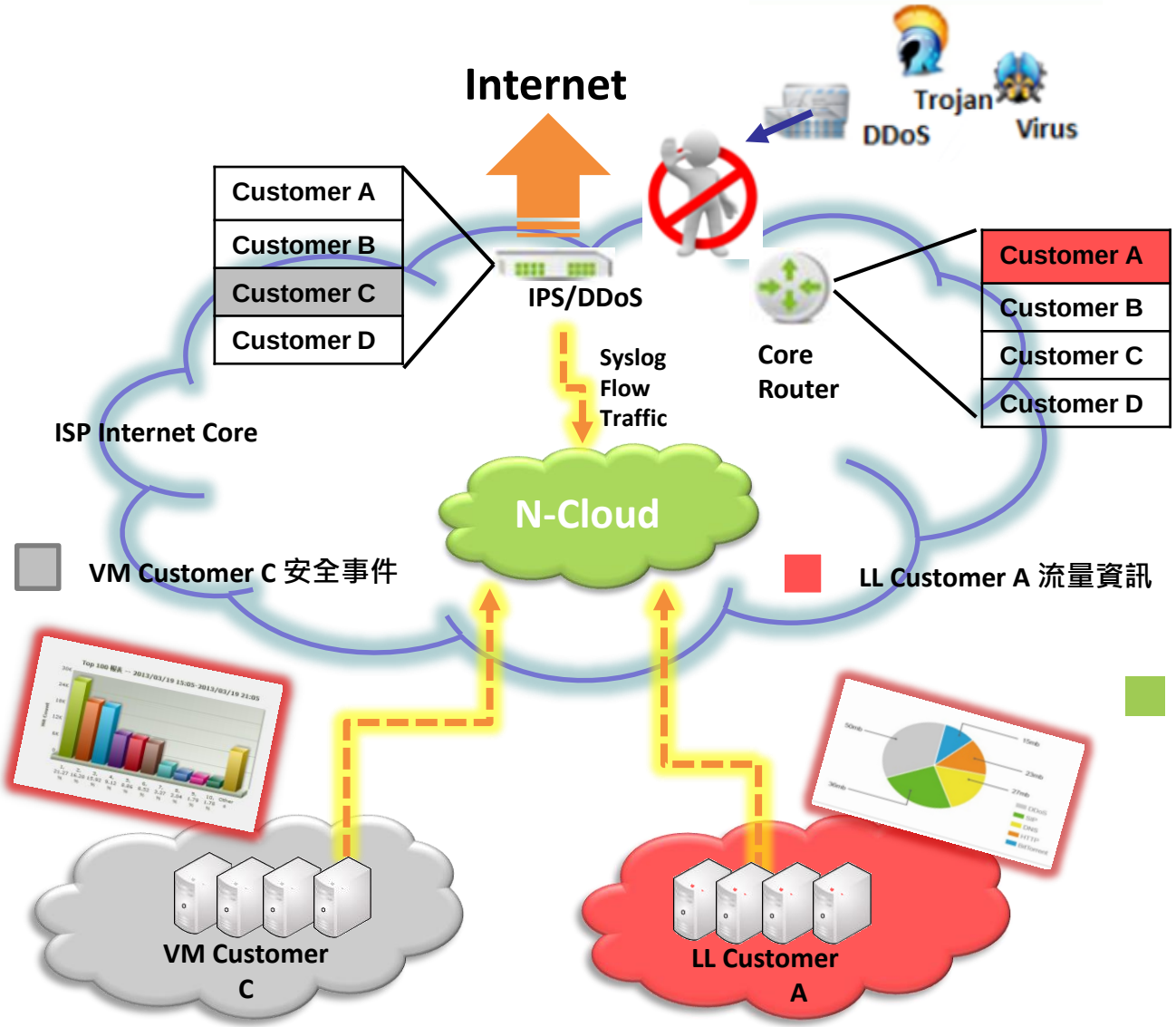
A10, Akamai, cisco, CLOUDFLARE, Infoblox, zscaler

《臺灣資安市場地圖》Alpha6版，囊括目前熱門的33種資安產品與服務，以及178家廠商，日後將持續更新資訊，以呈現臺灣資安市場完整面貌，歡迎與我們交流討論。

N-Partner

資安雲運用

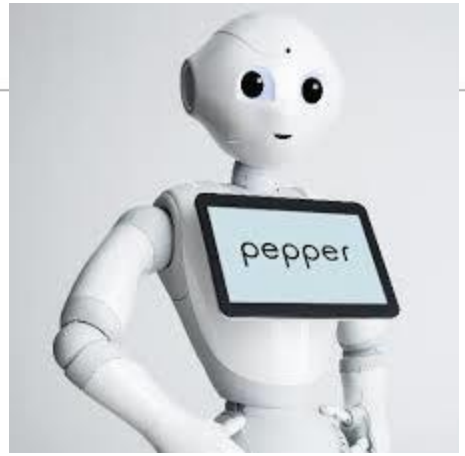
讓電信的資安加值服務(IPS, WAF, DDoS, APT...)更可視化



專屬Portal

每個客戶都有一個專屬Portal，可以查詢屬於自己的資安事件與流量使用

台灣IT行業的現況與未來



What’s the future?

AI=讓機器學習

A	形容詞	B	名詞	C	動詞
0	孤獨34	0	生命50	0	愛54
1	自由17	1	路37	1	碎37
2	迷惘16	2	夜29	2	哭35
3	堅強13	3	天空24	3	死27
4	絕望8	4	孩子23	4	飛26
5	青春7	5	雨21	5	夢想14
6	迷茫6	6	石頭9	6	祈禱10
7	光明6	7	鳥9	7	離去10

如果我們隨便寫一串數字，然後按照數位依次在形容詞、名詞和動詞中取出一個詞，連在一起會怎麼樣呢？
例如取圓周率 3.1415926，對應的詞語是：堅強，路，飛，自由，雨，埋，迷惘。稍微連接和潤筆一下

堅強的孩子，
依然前行在路上，
張開翅膀飛向自由，
讓雨水埋葬他的迷惘。

N-Partner

鼓勵年輕學子

有情感的創意

懂得團隊合作

開發能力

One step forward

Do things done

to

Excellently

Multi- Expertise

Q & A

感謝您的耐心聽講與寶貴意見

石謂龍 Robin Shih
Product Director
rshih@npartnertech.com
+886-935784086

N-Partner