



REDSOCKS
malicious threat detection

惡意威脅的薩德預警系統

力悅資訊

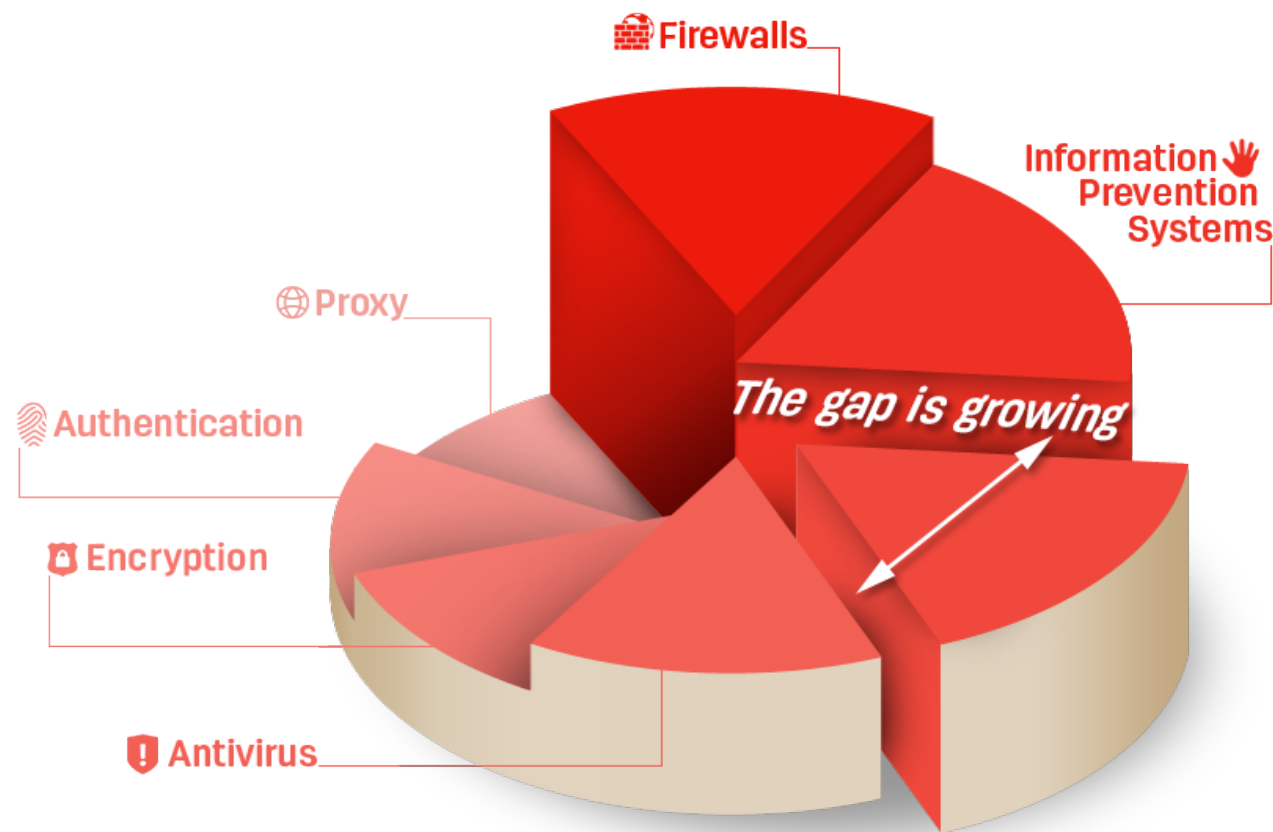
彭國達

資訊安全的著眼點正在改變



許多資安專家聲稱防禦型的產品
已經快跟不上時代的變化。

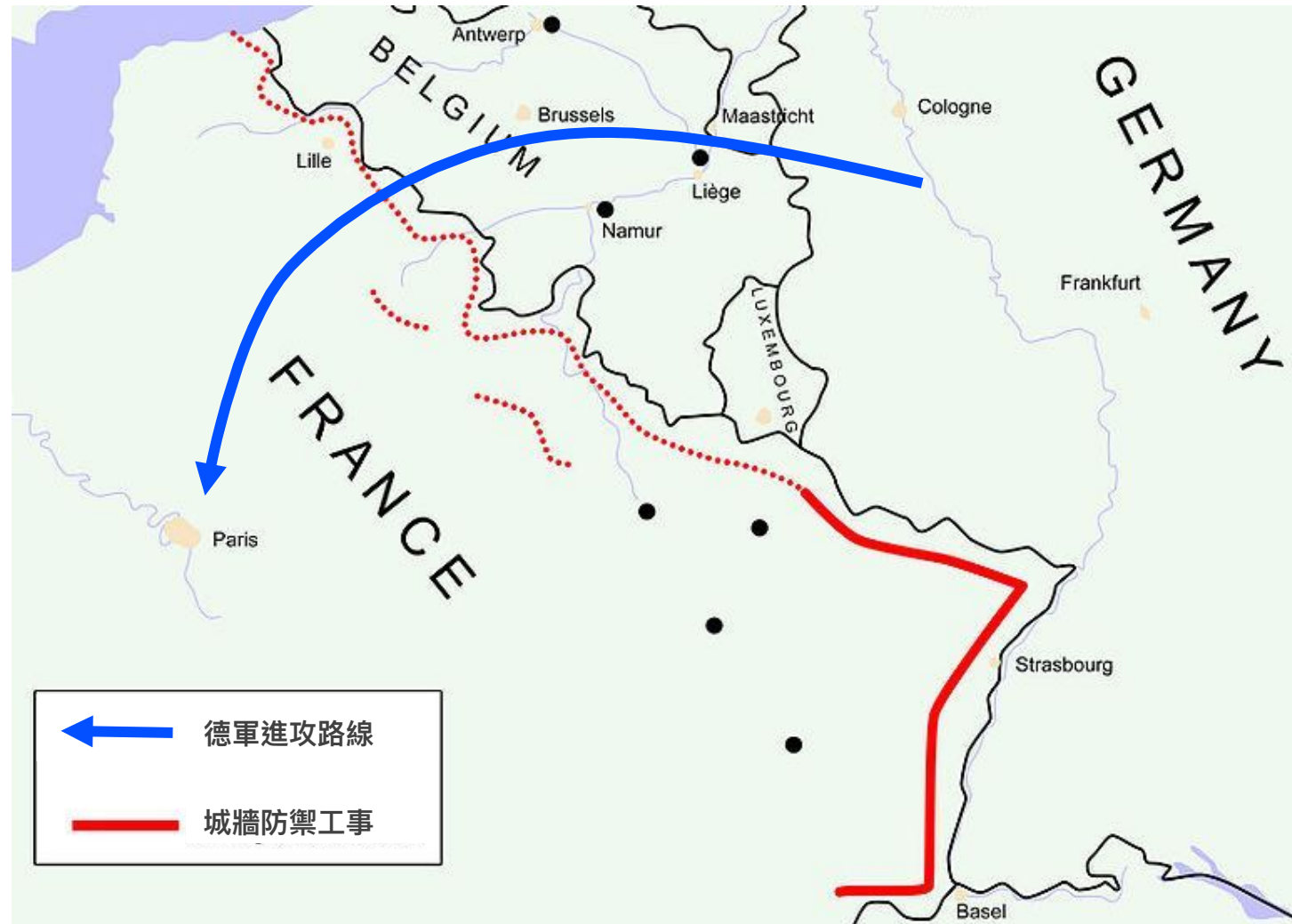
在資訊爆炸的商業環境中，
網路犯罪者都會用許多**意料不到**
途徑達成他們的目標與目的



防禦機制真的越多越好嗎？



法國 馬其諾防線要塞



早期預警系統



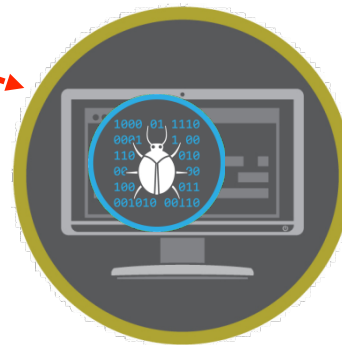
早期預警系統



惡意攻擊者



incoming threat 惡意威脅來襲



① 早期預警系統偵測到
惡意威脅來襲



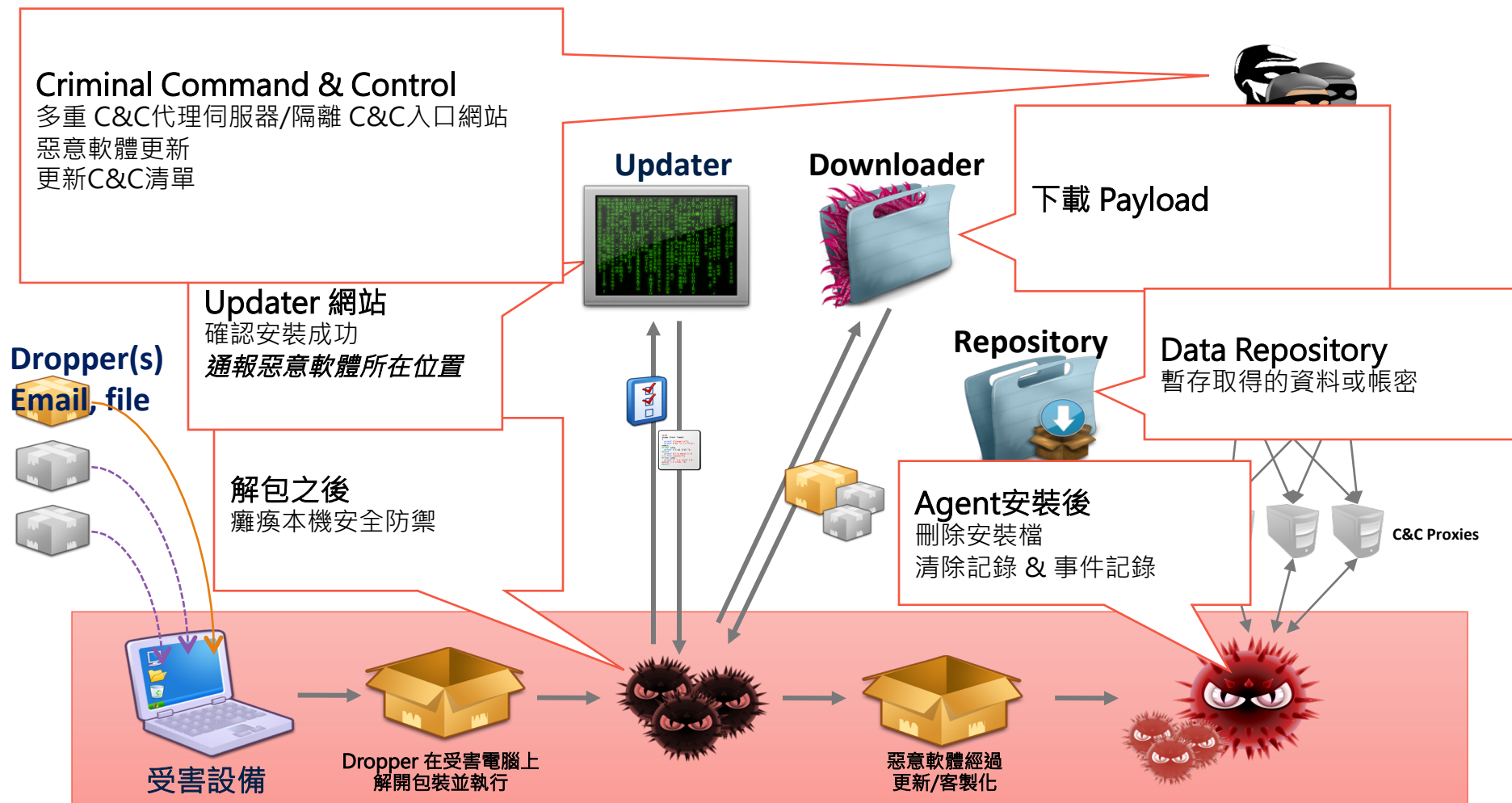
② 辨識威脅等級與類別
提供建議處理順序



③ 專業人員按照順序於
惡意威脅尚未爆發前
好整以暇地解除危機

惡意威脅是可以預警的？

如果您知道要找什麼行為跡證



網路攻擊鍊 - 無法防禦的40%



一旦防禦失敗，後續的修復將會和時間賽跑

專家這麼說，但有限的資源應該放在1天、187天、49天？



<1 day



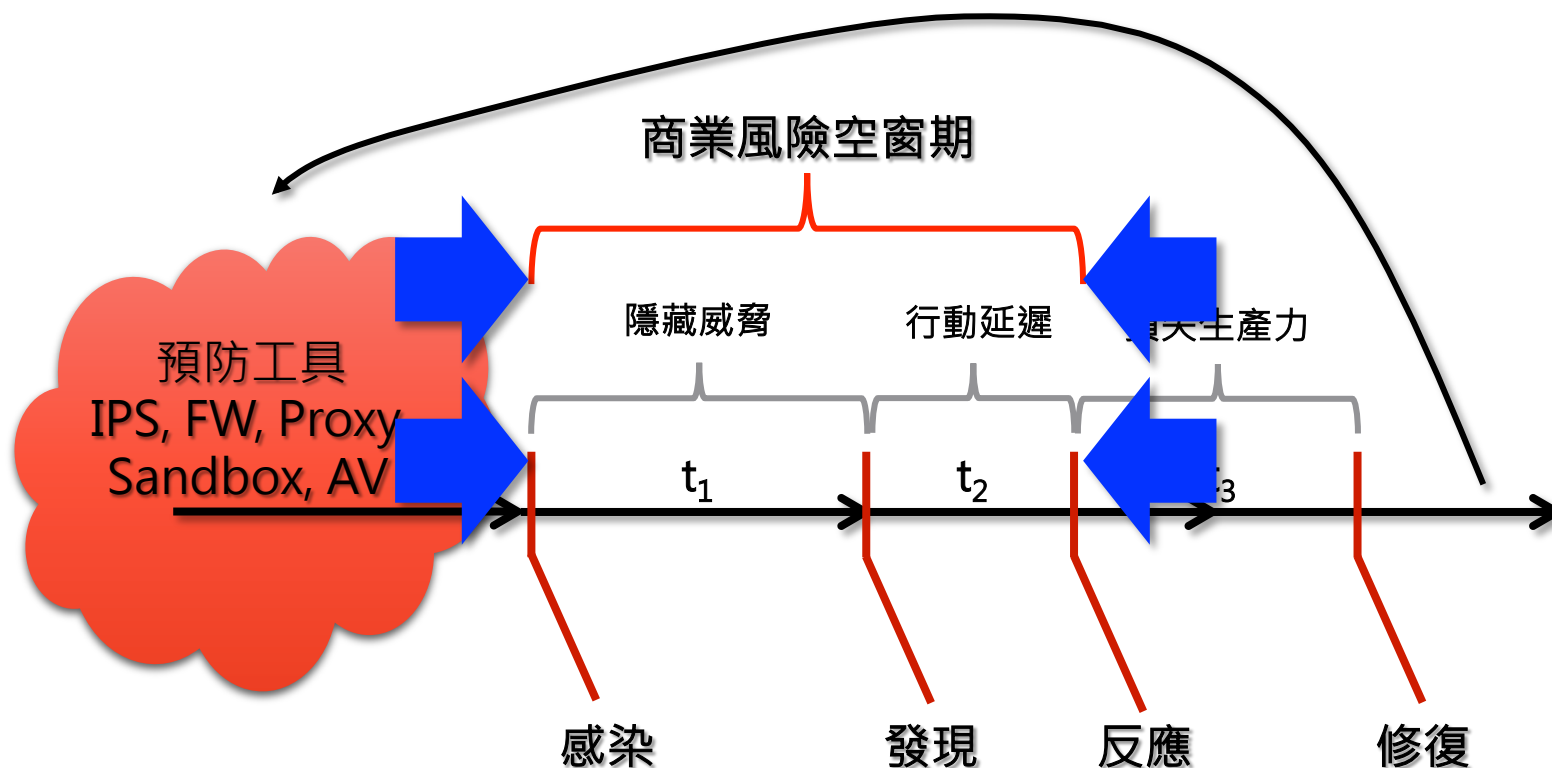
187 days



49 days

潛伏的威脅是可以被預警的，如果你知道要找什麼行為跡證

早期預警系統的商業價值何在？



1. 阻止惡意威脅於未然

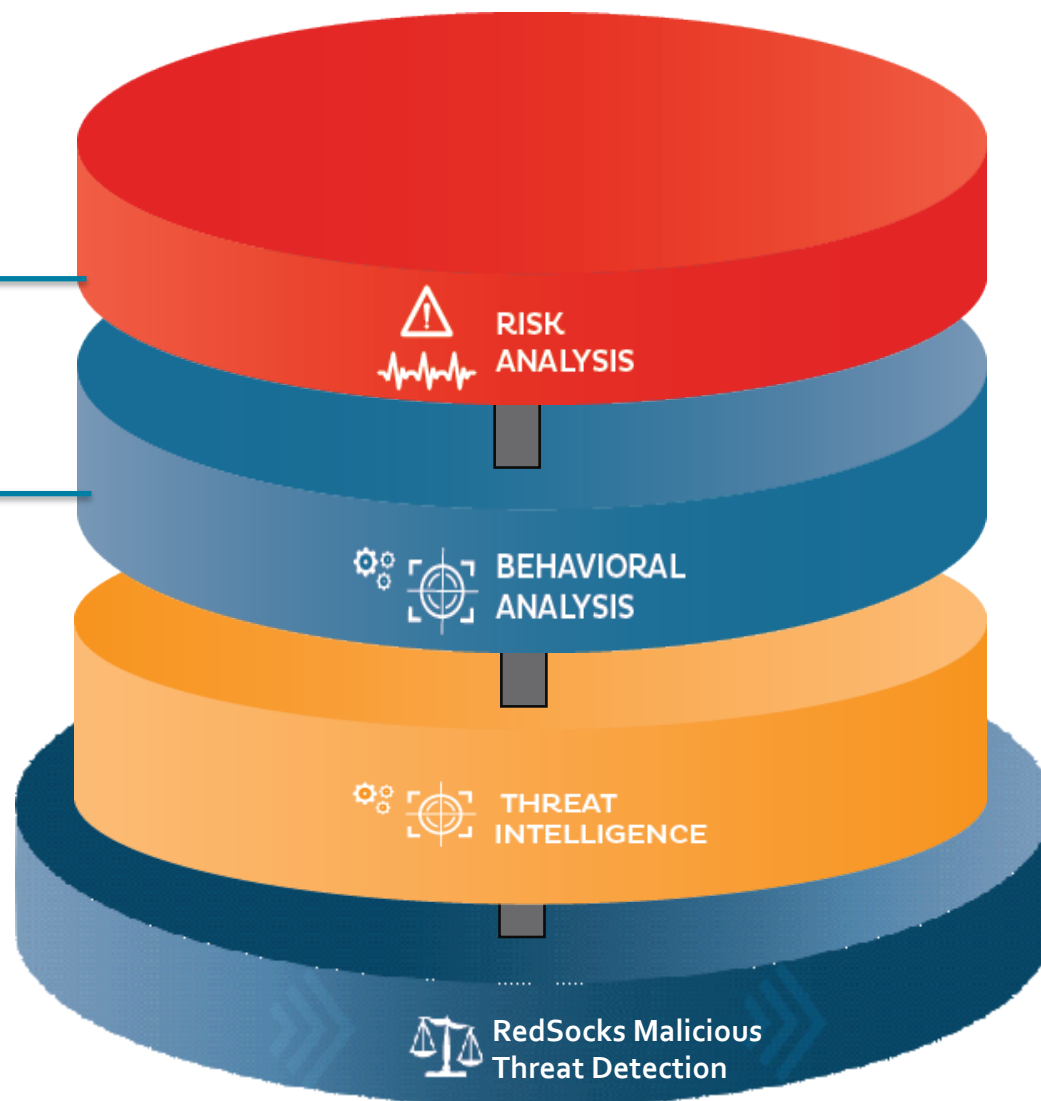
2. 依“現況”正確擬定資安策略

早期預警雷達



9種
風險等級

39+類
網路行為
雷達偵測

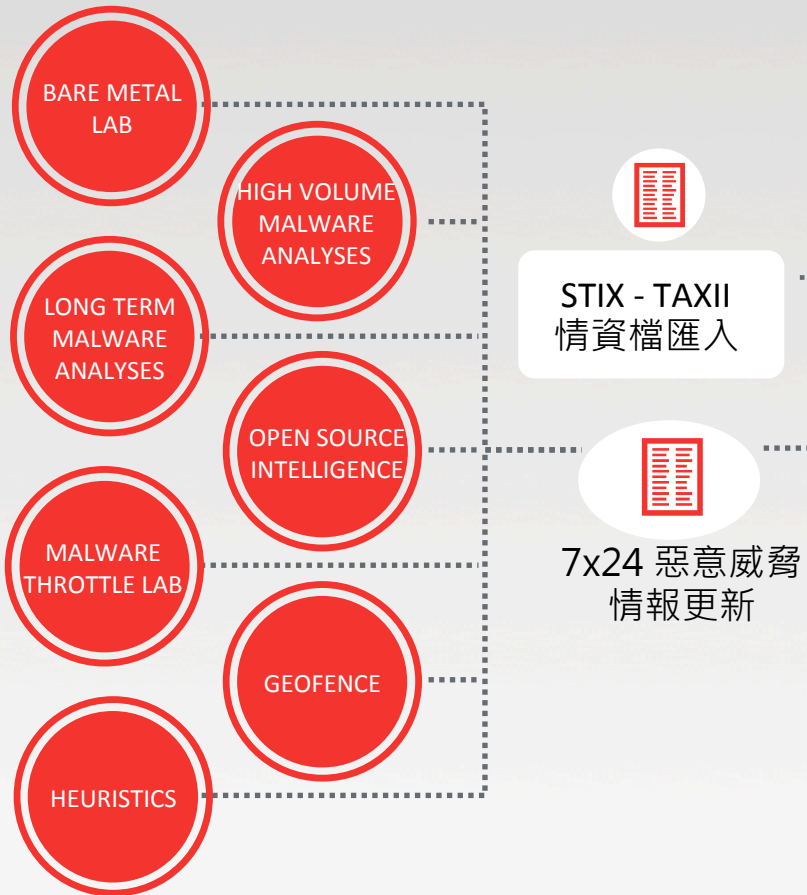


- ①
 - ✓ Blacklisted hostnames and URLs
 - ✓ Botnet Controller
 - ✓ Malware-specific behavioral heuristics
 - ✓ Sinkhole
 - ✓ TOR Network
- ②
 - ✓ Disguised executable file
 - ✓ Experimental
 - ✓ Mining Pool
 - ✓ Miscellaneous
 - ✓ Path traversal
 - ✓ Periodic heartbeat
 - ✓ Port scan
 - ✓ Web shells
- ③
 - ✓ Adware
 - ✓ Bad Internet Neighbourhood
 - ✓ BitTorrent tracker
 - ✓ Cloud Storage Service
 - ✓ File sharing
 - ✓ File sharing Tool
 - ✓ Instant Messaging
 - ✓ Public Proxy
 - ✓ Remote Administration
 - ✓ Geofence (Syrian, Iran, Nigeria, Romania, Ukraine, Indonesia, China...)
- ④
 - ✓ Domain Parker (DGA)
 - ✓ Dynamic DNS domains
 - ✓ Free hosting domains
 - ✓ IP Self Check Service
 - ... More...

RedSocks Malicious Threat Detection 運作方式

RedSocks 威脅情資實驗室

>39+ 種網路行為分析
>100.000 每小時持續更新



公司內部網路

導入 RedSocks Malicious Threat Detection



PROBE
MNGT & FLOW DATA / IPFIX



Malicious Threat Detection (MTD)



數位鑑識儲存庫
網路行為長期保留備查

網際網路

熱門網站
惡意電子郵件





實務案例的探討分析

案例探討分析① – Domain Parker



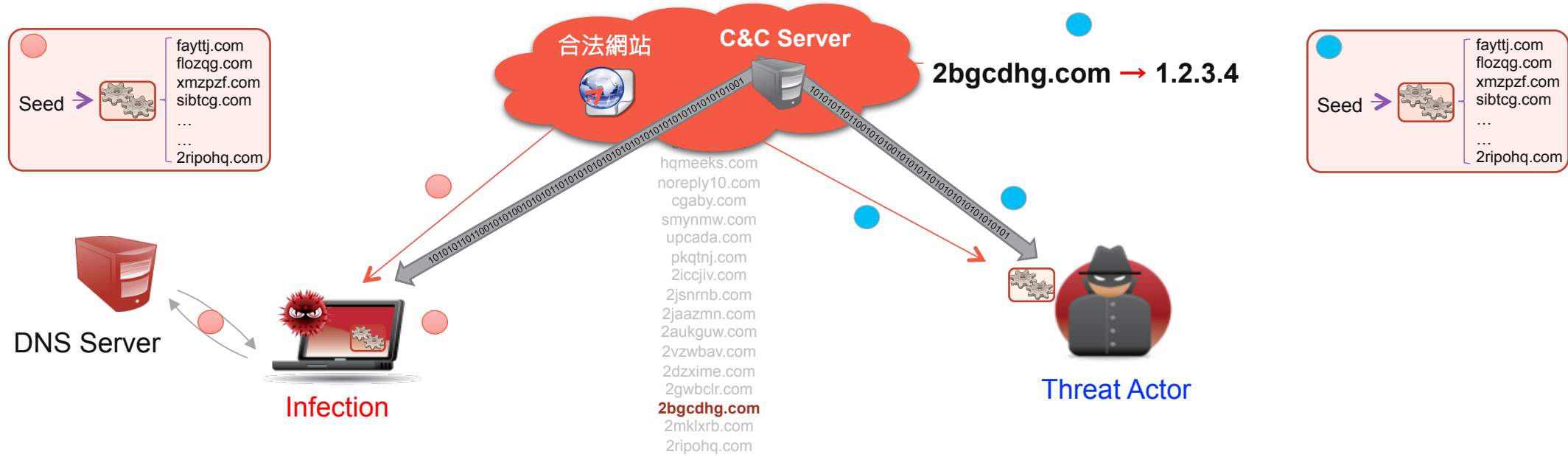
Domain Parker – 5 Infected device

Domain parkers are IP's which host expired domains. Recurring connections to domain parkers can indicate infection with malware.

端點	感染類別 Level 5
10.80.1.113 172.16.121.171 10.80.199.122 10.80.142.46 10.80.80.56	Domain Parker

Timestamp (GMT+0800)		Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail
Wed Dec 20 2017 15:45:44	5	Domain Parker	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.1.113	3699	184.168.221.40	27433	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 15:21:16	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.121.171	49548	5.39.99.50	80	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 15:20:29	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.121.171	49540	204.11.56.48	80	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:45:10	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.199.122	54152	50.63.202.91	80	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:32:04	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.142.46	63683	185.53.179.8	443	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:32:04	5	Domain Parker	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.142.46	63684	185.53.179.8	443	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:29:54	5	Domain Parker	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.80.56	52087	209.99.40.223	80	TCP	RSMIT - Expired Domain Parking IP

DGA(Domain Fluxing) and Domain Parker



- Infection seeks a 'Seed' (e.g. cnn.com for date)
- Seed is entered into DGA, generating pseudo-random domains (e.g. 1000 domains)
- Infection queries Domains, seeking one with an IP
- Infection connects to domain with an IP, communicates with threat actor
- Cycle begins again

- Threat Actor seeks a 'Seed' (e.g. cnn.com for date)
- Seed is entered into DGA, generating pseudo-random domains (e.g. 1000 domains)
- Threat actor registers one domain, with an IP
- Infection connects to domain with an IP, threat actor communicates with infection
- Cycle begins again

案例探討分析② – Sinkhole



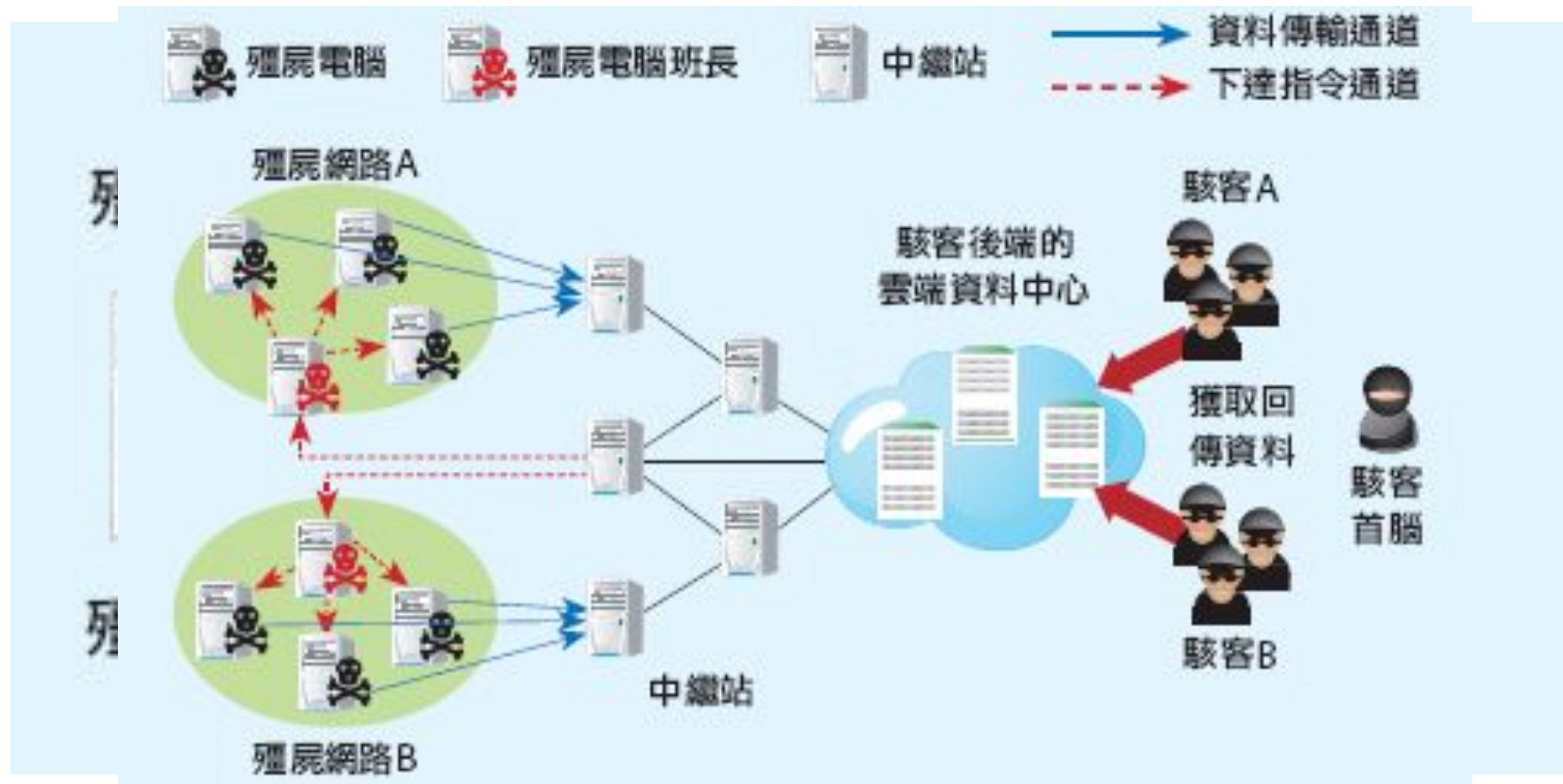
Sinkhole – 4 Infected device

Malware is active on your client's system, but the controller IP has been seized or diverted in order to disable the botnet. The infected client still tries to connect to it and, therefore, a breach and an infection occurred in the past.

端點	感染類別 Level 1
10.80.153.128 10.80.130.59 10.80.148.63 10.80.239.10	Sinkhole

Timestamp (GMT+0800)		Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail
Thu Dec 21 2017 10:24:19	1	Sinkhole	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.153.128	1315	193.166.255.171	41801	UDP	RSMIT - FitSec Malware Sinkhole (sinkhole.fitsec.c...
Thu Dec 21 2017 10:23:49	1	Sinkhole	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.153.128	1314	23.253.126.58	41801	UDP	RSMIT - Arbor Networks Malware Sinkhole
Thu Dec 21 2017 10:15:58	1	Sinkhole	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.130.59	4067	193.166.255.171	41801	UDP	RSMIT - FitSec Malware Sinkhole (sinkhole.fitsec.c...
Thu Dec 21 2017 10:15:28	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.130.59	4031	23.253.126.58	41801	UDP	RSMIT - Arbor Networks Malware Sinkhole
Thu Dec 21 2017 10:14:12	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.148.63	49502	204.95.99.243	3720	TCP	RSMIT - Malware Sinkhole (Microsoft DDNS Take...
Thu Dec 21 2017 10:12:50	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.239.10	50396	204.95.99.109	80	TCP	RSMIT - Malware Sinkhole (Microsoft DDNS Take...
Thu Dec 21 2017 10:08:27	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.130.59	3925	193.166.255.171	41801	UDP	RSMIT - FitSec Malware Sinkhole (sinkhole.fitsec.c...

殭屍網路與 Sinkhole





Bad Hood & Ming Pool – 3 Infected device

These IP-addresses are frequently used in targeted attacks, phishing/pharming campaigns or as Botnet Controllers.

Cryptocurrencies are generated by users who offer their CPU or GPU power to calculate complex algorithms

A mining pool occurs when multiple people combine computing resources to produce cryptocurrencies. Malware writers are always looking for ways to make money and illicitly using your computer to generate cryptocurrencies pays off. In addition to malware, mining can also be done by personnel who uses resources for personal benefit. An alert in this category should warrant further investigation.

端點	感染類別 Level 3
172.16.36.19 172.16.142.28 172.16.134.108	Bad Hood Ming Pool

Timestamp (GMT+0800)	TL	Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail	
Thu Dec 21 2017 10:15:21	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	43110	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...	
Thu Dec 21 2017 09:51:10	3	Bad Hood	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.142.28	39526	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...	
Thu Dec 21 2017 09:31:59	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	42676	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...	
Thu Dec 21 2017 09:00:02	3	Bad Hood	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.134.108	50014	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...	
Thu Dec 21 2017 08:59:59	3	Bad Hood	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.134.108	44125	49.4.20.52	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...	
Thu Dec 21 2017 08:44:09	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	42608	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...	
Thu Dec 21 2017 07:57:40	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	42590	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...	

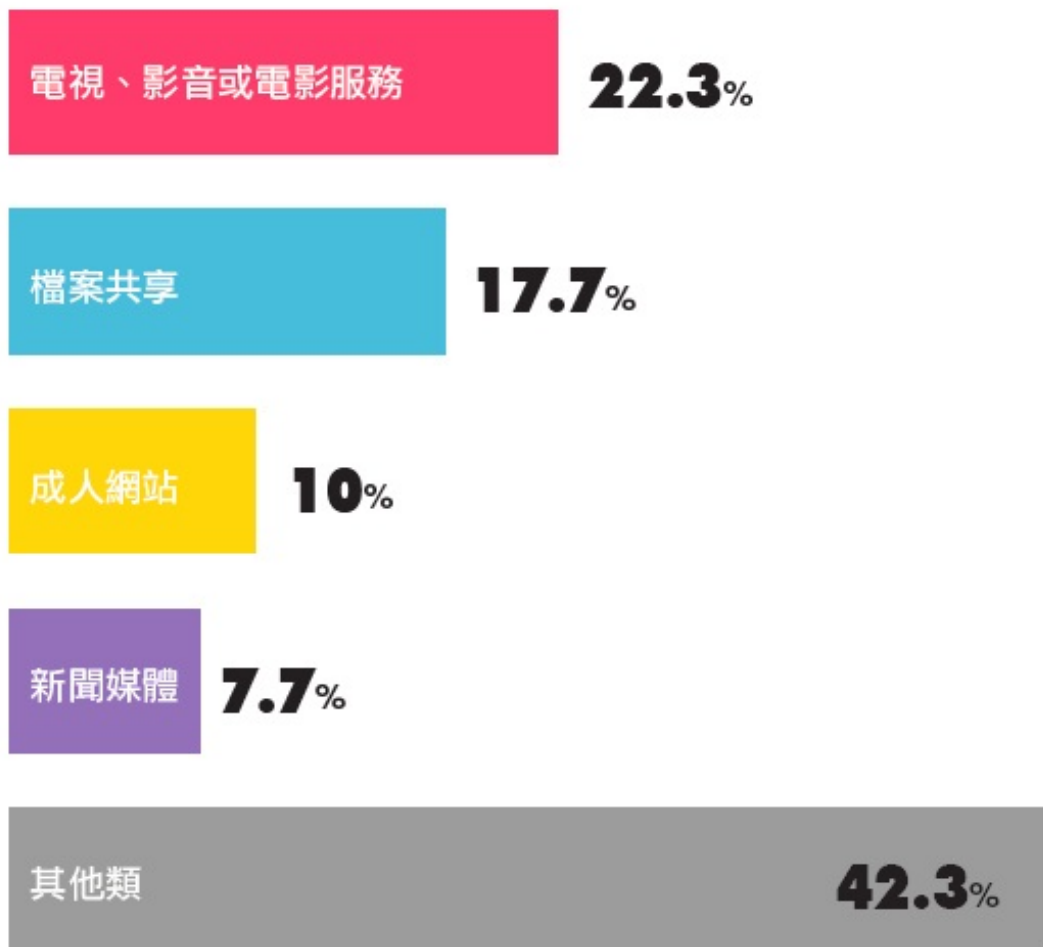
盜用電腦資源挖礦



挖礦網站來源



挖礦網站類型分布



資料來源：AdGuard · 2017年10月12日 · iThome整理

案例探討分析④ – TOR Network



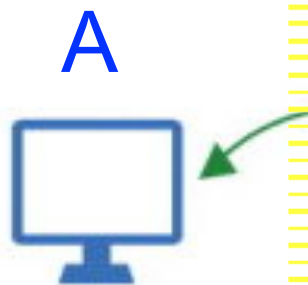
TOR Network – 2 Infected device

The Tor Network is designed to offer anonymous Internet access to its users and can also be used to hide a Botnet Controller. Anonymous access could be used as a means to subvert company usage policy or even engage in illicit activity. Since mid-2013, the Tor Network has been used by an increasing number of operators to hide communications with Botnet Controllers. If not initiated by an employee, then an infection is present within your network. An alert in this category should be investigated at all times.

端點	感染類別 Level 1
172.16.126.71 172.16.126.14	TOR

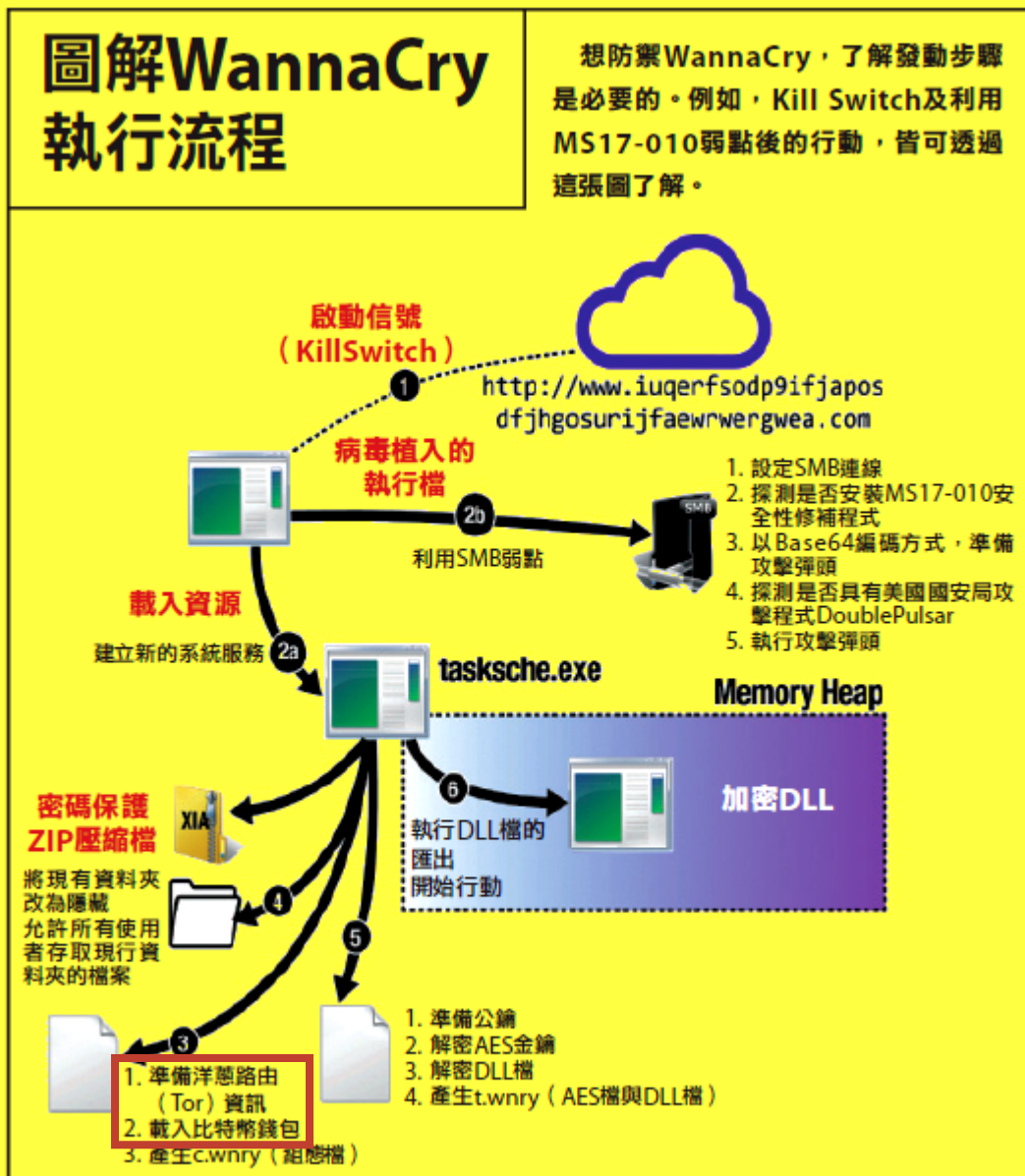
Timestamp (GMT+0800)	▼ TL	Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail	▼
Wed Dec 20 2017 12:39:26	1	Tor	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.126.71	51238	62.210.244.146	9001	TCP	RSMIT - Tor Connecting IP - Country FR - hxxp://6...	
Wed Dec 20 2017 11:54:09	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.71	51230	136.243.243.6	1444	TCP	RSMIT - Tor Connecting IP - Country DE - hxxp://t...	
Wed Dec 20 2017 11:54:09	1	Tor	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.126.71	51227	146.0.77.50	443	TCP	RSMIT - Tor Connecting IP - Country NL	
Wed Dec 20 2017 10:06:42	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.71	49447	178.16.208.57	443	TCP	RSMIT - Tor Connecting IP - Country SE - hxxp://b...	
Mon Dec 18 2017 18:43:41	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.14	52722	77.68.11.42	9001	TCP	RSMIT - Tor Connecting IP - Country GB	
Mon Dec 18 2017 13:54:11	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.14	50238	91.121.23.100	9001	TCP	RSMIT - Tor Connecting IP - Country FR - hxxp://0...	
Mon Dec 18 2017 13:41:55	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.14	55805	128.31.0.39	9101	TCP	RSMIT - Tor Connecting IP	

TOR (洋蔥路由)網絡運作原理



A 的 TOR 軟體會自動選擇隨機路徑並抵達伺服器 B

B 看到的來源只會是上一個來源位址



B



No recovery e-mail address has been set for your account.

ALERTS

Dashboard

History

Analysis

Alert Dashboard - Latest Alerts

Flows analyzed: 20480030

Timestamp	TL	Category	Exporter IP	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail
Thu 3月 1 2018 14:28:07	TL 3	IM	::ffff:ac8:c8c8	1	84:b8:02:c7:4a:bf	192.168.12.15	3392	203.104.150.2	443	TCP	RSMIT - Line Messenger
Thu 3月 1 2018 14:28:05	TL 4	Geofence	::ffff:ac8:c8c8	1	00:15:5d:08:b9:05	192.168.10.245	61378	202.102.128.69	53	UDP	location: China (CN); Asia (AS), registered: China (CN)
Thu 3月 1 2018 14:28:02	TL 4	Geofence	::ffff:ac8:c8c8	1	00:15:5d:08:b9:05	192.168.10.245	60573	210.68.80.1	53	UDP	location: China (CN); Asia (AS), registered: Taiwan (TW)
Thu 3月 1 2018 14:28:00	TL 1	Sinkhole	::ffff:ac8:c8c8	1	00:15:5d:09:ba:00	192.168.8.245	2450	1.1.1.1	135	TCP	RSMIT - Google Malware Sinkhole - Occasionally causes FP's due to misconfigured devices
Thu 3月 1 2018 14:27:57	TL 4	Geofence	::ffff:ac8:c8c8	1	88:5a:92:64:9f:c0	192.168.20.206	22	185.165.31.79	44497	TCP	location: Iran (IR); Asia (AS), registered: Iran (IR)
Thu 3月 1 2018 14:27:56	TL 3	IM	::ffff:ac8:c8c8	1	bc:ae:c5:23:e6:31	192.168.11.118	62202	203.104.153.7	443	TCP	RSMIT - Line Messenger
Thu 3月 1 2018 14:27:50	TL 4	Geofence	::ffff:ac8:c8c8	1	00:15:5d:08:b9:05	192.168.10.245	61070	218.30.26.70	53	UDP	location: China (CN); Asia (AS), registered: China (CN)
Thu 3月 1 2018 14:27:49	TL 4	Geofence	::ffff:ac8:c8c8	1	00:15:5d:08:b9:05	192.168.10.245	60456	119.188.67.105	53	UDP	location: China (CN); Asia (AS), registered: China (CN)
Thu 3月 1 2018 14:27:48	TL 4	Geofence	::ffff:ac8:c8c8	1	00:15:5d:09:ba:00	192.168.8.245	63797	220.181.126.35	53	UDP	location: China (CN); Asia (AS), registered: China (CN)
Thu 3月 1 2018 14:27:45	TL 4	Geofence	::ffff:ac8:c8c8	1	00:15:5d:09:ba:00	192.168.8.245	56686	111.206.53.6	53	UDP	location: China (CN); Asia (AS), registered: China (CN)

RedSocks 威脅分析 ① - 直覺式高風險排序



RED SOCKS

ADMIN

No recovery e-mail address has been set for your account.

Alerts

Dashboard

History

Analysis

Alert Analysis

192.168.16.107	c1	.tw	::ffff:ac8:c8c8	1	52	0	0	29
192.168.16.119	c2	.tw	::ffff:ac8:c8c8				409	54
192.168.9.209	mi	tw	::ffff:ac8:c8c8	1			372	295
192.168.11.118	e1	.tw	::ffff:ac8:c8c8	1			358	1
192.168.10.216			::ffff:ac8:c8c8	1			321	67
192.168.17.164	b2	.tw	::ffff:ac8:c8c8	1			244	1613
192.168.10.215			::ffff:ac8:c8c8	1			307	161
192.168.13.141	c3	.tw	::ffff:ac8:c8c8	1	33	0	0	0
192.168.14.140	d1	.tw	::ffff:ac8:c8c8	1		98	0	0
192.168.17.109			::ffff:ac8:c8c8	1	23	0	41	571
192.168.9.105			::ffff:ac8:c8c8	1			1	6031
192.168.40.52	e3	.tw	::ffff:ac8:c8c8	1			233	224
192.168.18.102	ps	.tw	::ffff:ac8:c8c8	1			234	4
192.168.12.15	c3	.tw	::ffff:ac8:c8c8	1			222	39
192.168.14.248	d1	om.tw	::ffff:ac8:c8c8	1		63	0	0
192.168.13.125	a1	.tw	::ffff:ac8:c8c8	1	20	0	0	2

RedSocks威脅分析 ② - C&C詳細通聯紀錄



REDSOCKS

ADMIN

No recovery e-mail address has been set for your account.

ALERTS

[Dashboard](#)

[History](#)

[Analysis](#)

Alert Analysis

192.168.10.203	::ffff:ac8:c8c8	1			5		
192.168.16.107	c11	w	::ffff:ac8:c8c8	1	52	0	0
192.168.16.119	c2	w	::ffff:ac8:c8c8	1			409
192.168.9.209	mi	v	::ffff:ac8:c8c8	1			372
192.168.11.118	e1	w	::ffff:ac8:c8c8	1			358
192.168.10.216			::ffff:ac8:c8c8	1			322
192.168.17.164	b2	w	::ffff:ac8:c8c8	1			244
192.168.10.215			::ffff:ac8:c8c8	1			307
192.168.13.141	c3	w	::ffff:ac8:c8c8	1	33	0	0
192.168.14.140	d1	w	::ffff:ac8:c8c8	1		98	0
192.168.17.109			::ffff:ac8:c8c8	1	23	0	41
192.168.9.105			::ffff:ac8:c8c8	1			1
192.168.40.52	e3	w	::ffff:ac8:c8c8	1			233
192.168.18.102	ps		::ffff:ac8:c8c8	1			234
192.168.12.15	c3	w	::ffff:ac8:c8c8	1			222
192.168.14.248	d1		::ffff:ac8:c8c8	1		63	0
192.168.13.125	a1	w	::ffff:ac8:c8c8	1	20	0	0
192.168.40.125	c1	w	::ffff:ac8:c8c8	1			177
192.168.20.206			::ffff:ac8:c8c8	1			7

[Back](#)

Source IP
192.168.16.107

Exporter IP
::ffff:ac8:c8c8

ODID
1

Dismiss Existing Alerts From This Source

Threat level All 52 29

Status	Time	Destination	Category	TL
?	Tue 2月 27 2018 11:32:36	160.153.47.192	URL blacklist	TL 1
?	Tue 2月 27 2018 08:52:56	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:42:08	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:24:36	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:05:54	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:42:20	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:27:09	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:09:38	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 15:52:25	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 15:33:30	160.153.47.192	URL blacklist	TL 1

[« First](#) [« Previous](#) Page 1 of 9 [Next »](#) [Last »](#)

Cyberview 力悅資訊

RedSocks威脅分析 ③ - 威脅分析



REDSOCKS

ADMIN

No recovery e-mail address has been set for your account.

ALERTS

[Dashboard](#)

[History](#)

[Analysis](#)

Alert Analysis

[Back](#)

Source IP
192.168.16.107

Exporter IP
::ffff:ac8:c8c8

ODID
1

Dismiss Existing Alerts From This Source

Threat level

All

52

29

Status	Time	Destination	Category	TL
	Tue 2月 27 2018 11:32:36	160.153.47.192	URL blacklist	TL 1
	Tue 2月 27 2018 08:52:56	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 17:42:08	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 17:24:36	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 17:05:54	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 16:42:20	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 16:27:09	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 16:09:38	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 15:52:25	160.153.47.192	URL blacklist	TL 1
	Mon 2月 26 2018 15:33:30	160.153.47.192	URL blacklist	TL 1

[« First](#) [« Previous](#) [Page 1 of 9](#) [Next »](#) [Last »](#)

X Alert Details

Description: RSMIT - Blocker Ransom Trojan URL Request - hxxp://timeshargroup.com/wp-admin/includes/class-wip.txt
Time: 2018-02-27 11:32:36 (CST)
Category: URL blacklist
Threat level: 1
Protocol: TCP

Data Source

Exporter IP address: ::ffff:ac8:c8c8
Observation domain ID: 1

Source

IP address: 192.168.16.107 (c11[redacted]com.tw)
MAC address: 84:b8:02:c7:4a:bf (Cisco)
Port: 3869

Destination

IP address: 160.153.47.192 (ip-160-153-47-192.ip.secureserver.net)
Port: 80

[Copy to clipboard](#)

[Show flow data](#)

[Look up destination at VirusTotal](#)

[Whitelist similar alerts](#)

RedSocks威脅分析 ④ - 完整通聯紀錄



REDSOCKS

ADMIN

No recovery e-mail address has been set for your account.

ALERTS

Dashboard

History

Analysis

Alert Analysis

Back

Source IP

192.168.16.107

Exporter IP

::ffff:ac8:c8c8

ODID

1

Dismiss Existing Alerts From This Source

Threat level

All

52

29

Status	Time	Destination	Category	TL
?	Tue 2月 27 2018 11:32:36	160.153.47.192	URL blacklist	TL 1
?	Tue 2月 27 2018 08:52:56	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:42:08	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:24:36	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:05:54	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:42:20	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:27:09	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:09:38	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 15:52:25	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 15:33:30	160.153.47.192	URL blacklist	TL 1

First

Previous

Page 1 of 9

Next

Last

Show alert details

Time	Source IP	Port	Destination IP	Port	Protocol	TCP flags	Packets	Bytes	Host
11:32:36	192.168.16.107	3869	160.153.47.192	80	TCP	.APRSF	12	1.0 KB	timeshare
11:32:35	192.168.16.107	62087	172.217.24.14	443	UDP		15	5.0 KB	
11:32:30	192.168.16.107	3867	172.217.160.74	443	TCP	.AP.S.	6	547.0 B	www.googl
11:32:30	192.168.16.107	49732	172.217.160.74	443	UDP		9	3.0 KB	
11:32:30	192.168.16.107	49731	172.217.160.98	443	UDP		6	3.0 KB	
11:32:28	192.168.16.107	64793	216.58.200.34	443	UDP		6	2.0 KB	
11:32:28	192.168.16.107	64792	172.217.24.4	443	UDP		7	2.0 KB	
11:29:53	192.168.16.107	3696	219.80.60.208	1352	TCP	.AP...	2	96.0 B	
11:27:40	192.168.16.107	55285	172.217.24.3	443	UDP		1	51.0 B	
11:26:34	192.168.16.107	3823	219.80.60.208	1352	TCP	.AP.SF	7	538.0 B	
11:23:26	192.168.16.107	3767	172.217.24.10	443	TCP	.A.R.F	7	280.0 B	
11:21:26	192.168.16.107	3767	172.217.24.10	443	TCP	.A....	1	40.0 B	

Cyberview
力悅資訊

RedSocks威脅分析 ④ - 殭屍就在您我之間



ADMIN

No recovery e-mail address has been set for your account.

ALERTS

Dashboard

History

Analysis

Alert Analysis

← Back

Source IP

192.168.16.107

Exporter IP

::ffff:ac8:c8c8

ODID

1

Dismiss Existing Alerts From This Source

Threat level

All

52

29

Status	Time	Destination	Category	TL
?	Tue 2月 27 2018 11:32:36	160.153.47.192	URL blacklist	TL 1
?	Tue 2月 27 2018 08:52:56	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:42:08	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:24:36	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 17:05:54	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:42:20	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:27:09	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 16:09:38	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 15:52:25	160.153.47.192	URL blacklist	TL 1
?	Mon 2月 26 2018 15:33:30	160.153.47.192	URL blacklist	TL 1

« First

« Previous

Page 1 of 9

Next »

Last »

X

Show alert details

Time	Source IP	Port	Destination IP	Port	Protocol	TCP flags	Packets	Bytes	Host
11:32:36	192.168.16.107	3869	160.153.47.192	80	TCP	.APRSF	12	1.0 KB	timeshare
11:32:35	192.168.16.107	62087	172.217.24.14	443	UDP		15	5.0 KB	
11:32:30	192.168.16.107	3867	172.217.160.74	443	TCP	.AP.S.	6	547.0 B	www.googl
11:32:30	192.168.16.107	49732	172.217.160.74	443	UDP		9	3.0 KB	
11:32:30	192.168.16.107	49731	172.217.160.98	443	UDP		6	3.0 KB	
11:32:28	192.168.16.107	64793	216.58.200.34	443	UDP		6	2.0 KB	
11:32:28	192.168.16.107	64792	172.217.24.4	443	UDP		7	2.0 KB	
11:29:53	192.168.16.107	3696	219.80.60.208	1352	TCP	.AP...	2	96.0 B	
11:27:40	192.168.16.107	55285	172.217.24.3	443	UDP		1	51.0 B	
11:26:34	192.168.16.107	3823	219.80.60.208	1352	TCP	.AP.SF	7	538.0 B	
11:23:26	192.168.16.107	3767	172.217.24.10	443	TCP	.A.R.F	7	280.0 B	
11:21:26	192.168.16.107	3767	172.217.24.10	443	TCP	.A....	1	40.0 B	

Cyberview
力悅資訊



- 1、資安功能 VS 資安產品
- 2、公司官網淪為惡意程式下載點、C&C、Botnet
(主動攻擊C&C是否可行？)
- 3、平均感染率2%(台灣>全球平均)
- 4、DC (兵家必爭之地)

與眾不同的特點



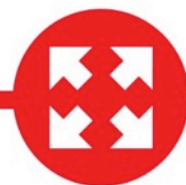
市場最佳威脅情資



快速即時



非侵入式



大規模擴充



最大隱私權



歐盟資料保護規範

- 任何協定與埠號，包含加密
- 不影響網路、大規模分散式佈建
- 時光回溯
- 紀錄所有通聯
- 零誤判
- 上線立即產生效益



彈性的商業模式



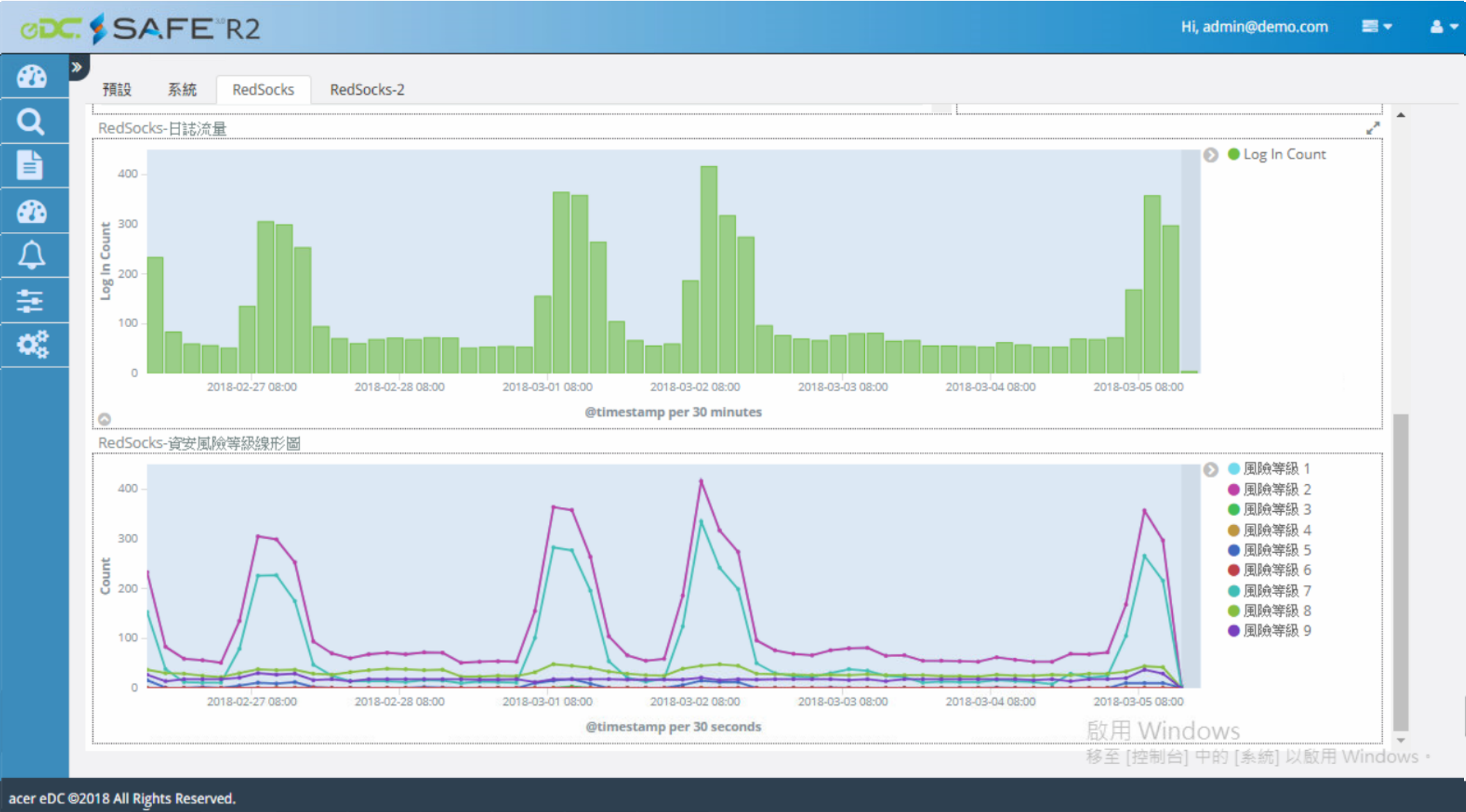
- 軟體建置長期分析
 - 持續且深入的資訊安全預警系統
 - 保持即時的威脅情資更新
 - 可依照彈性安排優先處理順序
- 短期資訊安全顧問服務
 - 為期四週的網路行為收集分析
 - 專業的資訊安全顧問深度剖析
 - 實証為資訊安全政策提供正確方向



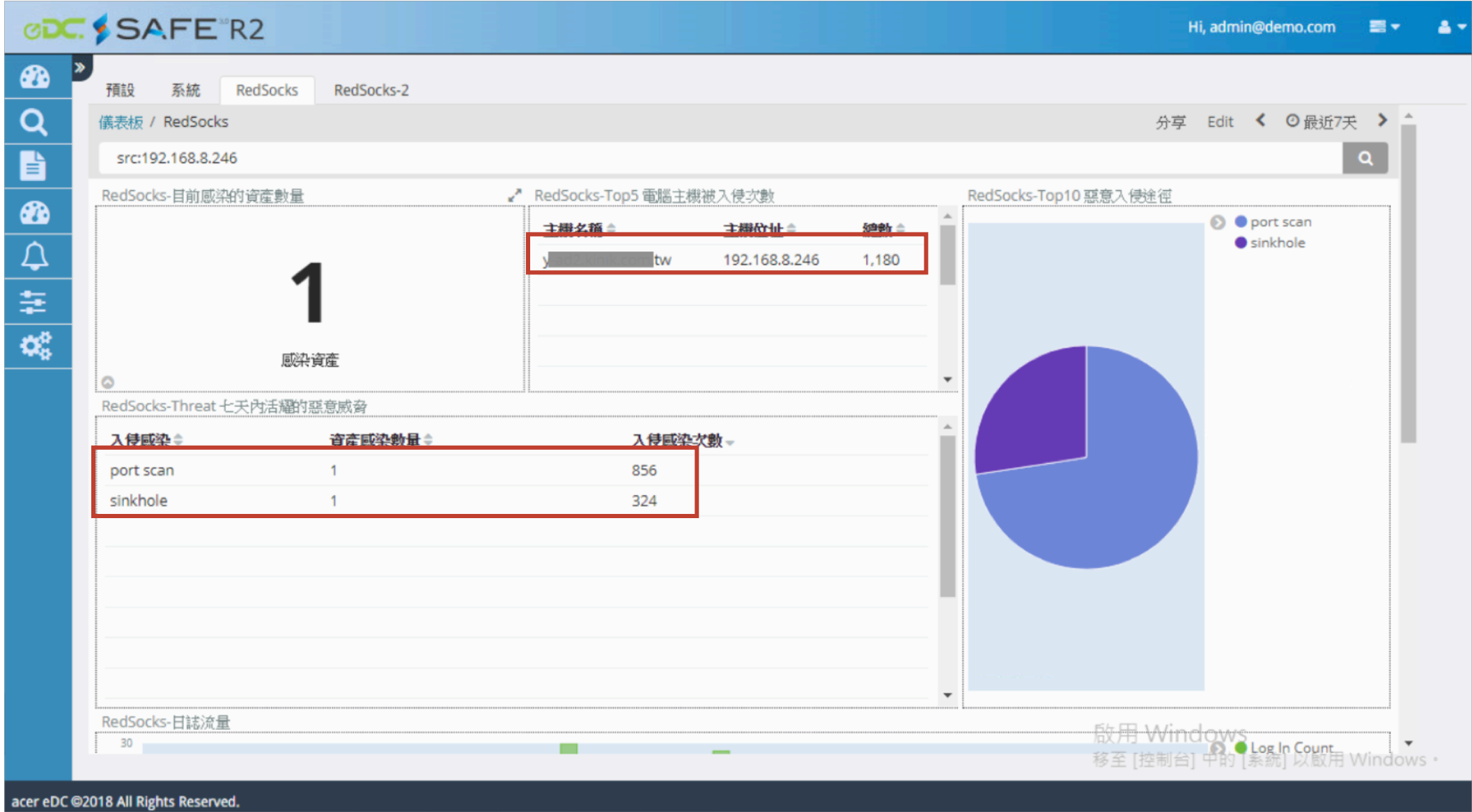


One more thing...

與宏碁雲架構合作強化預警系統



與宏碁雲架構合作強化預警系統－端點感染情況



與宏碁雲架構合作強化預警系統－高風險威脅感染情況

