

NAR
WHT
RATE
21/117
1138
10C

ACFT
N 51' 30' 9.352"
W 0' 0' 54.761"
1,337 HAT

數位偵察機

從駭客視角掌握企業資安防線

38

N 51' 30' 10.684"
W 0' 0' 51.522"
BRG 61
RNG 5116m
RNG 2,762 NM
ELV 6224-F

Kevin Tang 2018/3/1

外部資安防線偵察機 - RiskIQ

#1

Leadership

200+

Enterprise
Customers

18k+

Security
Analysts

150+

Employees

- 外部數位威脅管理的領導品牌
- 位於舊金山，成立於2009年
- 知名創投
Summit Partners, Battery Ventures,
Georgian Partners, MassMutual Ventures

FORRESTER®

WAVE LEADER
2016

Digital Risk Monitoring



An iceberg floating in a blue ocean under a blue sky with white clouds. The top part of the iceberg is visible above the water, while the much larger bottom part is submerged. The text 'Visibility 能見度' is overlaid on the submerged part of the iceberg.

Visibility 能見度

您有多少外部數位資產？

- 據RiskIQ客戶資料統計，導入RiskIQ的服務後，平均發現多出了**30%**的數位資產，這都是在過去確實存在卻不為客戶所知的。

您如何對不知道其存在的資產進行防護？

防火牆有些什麼？



External Threats / Rogue
Partner Websites, Mobile Applications, Social, and Integrations
Unknown Websites & Mobile Applications (Shadow IT)
Official Websites & Mobile Applications
Firewall



RiskIQ幫助您...

找到茫茫網海中與您相關的數位資產

已知

未知

偽冒

Knowing is the Best Defense.

數位化時代 - 客戶互動模式

數位化與虛擬化

**Online
Interactions**

**Well Connected
Departments**

**Simple
Applications**

**Real-Time
Status Updates**

Mobile Access

**Personalized
Products**

#Support

**Cashless
Transactions**

**Well Timed
Advice**

企業開始投入各種數位頻道



Websites



Web Apps



Mobile Apps



Social Profiles

電腦罪犯也是...

勒索軟體	Up 11x y/y
釣魚	155k sites FY16
惡意軟體	2000+ / day Q3-16
品牌濫用	2,754+ cases FY16
流氓App	Up 135% y/y
偽冒社群帳號	83M (Facebook)
惡意廣告	Up 136% y/y

透過未妥善管理的外部數位資產進行入侵；偽冒值得信賴的品牌、商標及社交資訊對用戶進行詐騙

電腦罪犯的新戰場

Easy to Attack

vs. Difficult to Attack Directly

90%

行動App放在非官方、
無完善審核機制的App市集

10%

行動App在擁有其企業
的完全掌控下

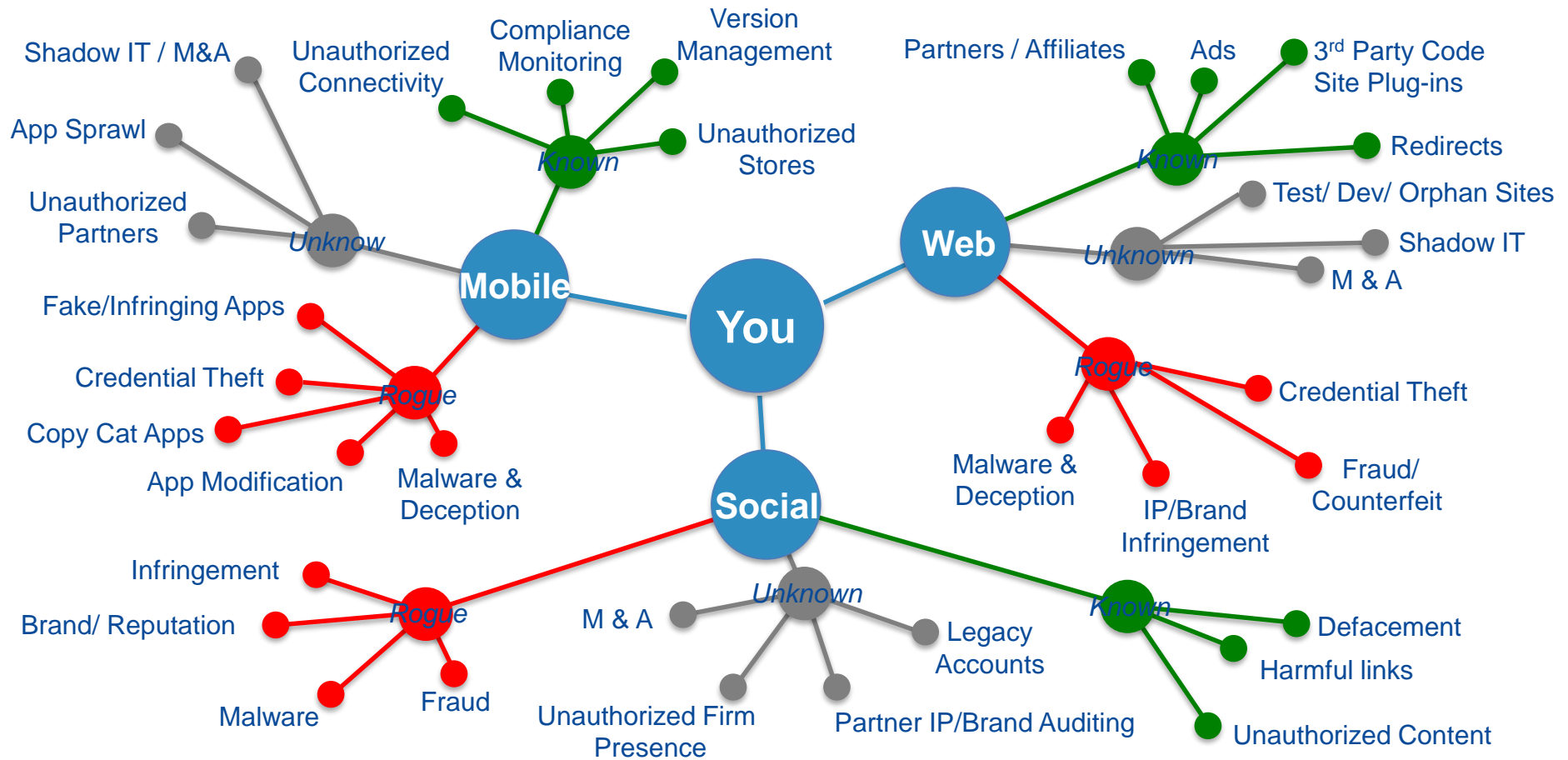
RiskIQ's Q2 2017 Mobile Threat Landscape Report

外部戰線持續擴大

- Website, Microsite
- Mobile Apps
- Forgotten, Abandoned Properties
- Test Servers
- Social Media Properties



Attack Surface



防火牆外的安全議題浮現



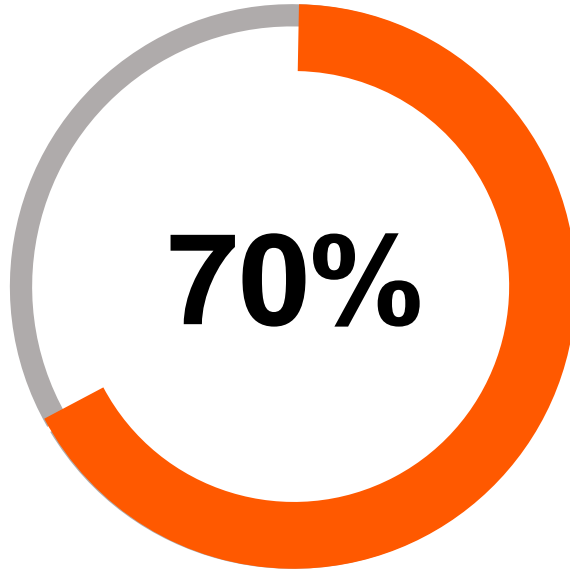
75%

資料洩漏的突破口
來自外部威脅



74%

無法找出
發起攻擊的
外部威脅為何



70%

缺乏縮小
受攻擊面(Attack Surface)
的有效方法

Verizon Data Breach Investigations Report (2017)
The SANS Continuous Monitoring Survey (2016)

? 攻擊者在忙些什麼？

北韓駭客「水坑式攻擊」 搶劫國際大型銀行



駭客先在金融監管機構網站植入病毒（JavaScript或HTML編碼），當訪客造訪網頁時，就會被引導到另一個偽造的惡意網站，下載惡意軟體的程式。

原文網址: [北韓駭客「水坑式攻擊」搶劫國際大型銀行 | ETtoday國際 | ETtoday新聞雲](https://www.ettoday.net/news/20170328/893559.htm#ixzz54VPYDYrR) <https://www.ettoday.net/news/20170328/893559.htm#ixzz54VPYDYrR>

▲ 北韓如果真的參與去年竊取孟加拉央行案件，就是國家搶銀行。（圖 / 示意圖 / 達志影像）

? 攻擊者在忙些什麼？

新聞

Check Point: 駭客大舉掃描網路伺服器安全漏洞，700台伺服器淪為採礦機

Check Point警告一駭客大規模掃描全球30%的網路伺服器，包含PHP、Microsoft IIS與Ruby on Rails等，察探是否存在安全漏洞，藉此植入XMRig採礦程式，目前已有700台伺服器淪陷，成為駭客採礦幫手。

文/ 陳曉莉 | 2018-01-16 發表

讚 4.6 萬 按讚加入iThome粉絲團

讚 242 分享

G+



IBM Cloud

DevOps 顛覆新時代
創新論壇

不只「持續交付」，更要「持續顛覆」！

立即報名

iThome Weekly 電腦報

按讚追蹤 iThome 最新報導

讚 4.6 萬

? 攻擊者在忙些什麼?

【2018關鍵趨勢10: GDPR】歐盟最嚴格個資法規來了, 想跟歐洲做生意都得遵守GDPR

號稱歐盟最嚴格個資法的GDPR, 未來只要網站或服務會直接或間接蒐集、處理和利用歐盟民眾個人可識別資料時, 都將強制受到GDPR的規範

文/ 黃彥棻 | 2017-12-31 發表

讚 4.6 萬

按讚加入iThome粉絲團

讚 35 分享

G+

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

TIME UNTIL GDPR ENFORCEMENT
UTC
149:16:46:23

IBM

聊聊 **SIEM (安全資訊與事件管理)** 的趨勢演進

2018年2月01日(四) 15:00 線上揭密!

立即報名

iThome 電腦報
Week

按讚追蹤 iThome 最新報導

讚 4.6 萬

2018 iT 邦幫忙鐵人賽熱門文章

? 攻擊者在忙些什麼?



依GDPR規定，企業若未遵循法規要求，主管機關得進行調查，最重更可裁處企業**2,000萬歐元**、或該年度全球營業額**4%**的罰鍰（取其高者）。

企業必須知道正在蒐集什麼樣的資料和其資料來源

根據RiskIQ去年針對FTSE 30的研究，發現對外蒐集客戶個資的網頁中，有高達三成的網頁是在不安全的狀況下進行個資蒐集。

34%的個資收集網站不安全

29% 沒有加密；
3.5%使用老舊、含有漏洞的加密；
1.5%憑證過期。

In Poor Form

RiskIQ Research Shows FTSE Companies Lack Secure Data Collection Methods

With one year remaining until the EU General Data Protection Regulation (GDPR) takes effect, new research by RiskIQ reveals that 34% of all public web pages of FTSE 30 companies capturing Personally Identifiable Information (PII) are in danger of violating the regulation by doing so insecurely.



更多案例...

2013年5月政府電子公文交換系統遭到駭客入侵，提供該軟體直接下載的網站，被置換成惡意程式，對外連線到不明的中繼網站，預估超過7,000個政府機關受到影響。

- 中華民國交通部觀光局網站被植入惡意連結
- 1111 人力銀行網站被植入惡意程式
- 八大電視台網站又被植入惡意連結
- 佛教慈濟綜合醫院網站又被植入惡意連結
- 台灣達人秀網站被植入病毒下載網址
(約2500網友受威脅)

.....



全盤的掌握您的外部數位資產

SSL 憑證過期、破損？

有多少公司網站頁面使用各類的第三方元件，如 Facebook Like, tracking code, Open Source Library, iFrame, Widget...？

Web Server的架構、版本是否存在已知漏洞？

網站內哪些login form不安全？

有哪些網站用於蒐集PII相關資訊？

總共有多少個重新導向連結 (redirect) 破損

總共有幾個 Web Sites

今天有任何新註冊的網站掛在公司Domain？

今天有任何公司網站登記email被變更？

今天有任何新網站掛在公司的IP下？

多少公司網站30天內註冊會到期？

有多少公司網站被植入惡意軟體或釣魚網站連結？

有那些公司網站今天Active/Inactive？

重新導向的連結會導向到哪邊網站？

我們能掌握那些重新導向的連結內容有被變更？



新的思維角度

內部防衛了，外部更要掌握

您不能在客戶、Partner 端裝上防火牆或防護軟體，但您還是能做一些事的，例如即時監控、掃描、自動化預警或進一步先移除惡意仿冒資產...等



資安的防護無法僅滿足於內部!

掌握外部的關鍵



Doing the Right Things Right

目前狀態



各式不同的情報

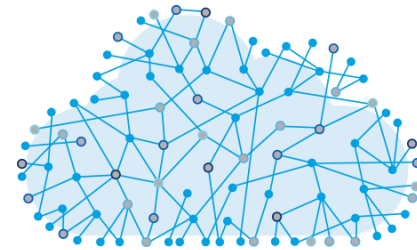


各式的工具組



低效率

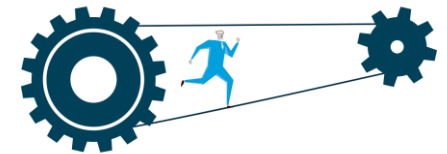
理想狀態



綜整情報
大數據分析



統一的工具組

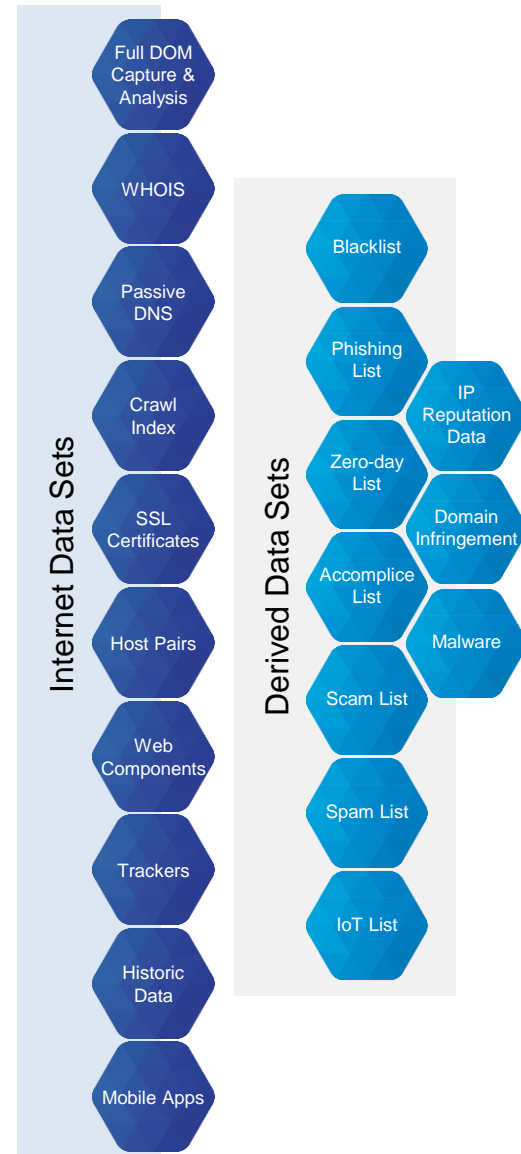
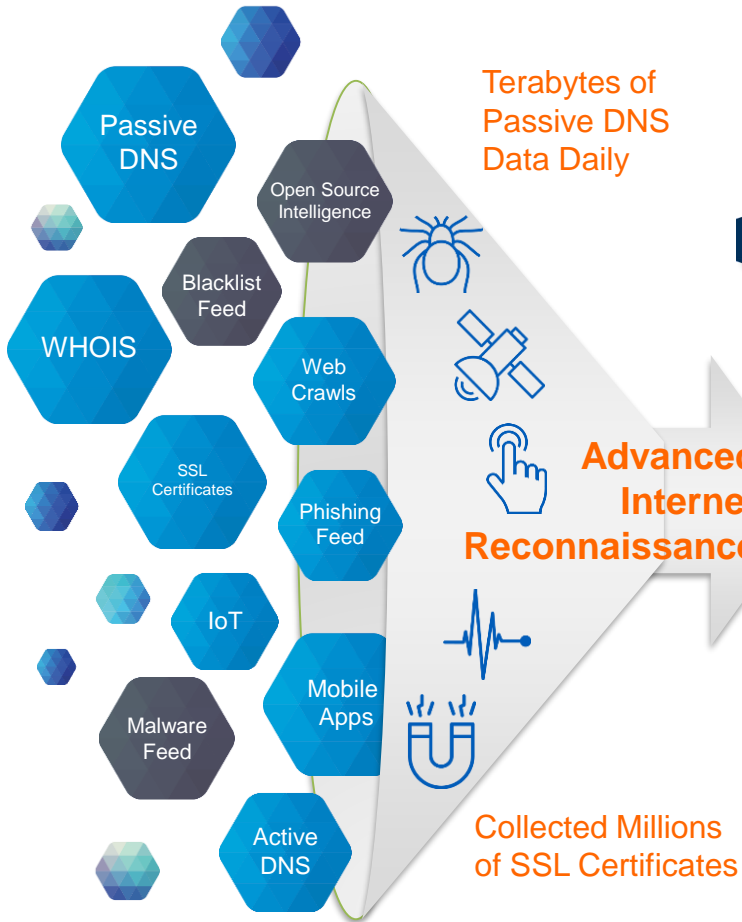


高效率

捕捉

分析

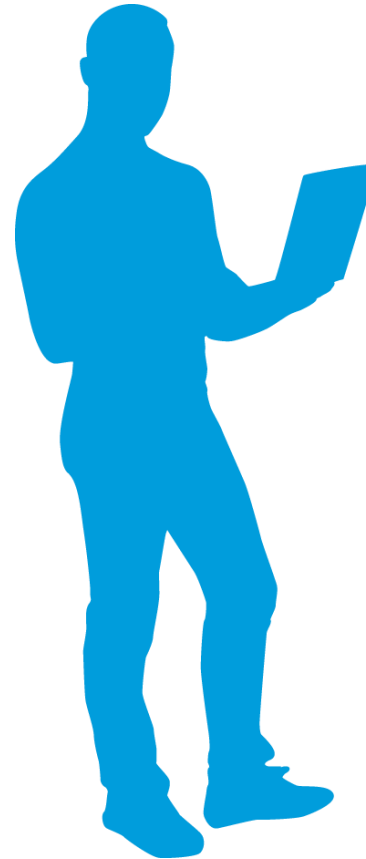
組合



RiskIQ資料收集技術 - Virtual User

防止反偵蒐技術

- 全球地理位置
- 各類流量來源(自用、商用、行動網路)
- 不同時區
- 各瀏覽器、版本、裝置
- 擬人瀏覽行為，滑鼠移動、等待時間、連結點擊、點擊順序、Session長度...等
- 使用者Cookie



大規模數據每日入庫

- 1+ TB DNS Data
- 1.8 B web sessions (incl. Doc Object Model)
- 300 M domain records
- 16 Million Mobile Apps

Virtual User實績

2015年9月18日, RiskIQ 偵測到竊取憑證的惡意軟體被植到 jQuery 的下載包中



思考方向與對策

1. 對外公開的數位資產需做盤點與監控
 - 確實了解組織的受攻擊面
 - 對動態變化的外部資產能同步掌握
 - 了解外部資產可能存在的漏洞及風險
2. 如何應對偽冒的惡意攻擊事件，以防止商譽受損
 - 偽冒網站
 - 偽冒手機App
 - 偽冒社交帳號
 - 快速發覺可疑事件，透過足夠資訊做判斷，具備快速的流程做處置
3. 如何使資安調查團隊發揮極大效能，主動面對攻擊來源
 - 能針對可疑IP、Domain、Email快速找出大量關聯資料
 - 資料除當下狀況外，並可追溯過往，拓展調查範圍
 - 與多方鑑識資源連結，節省資訊整合時間
 - 團隊可即時共享調查狀況

思考方向與對策



RiskIQ
Digital Footprint

1. 對外公開的數位資產需做盤點與監控
 - 確實了解組織的受攻擊面
 - 對動態變化的外部資產能同步掌握
 - 了解外部資產可能存在的漏洞及風險

2. 如何應對偽冒的惡意攻擊事件，以防止商譽受損
 - 偽冒網站
 - 偽冒手機App
 - 偽冒社交帳號
 - 快速發覺可疑事件，透過足夠資訊做判斷，具備快速的流程做處置

3. 如何使資安調查團隊發揮極大效能，主動面對攻擊來源
 - 能針對可疑IP、Domain、Email快速找出大量關聯資料
 - 資料除當下狀況外，並可追溯過往，拓展調查範圍
 - 與多方鑑識資源連結，節省資訊整合時間
 - 團隊可即時共享調查狀況

滲透測試不是就夠了嗎？

- 得知在測試當下時間點的漏洞，要如何對應這次測試與下次測試之間新發現的漏洞？
- 測試已知給定的範圍，但不知其存在的資產呢？



全時監控

才能真正掌握動態變化的數位資產狀態

The screenshot displays a security monitoring interface. At the top, it shows the domain 'blueearth[redacted].gov' and a threat ID '17253495'. Below this, there are tabs for 'Summary', 'Affected Host', 'Threat Host', 'Pages Affected (1)', and 'Threat Urls (1)'. The 'Pages Affected' tab is active, showing a table with one entry:

Page	Threat Count	Match Type	Match Level	Matched By	Confidence	Links
https://blueearth[redacted].gov/streamlining-operations/northern-nj-final-redacted.pdf	1	Exact	Url	2	Low	

On the left side, a sidebar shows details for the malware threat, including its status as 'New', threat host as 'blueearth[redacted].gov', and first seen/scanned dates as '24 days ago'. The interface also includes a search bar at the top left and a footer with the copyright notice '© 2017 RiskIQ Inc. All Rights Reserved'.

24/7

FILTERS

Web Site (15,669) Host (7,889) Domain (1,836) SSL Cert (153) Name Server (44) ASN (2) IP Block (42) IP (7) Mail Server (26) Contact (79)

1-25 of 15,669 Sort: Created At Descending

	Asset Type	Name	Tags / Brands	Status	Confidence	Priority	Enterprise Asset	Title	Host
1	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	mx[REDACTED]
2	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	mx[REDACTED]
3	WEB SITE	https://[REDACTED]	WHOIS - Non-Official	Confirmed	Absolute	High			ftp[REDACTED]
4	WEB SITE	https://[REDACTED]	WHOIS - Non-Official	Confirmed	Absolute	High		default.secureserver.net	ftp[REDACTED]
5	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ftp[REDACTED]
6	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	us[REDACTED]
7	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	un[REDACTED]
8	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ns[REDACTED]
9	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ns[REDACTED]
10	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ftp[REDACTED]
11	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ed[REDACTED]
12	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ww[REDACTED]
13	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ww[REDACTED]
14	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	ww[REDACTED]
15	WEB SITE	https://[REDACTED]	WHOIS - Official	Confirmed	Absolute	High			ww[REDACTED]
16	WEB SITE	https://[REDACTED]	Name Server Domain Assets WHOIS - Official	Confirmed	Absolute	High		ERROR: The requested URL could not be retrieved	off[REDACTED]

- FILTERS
- COMMON
 - Auto Confirmed
 - Brand
 - Confidence
 - DNS Veracity
 - Discovery Run
 - Enterprise Asset
 - Infrastructure Policy
 - Keystone
 - Organization
 - Primary Contact
 - Priority
 - Secondary Contact
 - Status (3 / 25,789) : **Confirmed**
 - Tag
- ASN
 - CONTACT
 - DOMAIN
 - HOST
 - IP BLOCK

1-25 of 15,673 Sort: Created At Descending

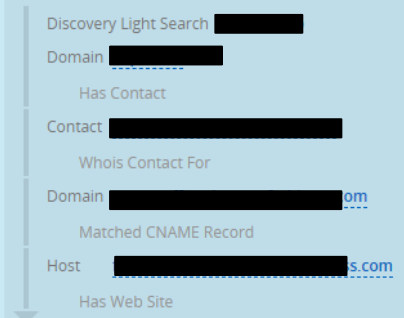
19	WEB SITE	https://[REDACTED]	WHOIS - Official	Confirmed	Absolute	High		
20	WEB SITE	https://[REDACTED]	Name Server Domain Assets	WHOIS - Official	Confirmed	Absolute	High	ERROR: The request
21	WEB SITE	https://[REDACTED]	Name Server Domain Assets	WHOIS - Official	Confirmed	Absolute	High	ERROR: The request

Name Server Domain Assets WHOIS - Official

LINKED ASSETS - ALL

Host: [ftp.\[REDACTED\]](#) Domain: [us.\[REDACTED\]](#) Contact: [d.\[REDACTED\]](#)

AUDIT TRAIL



[https://\[REDACTED\].com](#)

Created 3 months ago Updated a day ago Primary Contact : None Secondary Contact : None Watchers : 0

[Full Details >](#)

22	WEB SITE	http://[REDACTED]	Name Server Domain Assets	WHOIS - Official	Confirmed	Absolute	High	ERROR: The request
23	WEB SITE	http://[REDACTED]	Name Server Domain Assets	WHOIS - Official	Confirmed	Absolute	High	ERROR: The request
24	WEB SITE	https://[REDACTED]	Name Server Domain Assets	WHOIS - Official	Confirmed	Absolute	High	ERROR: The request

GLOBAL INVENTORY INSIGHTS

+ ADD INSIGHT

233

Individual IPs with an Open Port

IPs seen with at least 1 port open in the last 14 days



9

Expired SSL Certs

Confirmed Certificates which have expired.



2

Untrusted Certificates

WoSign and StartCom Certificates | Symantec-Owned EV Certificates



6

OpenSSL

Sites using OpenSSL potentially susceptible to the Heartbleed vulnerability



27

Broken Redirects

Sites that Redirect however the final URL response code is 4xx or 5xx



58

Test Sites

Potential Test Sites



24

At Risk Frameworks

Sites using at risk frameworks with known vulnerabilities



81

At Risk Servers

Servers with Operating Systems that have known vulnerabilities



111

Site Access

Login and Signin Pages



90

All Wordpress and Drupal Sites

Sites operating on Drupal & Wordpress



5

SHA-1 Certs

SSL Certificates using SHA-1



對策

1. 對外公開的數位資產需做盤點與監控
 - 確實了解組織的受攻擊面
 - 對動態變化的外部資產能同步掌握
 - 了解外部資產可能存在的漏洞及風險



RiskIQ
External Threats

2. 如何應對偽冒的惡意攻擊事件，以防止商譽受損
 - 偽冒網站
 - 偽冒手機App
 - 偽冒社交帳號
 - 快速發覺可疑事件，透過足夠資訊做判斷，具備快速的流程做處置

3. 如何使資安調查團
 - 能針對可疑IP
 - 資料除當下狀
 - 與多方鑑識資
 - 團隊可即時共



資料

對網路釣魚行為的監控



資安轉型年，2017如何備戰？

規畫你的2016藍圖

14.2%企業願意聘用大資料人才

新聞

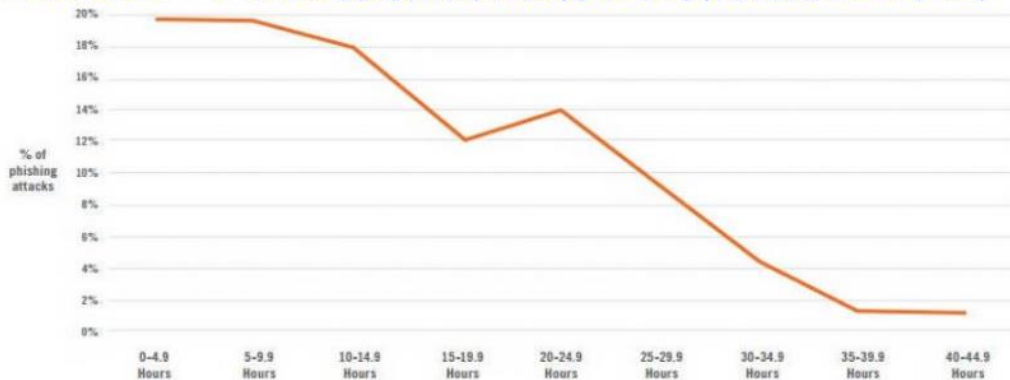
資安周報第53期：8成釣魚網站快閃詐騙，資安產品難防，強化員工警覺才是對策

根據資安公司Webroot的調查結果發現，今年有84%的釣魚網站存活時間低於24小時，平均存活時間低於15小時，最長存活時間為44小時，最短則只有15分鐘，增加資安公司偵測難度。最常被駭客用來模仿欺騙使用者的網站，今年前4名網站依序是Google、Yahoo、Apple、PayPal和富國銀行

文/黃彥霖 | 2016-12-15 發表

f 讚 3.6萬 按讚加入iThome粉絲團 f 讚 分享 271 G+ 5

84% of phishing sites last less than 24 hours. Webroot：84%的釣魚網站存活時間短於24小時

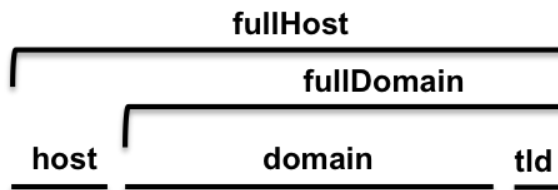


資料來源：Webroot 圖片來源：資安公司Webroot提供

資安公司Webroot調查顯示，2016年1月~9月期間，有84%的釣魚網站存活時間短於24小時。



WEB



url: [http://www.irs-tax-settlement-hq.com/...](http://www.irs-tax-settlement-hq.com/)

IRS Tax Lien? Need an [IRS Offer In Compromise](#)? You're at the place for all [Tax Debt Help](#) and IRS Payment Plans!



Do You Need...
IRS Tax Settlement
We'll Fight to Restore Your Life!

Call Us Now
(877) 627-1192
Llámenos Ahora

- Free Consultation
- Tax Problems
- Tax Solutions
- About Us
- Testimonials

Trustworthy & Effective...

- Free Case Review Process to Ensure Success!
- Resolve Your Business and Personal Tax Issues
- Qualified and Experienced Licensed Tax Professionals

Call Us Now at (877) 627-1192



content

Contact Today... Live Worry Free Tomorrow!

This year alone, our efforts have helped connect thousands of taxpayers to Tax Professionals resolve their IRS/State Tax Problems. The Licensed Tax Professionals in our network have several years' experience and have seen millions of dollars in tax debt. Call today for a free, no obligation consultation, and an IRS tax expert will review your individual situation with the IRS, communicate options to you, and execute the path you choose to pursue. This puts you in control, not the IRS!

"I was extremely skeptical at first. Well, long story short, after signing up they went to work immediately. Results followed. The help has been so priceless, no pun intended. Even if you're on a tight budget, they work with you. Excellent company."

Dana B.—Lawrence, KS

Your Information Is Safe with Us

title

```
Overview Original Response Rendered DOM Files Cookies L...
1. <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-tr
2. <html>
3.
4. <head>
5. <title>Free Consultation about Your Tax Problems from IRS Tax Settlement</title>
6. <meta NAME="keywords" content="free consultation, irs payment plan, tax debt"><meta content="IRS Tax Settlement
   your Tax Problems." name="description">
7. <link href="/feed.xml" rel="alternate" title="IRS Tax Settlement HQ RSS Feed" type="application/rss+xml" />
8. <meta content="text/html; charset=ISO-8859-1" http-equiv="Content-Type">
9. <link href="/style.css" rel="stylesheet" type="text/css" />
10. <script src="/shortform.js" type="text/javascript"></script>
11. <SCRIPT language="JavaScript" type="text/javascript">
12. <!-- Yahoo! Inc.
13.     var ysm_accountid = "1MN18KE6J0UTM9N3PAEBF90EBHS";
14.     document.write("<SCR + "IPT language='JavaScript' type='text/javascript' "
```

responseBody

- **Typosquatting** 近似域名

domain.com vs. domainn.com

- **Homoglyphs** 同形

domain.com vs. dornain.com

- **埋在Domain或Subdomain**

yourbrand.com vs.

iswearimnotyourbrand.com

yourbrand.imnotabadsiteiswear.com

- **Punycode**

xn--riskiqbnk-ora.com

riskiqbånk.com



riskiqbank.com

SOCIAL

Profile Homepage: <https://twitter.com/Wikimedia>

Profile Name

- Not unique to user
- Changeable with keeping the same username
- Available field: socialName

Username

- Unique to user
- Contained in homepage URL
- Available field: socialUsername

Description

- Available field: socialDescription

Location

- Not currently target-able

Profile Link

- Not unique to user, but limited to 1 per profile
- Available field: socialProfileLink

TWEETS 3,542 **FOLLOWING** 505 **FOLLOWERS** 30.8K **LIKES** 139

Tweets Tweets & replies Photos & videos

Wikimedia Retweeted
Michael Anton Dila @michaeldila · 22h
My daughter's agreed to give away \$100 instead of getting it as Xmas presents. So, we all donated to @Wikipedia and @TrevorProject #share

Wikimedia Retweeted
Mylee Joseph @myleejoseph · Dec 15
#Wikipedia on making pageview data easily accessible - blog.wikimedia.org/2015/12/14/pag... > a BIG priority for GLAMs to show #GLAMWIKI ROI

Wikimedia Retweeted
Motherboard @motherboard · Dec 16
Watch the world change but not really In Wikipedia's #Edit2015 bit.ly/1IP5nlf

Followers

- a.k.a. Likes, Friends, Connections, or Subscribers, etc.
- Not currently target-able



MOBILE

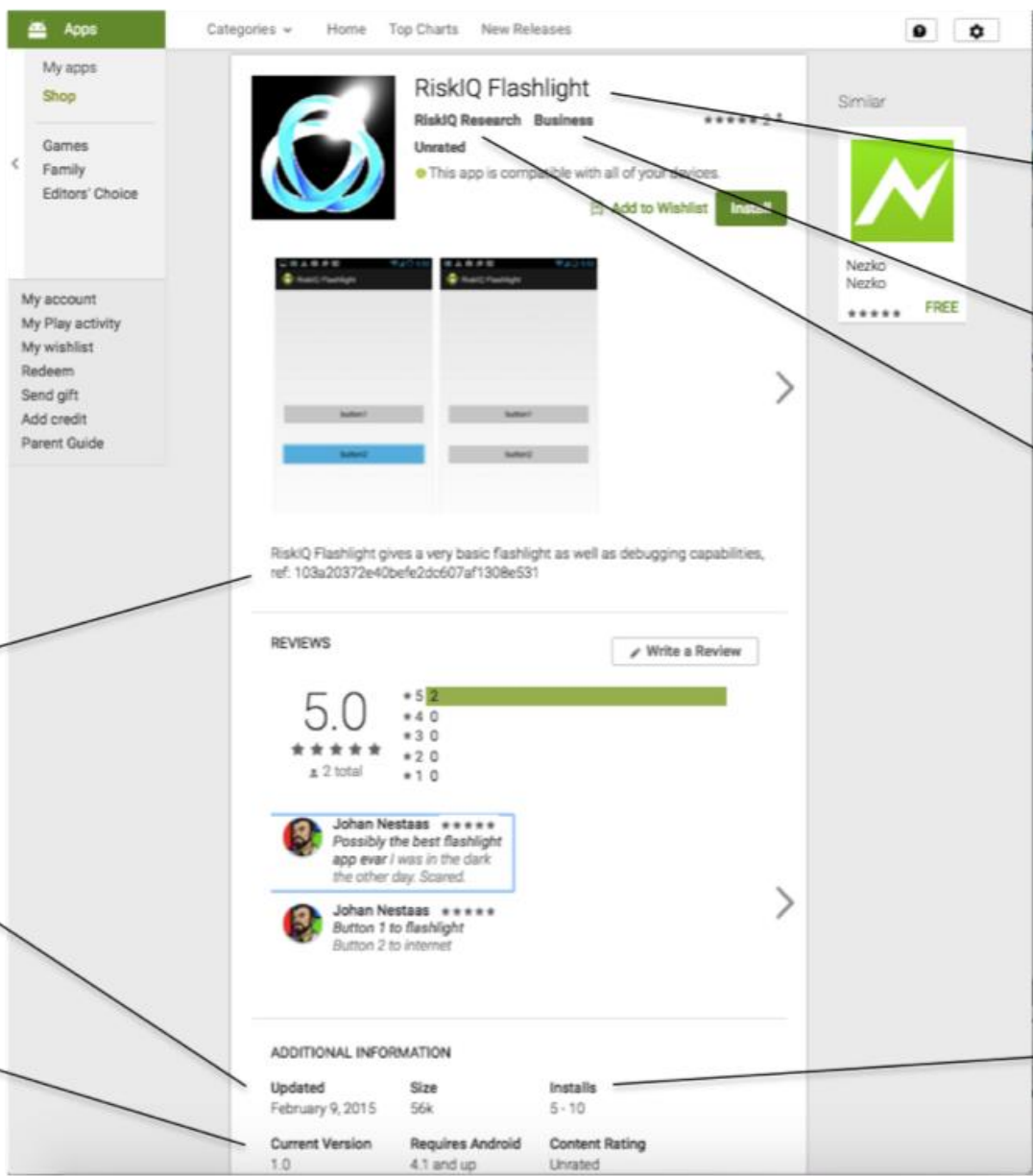
App: <https://play.google.com/store/apps/details?id=com.riskiq.riskiqflashlight>

App URL

- Contains store name and a unique identifier for the app, such as the title, official ID, or store-specific ID

Package Name/Official ID

- Available field: officialID



App Name

- Available field: title

Category

- Available field: category

Developer

- Available field: developer

App Description

- Available field: description

Date of Publication/Update

- Available field: releaseDate

App Version

- Available field: currentVersion

Downloads

- Not currently targetable

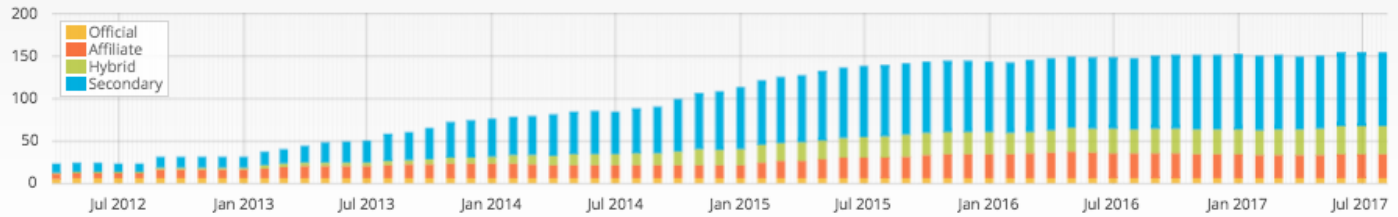
23,642,734
Active Apps

188
Stores

100
Active Stores

8
Platforms

9
Languages



CURRENT EVENT STATUS

1,424

New

30

Review

10

Confirmed

1

Enforced

639

Tenacious

252

Monitor

309

Resolved
Past Month

2,273

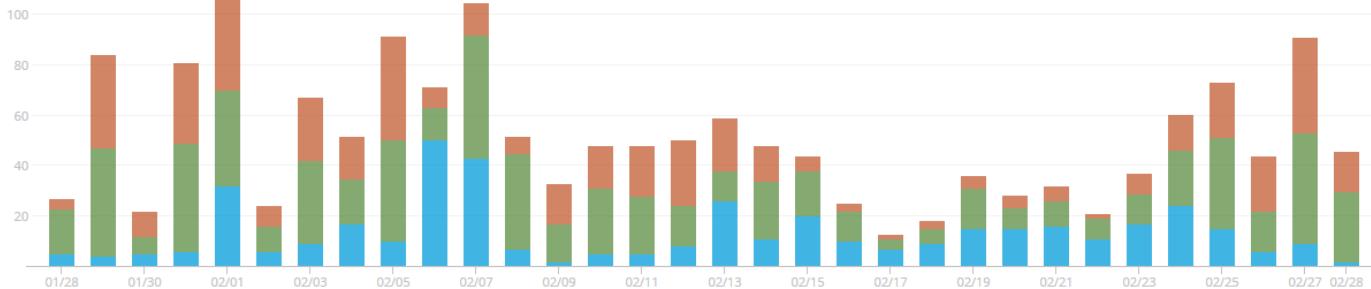
Active

CURRENT COUNTS BY TYPE

Malware	3
Phish	6
Domain Infringement	1,006
Rogue Mobile App	72
SSL	217
Web Compliance	56
Content	254
Infrastructure	415
Social	327
All	2,356

HISTORICAL DATA

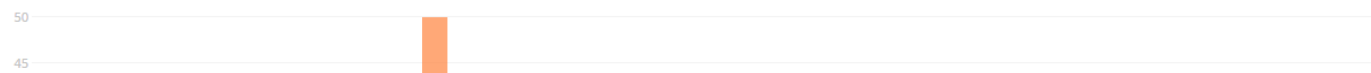
STATUS CHANGES BY DATE



TOTAL STATUS CHANGES

427	New
705	Resolved
508	Tenacious
1,640	All

EVENT CREATION BY DATE



TOTAL EVENT CREATIONS

1	Phish
170	Domain Infringement

對策

1. 對外公開的數位資產需做盤點與監控
 - 確實了解組織的受攻擊面
 - 對動態變化的外部資產能同步掌握
 - 了解外部資產可能存在的漏洞及風險

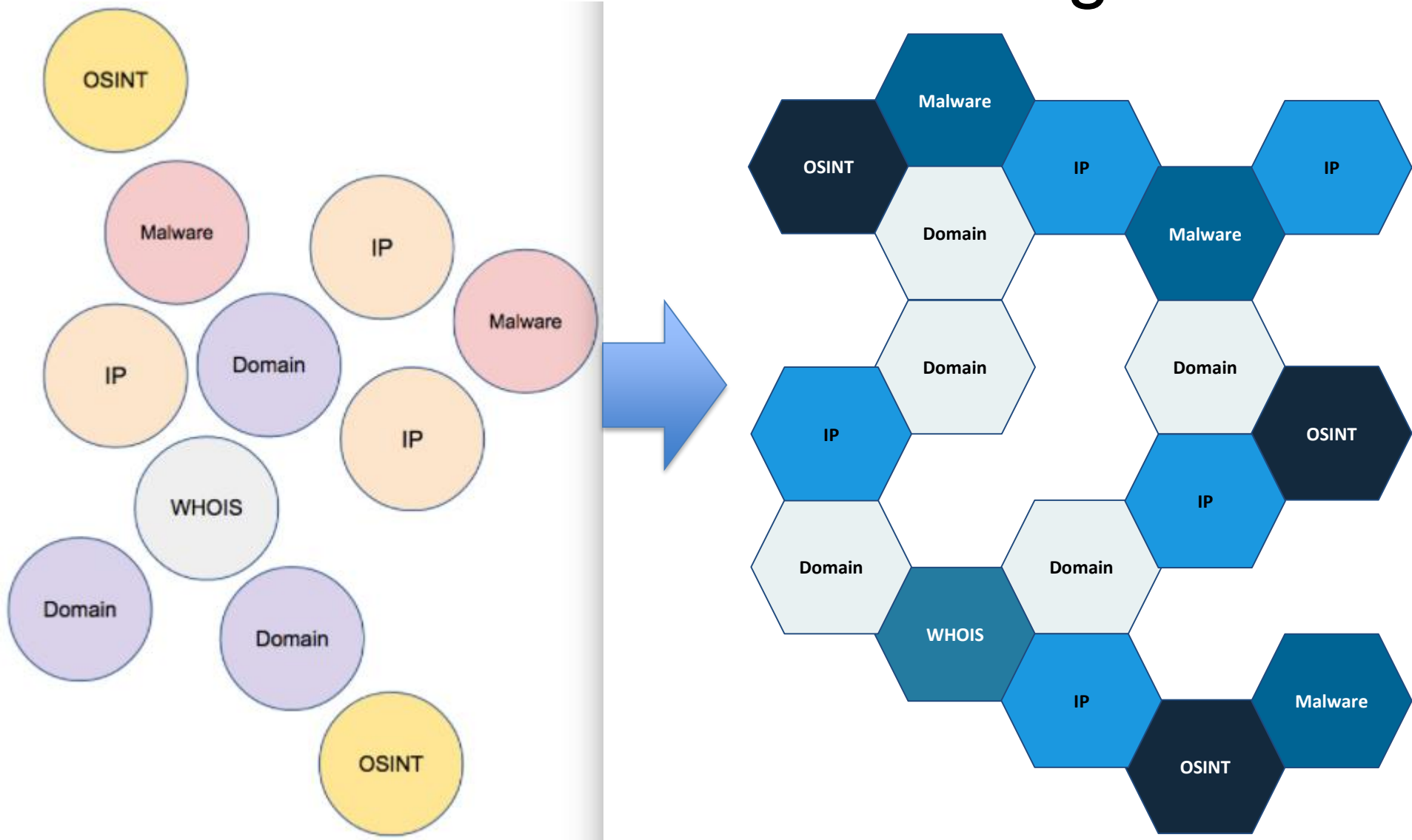
2. 如何應對偽冒的惡意攻擊事件
 - 偽冒網站
 - 偽冒手機App
 - 偽冒社交帖
 - 快速發覺可疑

RiskIQ
PassiveTotal

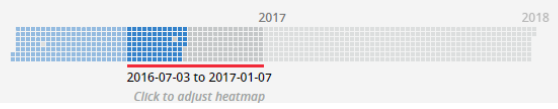
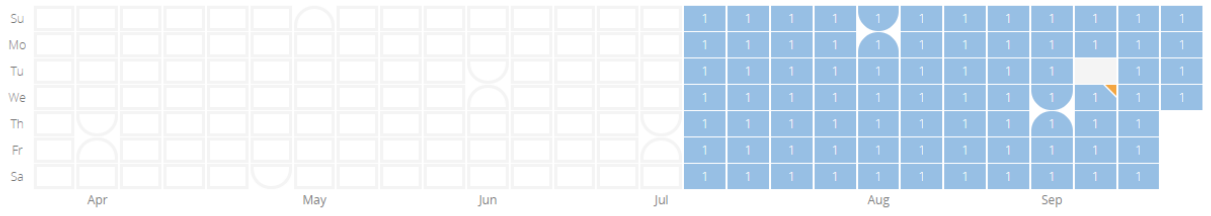


3. 如何使資安調查團隊發揮極大效能，主動面對攻擊來源
 - 能針對可疑IP、Domain、Email快速找出大量關聯資料
 - 資料除當下狀況外，並可追溯過往，拓展調查範圍
 - 與多方鑑識資源連結，節省資訊整合時間
 - 團隊可即時共享調查狀況

Infrastructure Chaining



HEATMAP You can click / shift-click the heatmap to filter the results below



- FILTERS
- IP (78 / 78)
 - ✓ x 104.86.110.104 1
 - ✓ x 104.86.110.113 1
 - ✓ x 107.170.2.22 1
 - ✓ x 128.241.90.162 1
 - ✓ x 128.241.90.170 1
 - Show More...

RESOLUTIONS

Show: 25 1-25 of 78 Sort: Last Seen Descending

Resolve	Location	Network	ASN	First	Last	Source	Tags
107.170.2.22	US	107.170.2.0/24	62567	2016-09-07	2016-09-21	pingly, riskiq	Digital-Ocean-Inc. Routable
52.70.175.181	US	52.70.0.0/15	14618	2016-03-10	2016-09-05	kaspersky, pingly, riskiq, virustotal	Amazon.Com-Inc. Routable
165.254.42.65	US	165.254.0.0/16	2914	2016-01-29	2016-03-08	pingly, riskiq	Ntt-America-Inc. Routable
165.254.42.83	US	165.254.0.0/16	2914	2016-01-29	2016-03-08	pingly, riskiq	Ntt-America-Inc. Routable
64.86.206.122	US	64.86.0.0/16	6453	2016-03-08	2016-03-08	riskiq	Routable Tata-Communications-America
64.86.206.74	US	64.86.0.0/16	6453	2016-03-06	2016-03-06	riskiq	Routable Tata-Communications-America

- NETWORK (36 / 78)
 - ✓ x 198.172.0.0/15 4
 - ✓ x 72.246.64.0/23 4
 - ✓ x 128.241.0.0/16 3

Passive DNS

- Historical set of records for the resolutions of domains and IP addresses. Reveals patterns of attackers and derives timelines

WHOIS

- Repository of registrant information that can provide leads on connecting different data points together. Sometimes reveals actor patterns

Subdomains

- Any hosts (host.domain.com) that have been seen related to the domain or IP address

OSINT

- Open source intelligence, both long and short form provided by individuals and companies.

Hashes

- PassiveTotal partners with a number of commercial and open source repositories of malware data.

Trackers

- Unique fingerprints identified within web page content that correlates to a single point. Helpful in surfacing abuse such as phishing

Components

- Technology used on websites or on IP addresses. This information can include web server software, operating system, web app frameworks.

Host Pairs

- Sequence data obtained from crawling the internet like a user. Identifies related hosts based on dependencies, linking, or redirection.

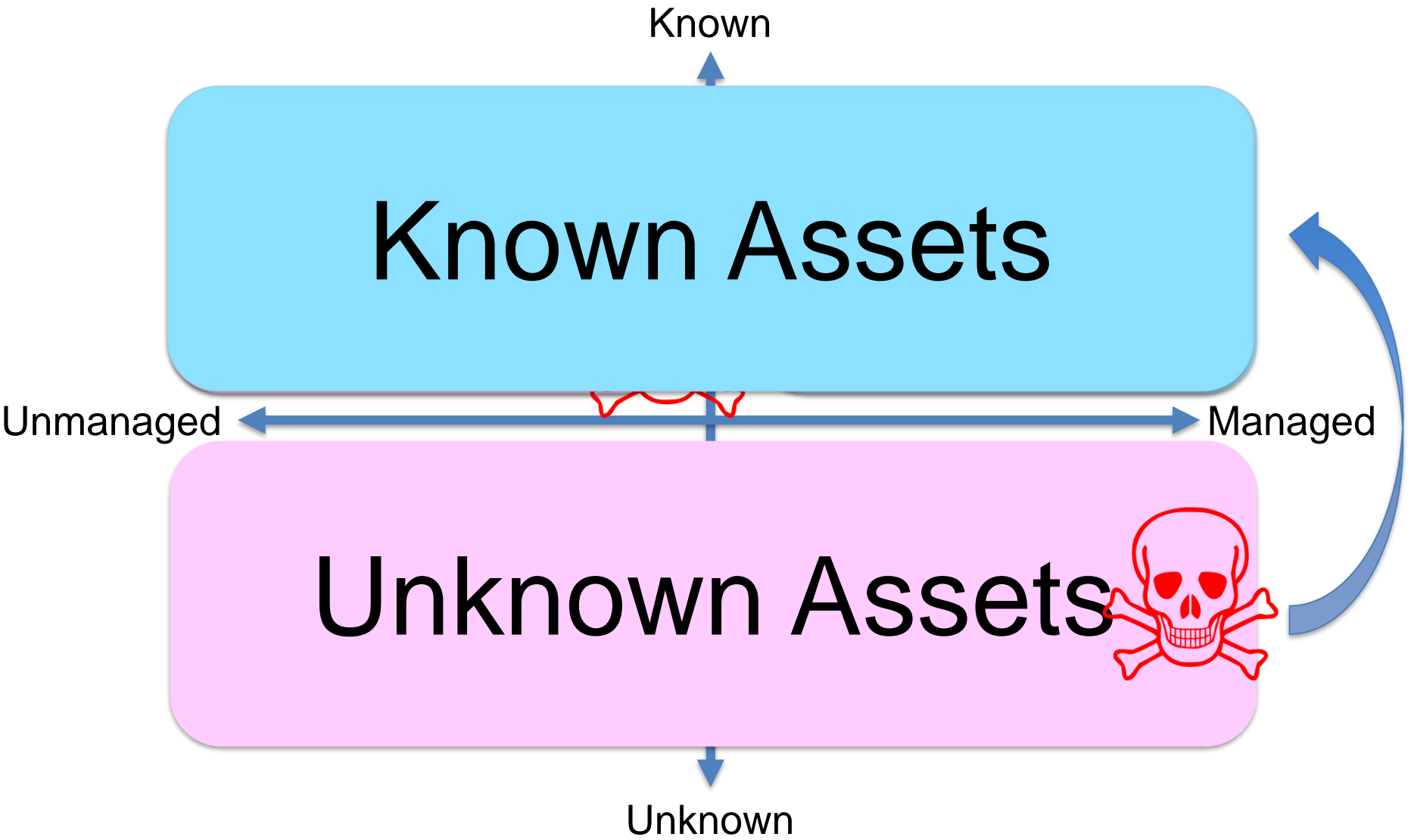
DNS

- MX (mail exchanger), NS (nameserver), TXT (text), SOA (start of authority), CNAME (canonical name) records

您有多少外部數位資產？

您如何對不知道其存在的資產進行防護？

賦予企業對自身外部資產的能見度



KNOWING IS THE BEST DEFENSE™