# Shodan簡介與應用

NASOC 二線工程師 林宜進

E-mail : tjline01@asoc.cc.ntu.edu.tw

大綱

- 1. Shodan 简介
- 2. 下載Shodan資料
- 3. 網路攝影機的特性
- 4. 結合Shodan尋找網路攝影機



# Shodan简介

SHODAN網頁上的相關操作介紹

基本介紹

●Shodan是一個搜尋引擎,主要是搜索網路上的IoT設備

●可以搜尋多種設備(例如:Webcam、SCADA、router、server),有時會有詳細資訊

●官方網址: https://www.shodan.io/





帳號註冊(2/3)

Shodan Developer Book More	
SHODAN Account Register	
	Create Account
	Username
	Password
	Confirm Password
	Email
	□ Subscribe to the newsletter 這是問您未來是否要收到Shodan的更新資訊,
	By creating an account you are agreeing to our Privacy Policy and Terms of Use 可不勾選
	СКЕАТЕ

帳號註冊(3/3)

### ●到註冊信箱收信,總共會收到兩封信。一封信是啟動確認信; 另一封是帳號建立完成信



S b/ 00.27	reply@shodan.io>	
工十 09:27		
收件者:	■ 帳號建立5	<b>毛成信</b>
ні		
You've successfully creat account information to l	ted an account on Shodan! Below you login, make sure to keep this email in y	will find all important our archive for later.
Account Information		
URL: https://account.sho	dan.io	
URL: <u>https://account.sho</u> Username: ETLtestforsho	idan.io	
URL: <u>https://account.sho</u> Username: ETLtestforsho	idan.io	
Username: ETLtestforsho	idan idan ted? Check out the following to get fami	liar with Shodan:
URL: https://account.sho Username: ETLtestforsho Not sure where to get star Discover Shared S	rdan rted? Check out the following to get fami Searches	liar with Shodan:
URL: https://account.sho Username: ETLtestforsho Not sure where to get star Discover Shared S Complete Guide to	idan idan ted? Check out the following to get fami <u>Searches</u> to Shodan book	liar with Shodan:
Username: ETLtestforsho Username: ETLtestforsho Not sure where to get star <u>Discover Shared S</u> <u>Complete Guide t</u> <u>Short Videos for d</u>	idan idan ted? Check out the following to get fami <u>Searches to Shodan book</u> <u>common tasks</u>	liar with Shodan:

基本操作-搜尋欄位(1/2)

●可任意輸入想查詢的設備(例如:Webcam、MySQL server...)

🔗 Shodan		Q
	$\overline{\nabla}$	
🔏 Shodan	Webcam	٩

💫 Shodan 🛛 🛛	Vebcam		۹ 🕯	Explore	Downloads	Reports	Pricing	Enterprise Access
Exploits Maps	Images	📥 Like 137	📥 Download Results	Lul Crea	te Report			
TOTAL RESULTS 5,201 TOP COUNTRIES		New Servi RELATED TAGS 24.18.117 c:2418117-70h Comcast Cable Added on 2019-05 United States	fice: Keep track of what your free free free free free free free fr	u have conn HTTF Cont WWW-	P/1.1 401 Unauth P/1.1 401 Unauth cent-Length: 0 Authenticate: D	ernet. Check orized igest qop="au	out Shodar	IP Webcam", nonce="1557711307"
United States Korea, Republic of Germany Romania Poland	1,023 495 480 319 304	124.51.10 Lg Powercomm Added on 2019-05	01.9 C	HTTF Cont WWW-	9/1.1 401 Unauth ent-Length: 0 Authenticate: D	orized igest realm="	IP Webcam",	nonce="1557711793", qop="auth"
TOP SERVICES HTTP (8080) 8081 HTTP HTTPS 8083	1,751 855 219 209 114	188.27.11 188-27-111-199.rd RCS & RDS Res Added on 2019-05	tanet.ro sidential 15-13 01:36:46 GMT Bucuresti	HTTF Cont WWW-	2/1.1 401 Unauth cent-Length: 0 Authenticate: D	orized igest qop="au	th", realm="	IP Webcam", nonce="1557711583"

基本操作-搜尋欄位(2/2)

•在輸入要查詢的設備名稱時,可搭配過濾器(filter),減少無關的資料顯示

•過濾器可以多種搭配使用,例如要找尋(1)IPcam (2)學術網路的設備,欄
位輸入: IPcam isp:TANet



## 搜尋欄位過濾器

過濾器	說明	範例(輸入時可不加雙引號)
net	搜尋指定的ip 位置或是網段	net:"140.112.0.0/16"
port	搜尋指定的連接埠	port:"80"
product	搜尋指定的作業系統/軟體/產品名稱	product:"windows"
country	搜尋指定的國家	country:"TW"
city	搜尋指定的城市	city:"Taipei"
org	搜尋指定的組織或公司	org:"TANet"
isp	搜尋指定的isp業者	isp:"hinet"
hostname	搜尋指定的網域名稱	hostname:"ntu"
version	搜尋指定的軟體版本	version:"4.2"
geo	搜尋指定的地理位置(緯度,經度)	geo:"25, 121"
before/after	搜尋特定的時間前(後)的資料,格式dd-mm-yy	before:"01-01-18"

資料探索(Explore) (1/2)

### ●如果想要知道目前熱門的查詢項目,可以點選Explore頁面



### ●進入探索頁面,可以去找尋有興趣的設備類別







資料探索(Explore) (2/2)

●點擊IP,查看被Shodan紀錄的資訊

●點擊View Raw Data,檢視完整的Shodan掃描資料

• 當越多的資訊被公開在網路上, 就越有機會被入侵攻擊

		Shodan	<b>a</b> * E	Explore Downloads Reports Pricing Enterprise Access		62.93.33.23	
		- Kacławowka -	P			Property Name	Value
				A CARLES AND A C	¥.	area_code	null
						asn	AS25468
	N					city	Rzeszow
ET06.prz.rzeszow.pl	$ \longrightarrow  $	Ø 62.93.33.23 ET	U6.prz.rzeszoW. View Raw Data	Ports		country_code	PL
PRz Network Added on 2019-05-26 01:33:11 GMT	/	City	Rzeszow	8888		country_code3	POL
Poland, Rzeszow	V	Country	Poland			country_name	Poland
		ISP	PRz Network Rzeszow University of Technology		_	data.0shodan.crawler	97b9d37f0484f45ce64530712
		Last Update	2019-05-26T01:33:11.945888	dvr1614n web-cam httpd		data.0shodan.id	cd3b3b82-eeb8-4bd6-86e2-5
		ASN	ET06.prz.rzeszow.pl AS25468	http:simple.new connection: close Cache-control: no-cache Server: SD-WERGM		data.0shodan.module	http-simple-new
				CONTENT - LENGTH: 434		data.0shodan.ptr	True

© 2013-2019, All Rights Reserved - Shodan®

地圖分布(Maps)

- ●該功能是在Exploits的右邊,點擊Maps就會進入
- 這個功能可以查看關鍵字在全球的分布,一些使用者常利用此功能做一些分析,例如設備的分布密度、該設備全球分布狀況的推測等等





## 建立報告(Create Report) (1/2)

●只要註冊會員後,都可以使用此功能

- ●操作過程:
- 1. 查詢資訊
- 2. 按下Create Report
- 3. 建立Report標題
- 4. 按下綠框就開始建立報告



建立報告(Create Report) (2/2) ●建立完成會出現成功訊息,並告訴使用者等待信件通知 ●進入信箱點連結就可以看到產生的Report資訊 Report created <u>F7</u> Shodan <jmath@shodan.io> **III** Reports 上午 11:41 Keep track of and share interesting search results using reports. Success Your request is being processed. We will send you an email once the report is ready! The report "RDP TANet" has successfully been generated! Go ahead and check it out at: 1234 https://nam05.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.shodan.io% 82 Results 2Freport%2FcDPQ0bbt&data=02%7C01%7C% 7Cebb1b1115cdb4dce371e08d6e2553986%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1% 7C0% 7C636945252993272998&sdata=KT6YYSYpRnm372dimDNRBgbndSTQ3fxzAuchAY1F39U

%3D&reserved=0

Best regards,

-John



報告呈現(2/3)



報告呈現(3/3)



### 其他項目補充-上半部



### Developers

#### SHODAN DEVELOPER Dashboard API Reference Integrations Pricing Contact Us

77.181.41.118 5060 x4db52976.dyn.telefonica.de SIP/2.0 200 0K/r/nVia: SIP/2.0/UDP nm;branch=foo;rport=26810;received=xxx.xxx.xxx/r/nFrom: <sip:nm20mm2;ta =root/r/nTo: <sip:nm20mm2;tag=1676398943/r/nCall-ID: 550000/r/nC5eq: 42 0PTINS/r/nUser-Agent: o2-2/XEL-1.00/AAJG.0)D9-VDSL IAD BSA WLAW/r/nContent-Length: 0/r/n/r/n 81.153.78.113 8081 host81-153.78-113.range81-153.btcentralplus.com HTTP/1.1 401 Unauthorized/r/nConnection: Keep-Alive/r/nWWM-Authenticate: Basic realm="HuaweiH meGateway"/r/nContent-Length: 0/r/n/r/n 58.64.157.58 111 edm3.xgate.com.hk Portmap/nProgram/tVersion/tProtocol/tPort/nportmapper/t4/ttcp/t111/nportmapper/t3/ttcp/t111

bolksbptPriveryLinkbptPri

Leverage the Power of Shodan

Shodan <sup>(79d25fe59c8494bdc885ed18be72b76\*)</sup>

Introducing the Shodan API, the easiest way to access the Shodan search engine on your own terms. (inversion: 1.8)

Xcmange type::identity frotection(in top):ident for the set of the set o

30,45,200 500 173-30.45-200.client.mchsl.com VPN (IKE)\n\nInitiaTor SPI: e5f8580805645750\nResponder SPI: 6712f11e0c7e4552\nNext Payload: Notification sion: 1.6\nExchange Type: Informational\nFlags:\n Encryption: Cammit: False\n Authentication: False\nMessage ID: c2992d64\nLengt 80,43.27 80 HTTP/I.1 400 Bad Request\r\nContent-Type: text/html\r\nDate: Mon, 16 Jan 2017 20152:23 GMT\r\nConnection: closer\r\nContent-Lengt



#### Easy Integration

The Shodan API is the easiest way to provide users of your tool access to the Shodan data. The API provides access to all of the search features, allowing you to get exactly the information you want.



#### Beyond the Web

The website only shows a small fraction of the information that is gathered by Shodan. Use the API to gain full access to all the data collected and extract the information you care about.



#### Automate Everything

Use the API to automatically generate reports, notify you if something popped up on Shodan or keep track of results over time.

#### **Real-Time Notifications**

The Streaming API gives you the ability to subscribe to events in real-time so you can immediately respond to new discoveries.



### Monitor

SHODAN Monitor Overv	view Pricing 🗗 Access Portal			
	Know What's Connected Keep track of the devices that you have exposed to the Internet. Setup notifications, launch scans and gain complete visibility into what you have connected.			
	Network Monitoring Made Easy Within 5 minutes of using Shodan Monitor you will see what you current connected to the Internet within your network range and be setup with notifications when something unexpected shows up.	ly have real-time	Coschooret 2 SERVICES 2 SERV	

### View ALL

Shodan Developers Monitor View All									
Shodan World's first search engine for the Internet of Things.	Enterprise Full access to the Shodan data and infrastructure.	<b>Maps</b> Intuitive map interface to search the Shodan database.	Images A stream of screenshots from crawled devices.	Exploits Search across a variety of vulnerability databases at once.	Help Center Learn how to get the most out of the Shodan platform.	My Account			
<section-header></section-header>		Network Monitor	Chrome Browser Plugin	Firefox Plugin 3rd party	ICS Map 2014       Control optimizer of the tree tree of the t	ICS Radar			
Shodan CLLI Shodan CLLI Shodan CLLI Shodan Shodan Shoda	Map of the Internet	Honeypot Or Not O	Shodan 3D	Complete Guide to Shodan	Status Dashboard	Shiptracker			
© 2013-2015, All Rights Reserved - Shodan®									

其他欄位補充





Shodan Developers Monitor View All	Q ♠ Explore Downloads Reports	Show API Pricing Enterprise Access
Getting Started	Latest Additions shared searches	Developer Access Want to build your own tools using Shodan d
What is Shodan?	1 canary	the official Shodan API and get started writing scripts:
Search Query Fundamentals	1 TwistedWeb / 13.2.0 HTTP/1.1 text/html 200 OK	Learn more
How to Download Data with the API	country:it	Filter Cheat Sheet
<ul> <li>Tracking Hacked Websites</li> <li>Understanding SSL by Country</li> </ul>	1 www.baidu.com	Filters let you narrow down search results ba criteria. They are always lower-case and can t include and exclude results. For example, the
Visit the Shodan Help Center for more articles	1 Id hck raima haddi	query finds Modbus results in the US:
SHORT VIDEOS	Discover more queries other users have shared	<b>port:502 country:US</b> Here are a few search filters to help navigate
Top 10 Results for Facet: port 443 1,596,445 903 230 245		Name Description
335         237,7528           8443         134,627           465         109,613           3389         103,815           992         32,216           444         22,616           636         3 92		org Use the org filter to find devices that are on a specific organization's network.

### Downloads



## Pricing & Enterprise Access & Upgrade









## Help Center

Shodan Developers Book N	/iew All						
SHODAN Help Center							
	Search the knowledge base	Search					
The Basics	Guides	Data Analysis					
What is Shodan?	How to Convert Shodan Data to Excel	Create a GIF from an IP Image History					
Search Query Fundamentals	How to Download Data with the API	Understanding SSL by Country					
Navigating the Website	How to Monitor a Network in Real-Time	Tracking Hacked Websites					
Shodan Credits Explained	Developer Fundamentale						
On-Demand Scanning	Developer Fundamentals	Mastery					
	Looking up IP Information	Pivoting with Property Hashes					

Working with Shodan Data Files

🗋 test.json 🗙

下載Shodan資料

從SHODAN下載資料去分析

前言

●Shodan官方有提供python套件,讓使用者選擇用CLI(命令列)或是在寫 python程式碼去使用Shodan服務

●下載網址: https://github.com/achillean/shodan-python

●本次操作以CLI為主

achillean@demo:~ achillean@demo:~ achillean@demo:~	<pre># Lets see which ports are running shodan statsfacets ssl.version,port country:de has_ssl:true</pre>
Top 10 Results f	Facet: port
443	1,596,445
993	230,245
995	207,528
8443	134,627
465	109,613
3389	103,815
992	32,216
444	22,616

圖片來源:https://asciinema.org/a/48143

虛擬機環境

▶OS:Ubuntu 14.04 LTS
▶CPU: 1 core
▶Memory: 2GB
▶HD: 20GB
▶Python版本: 2.7.6

System Se	ettings			
	Details     All Settings Details     Overview     Default Applications			
<b>•</b> <b>2</b> •	Removable Media Legal Notice	Device name	ubuntu 14.04 LTS	
		Processor Int Graphics Ga OS type 64 Disk 18	itel <sup>®</sup> Core <sup>™</sup> i5-8250U CPU @ 1.60GHz allium 0.4 on SVGA3D; build: RELEASE; 4-bit 8.9 GB	LLVM; Install Updates

### 安裝Shodan 套件

### •有雨種安裝指令可以安裝,兩個安裝方式差異不大

> easy\_install shodan

pip install shodan

#### 備註:

- 1. easy\_install 要安裝python-setuptools
- 2. pip 要安裝python-pip

#### E README.rst

#### shodan: The official Python library for accessing Shodan

Shodan is a search engine for Internet-connected devices. Google lets you search for websites, Shodan lets you search for devices. This library provides developers easy access to all of the data stored in Shodan in order to automate tasks and integrate into existing tools.

#### Features

- Search Shodan
- Streaming API support for real-time consumption of Shodan data
- Exploit search API fully implemented

#### Installation

To install the Shodan library, simply:

\$ pip install shodan

Or if you don't have pip installed (which you should seriously install):

\$ easy\_install shodan

#### 圖片來源:https://github.com/achillean/shodan-python

### Shodan指令(1/2)

- ●查詢可用指令 → shodan
- ●指令詳細用法 >shodan <<mark>指令</mark>>-h

•可用指令介紹可參考下一頁

😣 🗐 🗊 asoc@master: ~	
asoc@master:~\$ shodan p Usage: shodan parse [OP	arse -h TIONS] <filenames></filenames>
Extract information o	ut of compressed JSON files.
Options: color /no-color fields TEXT ¿ -f,filters TEXT L	List of properties to output. Filter the results for specific values using key:value pairs.
-O,filename TEXT	Save the filtered results in the given file (append if file exists).
separator TEXT (	The separator between the properties of the search results.
-h,help asoc@master:~\$	Show this message and exit.

#### 😑 🗉 💿 asoc@ubuntu: ~

asoc@ubuntu:~\$ shodan Usage: shodan [OPTIONS] COMMAND [ARGS]...

#### Options:

-h, --help Show this message and exit.

#### Commands:

	alert	Manage the network alerts for your account
	convert	Convert the given input data file into a different format.
	count	Returns the number of results for a search
	data	Bulk data access to Shodan
	domain	View all available information for a domain
	download	Download search results and save them in a compressed JSON
	honeyscore	Check whether the IP is a honeypot or not.
	host	View all available information for an IP address
	info	Shows general information about your account
	init	Initialize the Shodan command-line
	myip	Print your external IP address
	огд	Manage your organization's access to Shodan
	parse	Extract information out of compressed JSON files.
	radar	Real-Time Map of some results as Shodan finds them.
	scan	Scan an IP/ netblock using Shodan.
	search	Search the Shodan database
	stats	Provide summary information about a search query
	stream	S <u>t</u> ream data in real-time.
1	soc@ubuntu:~	\$

## Shodan指令(2/2)

	Commands (基礎)
指令	功能
init	帳號初始化
info	顯示帳號的資訊
myip	顯示使用者的IP
host	顯示一個IP所有可用的詳細資訊
count	回傳查詢結果數量
download	下載查詢結果*1
convert	轉換輸入文件到其他格式(csv、xlsx等)
honeyscore	檢查 IP 是否為蜜罐(Honeypot) *2
parse	解析提取壓縮的JSON資訊
search	查詢Shodan資料庫
stats	提供搜索結果的總結資訊

	Commands (進階)
指令	功能
alert	管理帳戶的網路告警事件(shodan monitor)
stream(企業)	即時顯示資料流
scan	使用Shodan掃描一個IP或網段*3
domain	查詢Domain的ip資訊*4
org (企業)	管理組織內部的shodan帳號
radar (企業)	即時觀看Shodan掃描資訊

- 1. 如果要下載大量資料,可能要花費query點數才能下載
- 2. 此分數僅供參考, Shodan並沒有公布判斷方式與標準
- 3. scan指令要花費scan點數;另外無法在短時間內scan同一個目標
- 4. domain指令要花費query點數

#### 備註:

Shodan的指令data,因為測試時發現無法單獨使用,要搭配其他指令操作,怕混淆而不 列在上面

## 下載Shodan資料操作(1/3)

- •使用shodan指令前,要先輸入API Key
  - shodan init < API Key</p>



●雨種方式取得API Key

1.點選右上角Show API Key,之後會顯示個人帳號的API Key

2.點選My Account,就可以看到了





### 下載Shodan資料操作(2/3)

●要調查校內有多少資料筆被Shodan紀錄,可以用count去查詢
 > shodan count < Key Word > (這裡關鍵字查詢跟網頁版相同)



備註:查詢的關鍵字先後順序不會影響查詢結果



## 下載Shodan資料操作(3/3)

- ●要下載shodan的資料,用download指令;下載壓縮格式是.gz;儲存資訊為.json
- ●指令為 shodan download <<mark>filename</mark>> <<mark>Key Word</mark>>

>shodan download IPcam\_TANet IPcam isp:TANet

😵 🗖 🔲 asoc@ubuntu: ~	
asoc@ubuntu:~\$ shodan download	IPcam_TANet IPcam isp:TANet
Search query:	IPcam isp:TANet
Total number of results:	36
Query credits left:	0
Output file:	IPcam_TANet.json.gz
[######################################	#######+=] 97% 00:00:01
Saved 36 results into file IPca	m_TANet.json.gz
asoc@ubuntu:~\$	

### Shodan轉檔

●轉換輸入的文件到其他格式(可轉換格式有:kml、csv、geo.json、images、 xlsx)

▶ shodan convert < 檔名.json.gz > < 要轉換的格式>

>shodan convert TANet\_ipcam.json.gz csv



csv的資料欄位

### ▶總共有31個欄位,可參考下圖

▶某些欄位的值可能為空(Null),可能是當時掃描沒有抓到資訊

1	2	3	4	5	6	7	8	9
data	hostnames	ip	ip_str	ірvб	org	isp	location.country_code	location.city
10	11	12	13	14	15	16	17	18
location.country_name	location.latitude	location.longitude	OS	asn	port	tags	timestamp	transport
19	20	21	22	23	24	25	26	27
product	version	vulns	ssl.cipher.version	ssl.cipher.bits	ssl.cipher.name	ssl.alpn	ssl.versions	ssl.cert.serial
28	29	30	31					
ssl.cert.fingerprint.sha1	ssl.cert.fingerprint.sha256	html	title					

![](_page_39_Picture_0.jpeg)

1	2	3	4	5	6	7	8	9
Data	hostnames	ip	ip_str	ipv6	org	isp	location.country_code	location.city
HTTP/1.0 401 Unauthorized Date: Thu, 01 Jan 1970 00:00:00 GMT Connection: close WWW-Authenticate: Basic realm="webcam" Content-Type: text/html		2XXXXXXX0	140.XXX.XXX.14 National X X University		National X X University	Taiwan Academic Network (TANet) Information Center	TW	
10	11	12	13	14	15	16	17	18
location.country_name	location.latitude	location.longitude	OS	asn	port	tags	timestamp	transport
Taiwan	23.5	121		ASXXXX7	80		2019-06- 05T16:20:50.861880	tcp
19	20	21	22	23	24	25	26	27
product	version	vulns	ssl.cipher.version	ssl.cipher.bits	ssl.cipher.name	ssl.alpn	ssl.versions	ssl.cert.serial
28	29	30	31					
ssl.cert.fingerprint.sha1	ssl.cert.fingerprint.sha256	html	title					

xlsx的資料格式

▶總共有17個欄位,可參考下圖

▶某些欄位的值可能為空(Null),可能是當時掃描沒有抓到資訊

1	2	3	4	5	6	7	8	9
IP	Port	Timestamp	Data	Hostnames	Organization	ISP	Country	Country ISO Code
10	11	12	13	14	15	16	17	
City	OS	ASN	Transport	Product	Version	Web Server	Website Title	

## xlsx範例(部分敏感資訊已經刪除)

1	2	3	4	5	6	7	8	9
IP	Port	Timestamp	Data	Hostnames	Organization	ISP	Country	Country ISO Code
140.XXX.XXX.14	80	2019-06- 05T16:20:50.861880	HTTP/1.0 401 Unauthorized Date: Thu, 01 Jan 1970 00:00:00 GMT Connection: close WWW-Authenticate: Basic realm="webcam" Content-Type: text/html		National X X University	Taiwan Academic Network (TANet) Information Center	Taiwan	TW
10	11	12	13	14	15	16	17	
City	OS	ASN	Transport	Product	Version	Web Server	Website Title	
		ASXXX7	tcp				401 Unauthorized	

## 其他常用的Shodan指令

● 顯示目前帳號的資訊
Shodan info

asoc@master:~ asoc@master:~\$ shodan info Query credits available: 0 Scan credits available: 0

● 顯示使用者的IP
 →shodan myip

![](_page_42_Picture_4.jpeg)

 ● 顯示一個IP所有可用的詳細資訊
 Shodan host <</p>

![](_page_42_Picture_6.jpeg)

### Shodan資料來源

●Shodan的掃描伺服器在全世界都有建置

●每天都有在更新資料

### ●資料限制:

1. 不保證可以在短時間內獲得最新資訊,最晚一個月內會更新資料

2. 每次更新時,上次的資料不一定馬上刪除

### 原始資料內容(部分敏感資訊已經刪除)

{"\_shodan": {"id": "0528b36c-30d0-4d85-a7da-1caeeca532c1", "options": {}, "ptr": true, "module": "onvif", "crawler": "f7946cbe2dc20c40fcbcb81ad90aa01731b690ab"}, "hash": -512260510, "os": null, "opts": {}, "ip": 2OOOOOOOO8, "isp": "Taiwan Academic Network (TANet) Information Center", "port": 3702, "hostnames": [], "location": {"city": "XXXXX", "region\_code": "06", "area\_code": null, "longitude": 120.4488999999998, "country\_code3": "TWN", "country\_name": "Taiwan", "postal\_code": null, "dma\_code": null, "country\_code": "TW", "latitude": 23.47919999999999}, "timestamp": "2019-05-08T03:20:14.291096", "domains": [], "org": "Taiwan Academic Network (TANet) Information Center", "data": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<SOAP-ENV:Envelope xmlns:SOAP-ENV=\"http://www.w3.org/2003/05/soap-envelope\" xmlns:SOAP-ENC=\"http://www.w3.org/2003/05/soap-encoding\" xmlns:wsa=\"http://schemas.xmlsoap.org/ws/2004/08/addressing\" xmlns:d=\"http://www.onvif.org/ver10/network/wsdl\"><SOAP-ENV:Header><wsa:MessageID>uuid:1419d68a-1dd2-11b2-a105-001655099A2B</wsa:To><wsa:To SOAP-ENV:mustUnderstand=\"true\">urn:schemas-xmlsoaporg:ws:2005:04:discovery</wsa:To><wsa:Action SOAP-ENV:mustUnderstand=\"true\">http://schemas.xmlsoap.org/ws/2005/04/discovery/Hello</wsa:Action></SOAP-

ENV:Header><SOAP-ENV:Body><d:Hello><wsa:EndpointReference><wsa:Address>urn:uuid:1419d68a-1dd2-11b2-a105-

001655099A2B</wsa:Address></wsa:EndpointReference><d:Types>dn:NetworkVideoTransmitter</d:Types><d:Scopes >onvif://www.onvif.org/type/video\_encoder onvif://www.onvif.org/name/IPCam

onvif://www.onvif.org/hardware/VIH\_Series onvif://www.onvif.org/location

onvif://www.onvif.org/Profile/Streaming</d:Scopes><d:XAddrs>http://140.XXX.XX.206:81/onvif/device\_service</d:X Addrs><d:MetadataVersion>1</d:MetadataVersion></d:Hello></SOAP-ENV:Body></SOAP-ENV:Envelope>\n", "asn": "ASXXX9", "transport": "udp", "ip\_str": "140.XXX.XX.206"}

### 原始資料欄位介紹 (jsonkat)

### ●Shodan儲存的資料為Banner資訊,在Developers頁面中有詳細說明

🔏 Shodan Developer	Dashboard	API Reference	Integrations	Pricing	Contact Us			🐣 My Account
	Bai	nner Sna	acificat	ion				
Introduction	Dai	inici Sp	centeat					
Clients								
	The bar	nner is the main type	e of information 1	hat Shodan p	rovides through t	ne REST and Streaming API. This document ou	utlines the various prop	perties that
REST API Documentation	are alw	ays present and whi	ich ones are optio	onal.				
Streaming API Documentation								
EXPLOITS API DOCUMENTATION	Prop	perties						
Introduction			asn (S	tring] The au	tonomous system	n number (ex. "A\$4837")		
REST API Documentation			data [S	tring] Contai	ns the banner in	formation for the service.		
_			ip [h	nteger] The IF	address of the	host as an integer.		
APPENDIX			ip_str [S	tring] The IP	address of the h	ost as a string.		
Banner Specification			ipv6 [S	tring] The IP\	6 address of the	host as a string. If this is present then the "i	p" and "ip_str" fields v	wont be.
Exploit Specification			port [li	nteger] The p	ort number that	the service is operating on.	the UTC times on F	
			umestamp [5	014-01-15T0	1estamp for whe 5:49:56 283713"	n the banner was relched from the device in	i the OTC timezone. Ex	xampie:
		ł	ostnames [S	tring[]] An ar	rav of strings cor	ntaining all of the hostnames that have been	assigned to the IP ad	dress for
			th	is device.				
			domains [S	tring[]] An ar	ray of strings cor	ntaining the top-level domains for the hostna	ames of the device. Th	nis is a
			ut	ility property	in case you wan	t to filter by TLD instead of subdomain. It is	smart enough to hand	dle global
			Tl.	Ds with seve	ral dots in the do	omain (ex. "co.uk")		
		location	location [C	)bject] An obj	ect containing a	l of the location information for the device.		
		location.	cation city [S	tring] The na	me of the city wh	pere the device is located		
		location.cou	intry code IS	tring] The 2-I	etter country co	de for the device location.		
		location.cour	ntry_code3 [S	tring] The 3-I	etter country co	de for the device location.		
		location.cou	ntry_name [S	tring] The na	me of the counti	y where the device is located.		

來源網址: https://developer.shodan.io/api/banner-specification

網路攝影機的特性

近期上課所學到的資訊,經過整理後的重點

主要特徵

### 1. 支援ONVIF協定

2. 即時影音串流

![](_page_47_Picture_3.jpeg)

![](_page_47_Picture_4.jpeg)

ONVIF简介

●ONVIF(英文全名: Open Network Video Interface Forum),由Axis、Bosch Security Systems 以及Sony等三家公司在2008年合作建立的全球開放性論壇

 其宗旨是促進不同廠牌的監控設備與系統的整合,幫助生產製造商、軟體開發商及獨立 軟體供應商之間的可互通性

 ONVIF採用統一開放的標準作為IoT設備、儲存設備與管理系統之間的溝通協定,易於整 合及擴充,因此逐漸為國內外視訊監控系統建置單位採用

![](_page_48_Picture_4.jpeg)

圖片來源:<u>https://www.onvif.org/</u>

ONVIF規範

●大部分的網路攝影機會遵守ONVIF規範(可參考下面兩張圖)

●此規範規定要符合和支援XML及WSDL格式

		闷叩死俗						
		型號:						
	操作系統	嵌入式RROS設計 · 雙核心32位DSP(H3518E)完美壓縮						
系 統	系統安全	三級用戶權限管理						
	最大用戶數	4個用戶同時觀看						
	圖像傳感器	1/4英吋100萬像素運行CMOS Sensor 1280x720 Pixels						
	傳感器性能	支援自動白平衡 · 自動加強控制 · 自動背光補償						
咸雁哭	雜訊比	小於50dB						
100 // UK AA	鏡頭	f=3.6mm/F=2.0 標準紅外線鏡頭						
	夜視	11颗850nmΦ5mm红外線燈·夜視10-15公尺						
	最低照度	0.1Lux/F1.6(彩色模式),0.01Lux/F1.6(黑白模式)						
	壓縮標示	H.264視訊編碼·支持ONVIF協定						
视频	分辨率	支持雙編碼流, 主碼流: 1280*720 子碼流: 640*480						

商品名稱:網路攝影機
商品型號:
商品型態:IP Camera
感應器:CMOS
Technology:紅外線
特色:室外攝影機
解析度:1080P
速率:15fps、25fps
格式:H.264、MJPEG
鏡頭:3.6mm(固定焦距)、2.4mm(光圈)
夜視距離: 5~10公尺
影像咸應器:1/2.7" CMOS
ONVIF 2.0 協議新增 NVR 產品
儲存:IF卡 64G (MAX)
網路連接(有線、WiFi)
1個RJ45以太網介面,10/100M自適應
支援 P2P
支援 AP
支援HTTP、FTP、TCP/IP、UDP、SMTP
、PPPOE、DHCP、DDNS、UPnP等網路
協議

50

### ONVIF配置文件說明

- ●ONVIF現今制定了六種配置文件(Profile),英文大寫字母作區別(A、C、G、Q、S、T)
- ●有定義門禁系統、網路監控設備、視訊儲存及管理系統的通訊方式與資料流
- ●定義網路攝影機相關的協議是 Profile S

С	ח(	VIF®	About -	Join <del>-</del>	Benefits 👻
P	ofiles &	Specifications			Ø
	ONV	/IF Profiles			Ø
		Profile A			٥
		Profile C			0
		Profile G			٥
		Profile Q			Ð
		Profile S			Ð
		Profile T			0

圖片來源:\_https://www.onvif.org/profiles/

Profile S說明

- ●規範相容ONVIF協定中影像管理系統和裝置共用的共用功能,這些系統和 裝置包括通過IP網路發送、配置、請求或控制媒體資料流程的IP攝影機或 編碼器
- ●有規範IP攝影機特定功能,例如搖攝(攝影機的方向控制)、變焦控制(鏡頭)、 音訊流(輸入或輸出聲音)和指定中繼點輸出影像

### 網路攝影機相關特徵

- 可能出現的關鍵字:ONVIF、IP cam、Webcam、RTSP、RTP
   特殊專用port:udp 3702
- 3. 影像串流port:tcp 554

							Time	Source	S	rc port Destination		Dst port Protocol	Length Info	
Time	Source	Src port	Destination		Dst port Protocol	Length Into	5788 2019-06-06 12:02:33.258974	140	.155	6970 19	2	54228 RTP	1490 PT=DynamicRTP-Typ	
502 2019-06-06 12:02:11.982232	192.	2 629	50 140.	.155	80 TCP	66 62950 → 80 [SYN] Se	5789 2019-06-06 12:02:33.258974	140	.155	6970 19	2	54228 RTP	230 PT=DynamicRTP-Typ	
503 2019-06-06 12:02:11.982346	192	2 629	51 140.	.154	80 TCP	66 62951 → 80 [SYN] Se	5790 2019-06-06 12:02:33.259091	192	2	63051 14	.155	554 TCP	54 63051 → 554 [FIN,	
504 2019-06-06 12:02:11.985429	192	2 542	21 239.	5.250	5702 UDP	773 54221 → 3702 Len=73	5791 2019-06-06 12:02:33.263134	140	.155	554 19	2	63051 KISP	119 Reply: RTSP/1.0 2	
505 2019-06-06 12:02:11.985430	192	2 542	13 239.	5.250	3702 UDP	791 54213 → 3702 Len=74	5792 2019-06-06 12:02:33.263134	140	.155	554 19	2	63051 TCP	54 554 $\rightarrow$ 63051 [FIN,	
506 2019-06-06 12:02:11.985460	192	2 542	17 239.	5.250	3702 UDP	787 54217 → 3702 Len=74	5793 2019-06-06 12:02:33.263193	192	2	63051 14	.155	554 TCP	54 63051 → 554 [RST,	
507 2019-06-06 12:02:11.985603	140	.157	80 192.	2	62949 TCP	66 80 → 62949 [SYN, AC	5794 2019-06-06 12:02:33.263287	192	2	63051 14	.155	554 TCP	54 63051 → 554 [RST]	
508 2019-06-06 12:02:11.985753	192	2 629	49 140.	.157	80 TCP	54 62949 → 80 [ACK] Se	5795 2019-06-06 12:02:33.263427	192	2	63090 14	.155	80 TCP	66 63090 → 80 [SYN]	
509 2019-06-06 12:02:11.985976	140	.154	80 192.	2	62951 TCP	66 80 → 62951 [SYN, AC	5796 2019-06-06 12:02:33.267451	140	.155	80 19	2	63090 TCP	66 80 → 63090 [SYN.	
510 2019-06-06 12:02:11.986068	192	2 629	51 140.	.154	80 TCP	54 62951 → 80 [ACK] Se	Frame 5791: 119 bytes on wire (952	hits) 11	9 hytes /	cantured (952	hits)			
Frame 504: 773 bytes on wire (6184	bits), 773	bytes captu	ured (6184	bits)			There shows in the optical on the table of the shows captured ( $32$ of table) There is a shown of the shows the table of the shows the table of the shows							
Ethernet II, Src: IntelCor_06:91:f	e (b4:6b:fc:	:06:91:fe),	Dst: IPv4	mcast_7f:f	f:fa (01:00:5e:7f:	f:fa)	Internet Protocol Version 4, Special 4, Section 2, Det 102, 162, 12, 1102, 100, 100, 100, 100, 100, 10							
Internet Protocol Version 4, Src:	192.168.1.2,	, Dst: 239.2	255.255.25	9			Transmission Control Dastasal Con		Det De	. 192.108.1.2	. 1470 4	-k. (02   -n. (5		
Jser Datagram Protocol, Src Port:	54221, Dst P	Port: 3702					Paol Time Streaming Partocal							
Data (731 bytes)							Real lime Streaming Protocol							
00 01 00 5e 7f ff fa b4 6b fc 06	91 fe 08 00	45 00	^k	· · · E ·			000 b4 6b fc 06 91 fe 78 44 76 f0	a8 58 08	00 45 00	·k···xD v··	X··E·			
10 02 f7 4c 2c 00 00 01 11 b9 25	c0 a8 01 02	efff ··	L,···· ·%·		<u> </u>	0700	010 00 69 e3 00 40 00 3a 06 bb d8	8c 70 53	9b c0 a8	·i··@·:· ···	pS···			
20 ff fa d3 cd 0e 76 02 e3 d0 3d 3c 73 3a 45 6e 76 ·····v···= <s:env ()2<="" port:3="" td=""><td colspan="7"></td></s:env>														
80 65 6c 6f 70 65 20 78 6d 6c 6e	73 3a 73 3d	22 68 el	ope xm lns.	:s="h			02 2d f2 42 00 00 52 54 53 50	2f 31 2e	30 20 32	·-·B··RT SP/	1.0 2	POI	1.554	
10 74 74 70 3a 2f 2f 77 77 77 2e	77 33 2e 6f	72 67 tt	p://ww w.w	13.org			040 30 30 20 4f 4b 0d 0a 43 53 65	71 3a 20	36 0d 0a	00 OK · C Seq	l: 6··			
0 2f 32 30 30 33 2f 30 35 2f 73	6f 61 70 2d	65 6e /2	003/05 /sc	ap-en			050 44 61 74 65 3a 20 46 72 69 2c	20 41 70	72 20 31	Date: Fr i,	Apr 1			
	<u> </u>		1				60 31 20 31 39 38 30 20 31 37 3a	34 30 3a	35 31 20	1 1980 1 7:4	40:51			
							070 47 4d 54 0d 0a 0d 0a			GMT····				

![](_page_53_Picture_0.jpeg)

## 結合Shodan尋找網路攝影機

根據前一頁的網路攝影機特徵資料,搭配SHODAN資料找出IP CAM

收集資料

1. 用掃描工具去掃IP,得到資料(例如:nmap)

- 優點:資料可以隨時更新
- 缺點:可能會被阻擋、視為網路攻擊等
- 2. 從Shodan下載資料
  - 優點:省時間去取得資訊(全世界)
  - 缺點:資料不能隨時更新、需要點數(金錢)

![](_page_54_Picture_7.jpeg)

![](_page_54_Picture_8.jpeg)

分析資料

- 1. 轉成csv、xlsx等格式,做後續的資料分析
- 2. 參考網路攝影機相關特徵,對幾個欄位找尋相關的特徵,列 出可能是網路攝影機的IP

A	В	С	D	E	F	G	Н		J	К	L	М		Ν	0	Р	Q	R	S	Т
data	hostnames	ip	ip str	ipv6	org	isp	location.o	location	loca	locati	locatie	<u>0S</u>	asn		port	tags	timestamp	transport	product	vers
HTTP/1.0 401 Unauthorized	140.1		Natie	Taiwa	TW		Taiw	23.5	121		A		80		2019-06-05T	tcp				
Date: Thu, 01 Jan 1970 00:00		140.1		Taiw	Taiwa	TW		Taiw	23.5	121		A		8080		2019-06-05T	tcp	webcam 7 http:	t I	
Connection: close		140.1		Natie	Taiwa	TW		Taiw	23.5	121		A:		80		2019-05-29T	tcp			
WWW-Authenticate: Basic realm="webcam"																				
Content-Type: text/ <u>html</u>																				

3. 針對這些IP列表,利用瀏覽器、ONVIF相關程式檢驗這些IP是 否為網路攝影機

![](_page_56_Picture_0.jpeg)

Ē	÷.	開始	È	$\times$ + $\vee$	
$\leftarrow$	$\rightarrow$	×	ŵ	⊕   140.	
				Windows 安全性 X	1
				Microsoft Edge	
				伺服器 140. 正要求您提供使用者名稱與密碼。	
				該伺服器也回報 "webcam"。	
				警告:將在不安全的連線上使用基本驗證來傳送您的使用者名稱與 密碼。	
				使用者名稱	
				密碼	
				確定取消	

### ONVIF檢查程式: ONVIF Device Manager介紹

- ●是一個可以檢查網路中的網路視訊設備(如IP cam)、網路儲存系統(如NAS) 是否有符合ONVIF協議的程式(程式名稱縮寫ODM)
- ●是用C#開發,支援英語、俄語兩種語系
- ●免費軟體,有開放原始碼
- ●目前找到的最新版本是2.2.250 (2016.11.15)
- ●預設會檢查內網網段(EX:192.168.X.X/24),

如果在內網中找到ONVIF協定設備,它會自動 列在Device list中

![](_page_57_Picture_7.jpeg)

![](_page_58_Picture_0.jpeg)

![](_page_58_Picture_1.jpeg)

- 1. 按下Add
- 2. 新增要連線的IP(修改綠圈處)
- 3. 根據跳出的訊息,決定下一步

### 狀況一: 沒有出現ONVIF標誌

- ●出現這個訊息,可能有兩種情況:
- 1. 連線被阻擋
- 2. 不是IP Cam
- ●可能要配合瀏覽器登入檢查,來確

認此IP是否為IPCam

![](_page_59_Figure_6.jpeg)

### 狀況二:需要登入設備

●出現ONVIF標誌及一些連結,但是出現授權(登入)相關問題,此時這個IP 有高機率是IPCam

如果要更詳細檢查,則可以用一些預設帳號密碼去嘗試登入

一旦用預設帳號密碼登入該設備,請盡快提醒設備負責人修改帳號密碼

![](_page_60_Picture_4.jpeg)

### 狀況三:直接登入IP Cam

此狀況較為嚴重,這說明這個設備可以利用ODM直接觀看攝影
 機內容、修改帳號密碼權限,需要立即通知設備負責人做出修正。

![](_page_61_Picture_2.jpeg)

總結

▶ Shodan 是一個非常適合找尋IoT 設備的大資料庫

▶業界也是利用ONVIF協定去找網路攝影機

▶目前還沒有找到可自動化且大量確認網路攝影機的方法

![](_page_63_Picture_0.jpeg)

謝謝大家