

NASOC 二線工程師 林宜進

E-mail: <u>tjline01@asoc.cc.ntu.edu.tw</u> 日期: 2021/12/14

大綱

- 1. Shodan介紹
- 2. Shodan基本操作
- 3. 下載Shodan資料
- 4. 簡易的Shodan資料分析

Shodan介紹

什麼是Shodan?

●Shodan是一個提供網際網路中IoT設備資訊的搜尋引擎

●透過過濾器(關鍵字)搜尋,可找到特定IoT設備資訊

●被CNN稱作「網際網路上最危險的搜尋引擎」

●官方網址: <u>https://www.shodan.io/</u>



CNN BUSINESS Markets Tech Media Success Video

"Shodan: The scariest search engine on the Internet" (from @CNNMoney): on.cnn.com/1egSoNY

上午1:37 · 2013年8月3日 · Twitter Web Client

原本縮網址已經無法連結,而原始連結如下: https://money.cnn.com/2013/04/08/technology/s ecurity/shodan/

The Cybercrime Economy

Shodan: The scariest search engine on the Internet

by David Goldman @DavidGoldmanCNN

April 8, 2013: 1:41 PM ET

find it. That's not true."



CNNMoney Sponsors

Falu Falur

These are your 3 financial advisors near you

This site finds and compares 3 financial advisors in your area

Check this off your list before retirement: talk to an advisor

Answer these questions to find the right financial advisor for you

Find CFPs in your area in 5 minutes

	2010	1.0

An Insane Card Offering 0% Interest Until Nearly 2020

That's according to John Matherly, creator of Shodan, the scariest search engine on the Internet.

創辦人有關的資訊

●創辦人為John Matherly,他在2009年建立Shodan搜尋引擎

- ●此名稱引用自遊戲「網路奇兵」(System Shock)中,具有邪惡人工智慧的電腦— SHODAN
- ●創辦人有發行一本官方電子書「Complete Guide to Shodan」





資料來源: <u>https://en.wikipedia.org/wiki/System_Shock</u>



資料來源: <u>https://www.youtube.com/watch?v=n1ChelLmQIc</u>



Complete Guide to Shodan

Collect. Analyze. Visualize. Make Internet Intelligence Work For You.

Complete Guide to Shodan

Collect. Analyze. Visualize. Make Internet Intelligence Work for You.

John Matherly

This book is for sale at http://leanpub.com/shodan

This version was published on 2017-08-23

Leanpub

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback pivot until you have the right book and build traction once

Contents

Introduction	1
All About the Data	1
Data Collection	3
SSL In Depth	4
Beyond the Basics	7
Web Interfaces	10
Search Query Explained	10
Introducing Filters	11
Shodan Search Engine	12
Shodan Maps	18
Shodan Exploits	25
Shodan Images	26
Evercises: Website	28
	20
External Tools	29
Shodan Command-Line Interface	29
Maltego Add-On	37
Browser Plug-Ins	37
Exercises: Command-Line Interface	38
Developer API	39
Usage Limits	39
Introducing Facets	40
Getting Started	41
Initialization	41
Search	41
Host Lookup	43
Scanning	43
Real-Time Stream	44
Network Alert	45
Example: Public MongoDB Data	48
Example Fublic Hongood Data	53
Lacterses should Art	33

如何使用 Shodan(攻擊方)?

●利用Shodan查詢服務, 找出特定IoT設備

●結合滲透工具、自製 攻擊程式做精準打擊 **Compromised Docker Hosts Use Shodan to Infect More Victims**

By Sergiu Gatlan

🛅 May 30, 2019 🛛 02:46 PM 🔲 0



Hackers are scanning for Docker hosts with exposed APIs to use them for cryptocurrency mining by deploying malicious self-propagating Docker images infected with Monero miners and scripts that make use of Shodan to find other vulnerable targets.

The cryptojacking campaign targeting exposed Docker hosts was unearthed by Trend Micro researchers after a Docker image containing a Monero (XMR) cryptocurrency miner binary was deployed on one of their honeypots.

This type of attack is definitely nothing new seeing that researchers from Imperva discovered a similar campaign abusing the CVE-2019-5736 runc vulnerability to deploy cryptominers during early-March.



如何使用 Shodan(防守方)?

 當發生CVE漏洞、0day攻擊時,利用
 Shodan查詢,找出符
 合條件的IoT設備

 研究漏洞發生原因, 尋找或自行開發漏洞 檢測程式,透過檢測 找出存在漏洞的設備, 並通知單位盡速修補。

AT&T Reveals Malware Targeting Millions of Routers, loT Devices The malware, BotenaGo, has more than 30 different functions. We Pathaniel Mott Nov. 13, 2021, 12:22 a.m.

10

AT&T has revealed malware that could affect millions of routers and Internet of Things devices.

The company's Alien Labs threat intelligence unit dubbed the malware BotenaGo because it's written in

Go, a programming language that Google designed specifically with networking in mind. It's also

capable of creating botnets that function across a variety of device types.

0 0 0110

0

AT&T Alien Labs says BotenaGo can exploit up to 30 different vulnerabilities against its targets. The company used Shodan, a search engine used to look up internet-connected devices, to determine that

millions of devices could be affected by at least some of the malware's functions.

資料來源: https://in.pcmag.com/security/146125/att-reveals-malware-targeting-millions-of-routers-iot-devices

Shodan基本操作

前言

使用Shodan服務前,需要建立一個使用帳號,否則有些功能會受到限制
Shodan帳號有不同等級,但免費帳號就可以使用一些基本功能
接下來會從註冊帳號開始,到如何操作Shodan網頁上的搜尋功能

註册Shodan帳號-1





SHODAN Account Register Create Account Username Password	
Create Account Username Password	
Create Account Username Password Password	
Username Password	
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	ι,
By creating an account you are agreeing to our Privacy Policy and Terms of Use 可不勾選	
Спеате	





註冊Shodan帳號-4

- ●到註冊的信箱收信,總共會收到兩封信:
 - ●第一封信是帳號啟動確認信,請點擊信中的連結啟動帳號
 - ●等啟動完成後會收到第二封信,是帳號建立完成信,此時就可以登入Shodan帳號

	weicome to Shodan
	Shodan <no-reply@shodan.io> 上午 09:27</no-reply@shodan.io>
Shodan Account Activation	收件者: Hi You've successfully created an account on Shodan! Below you will find all important
Shodan <no-reply@shodan.io> 上午 09:26</no-reply@shodan.io>	account information to login, make sure to keep this email in your archive for later. Account Information
收件者:	URL: https://account.shodan.io Username:
Click on the link below to activate your Shodan account.	Not sure where to get started? Check out the following to get familiar with Shodan:
URL: https://account.shodan.io/activate/	Discover Shared Searches Complete Guide to Shodan book Short Videos for common tasks Hele Center
If you have any problems activating your account or have questions about Shodan, please contact support@shodan.io	If you have any questions or suggestions let us know - we're here to help!







確認Shodan帳號資訊

SHODAN Explore Downloads	Pricing 🛃 Search	٩	Account	SHODAN AC	count		
Dachboard					Cvervlew	Account Overview	
Dashibuard					Settings Change Reconnect	API Key	JT. 7
Getting Started	>_ ASCII Videos	Access	_		Redeem Gift Code		
What is Shodan? Search Query Fundamentals Working with Shodan Data Files LEARN MORE	Setting up Real-Time Network Monitoring Measuring Public SMB Exposure Analyzing the Vulnerabilities for a Network VISIT THE CHANNEL	How to Download Data with the API Looking up IP Information Working with Shodan Data Files DEVELOPER PORTAL	→				RESET API KEY
SETUP NETWORK MONITORING	Filters Cheat Sheet		_			Display Name	ET
BROWSE IMAGES	Shodan currently crawls nearly Here are a few of the most com started.	1,500 ports across the Internet. Imonly-used search filters to get				Email Member	tji m No
MAP VIEW	Filter Name Descripti	on Example				Export Credits	0



	Free	Membership	Corporate API	Enterprise Data License		Compare Featu	Compare Features	Compare Features	Compare Features	Compare Features
iccess to Shodan Search Engine lity to search on Shodan using basic filters.	~	~	~	~			Membership	Membership Freelancer	Membership Freelancer Small Business	Membership Freelancer Small Business Corporate
udes Shodan Maps and Shodan Exploits.					Price		\$49 (one-time)	\$49 (one-time) \$59/ month	\$49 (one-time) \$59/ month \$299/ month	\$49 (one-time) \$59/ month \$299/ month \$899/ month
grations with Popular Tools					Query credits (per month)		100	100 10,000	100 10,000 200,000	100 10,000 200,000 Unlimited
cools that integrate out of the box with Shodan.	\checkmark	\checkmark	\checkmark	\checkmark	Scan credits (per month)		100	100 5,120	100 5,120 65,536	100 5,120 65,536 327,680
blore the Internet Visually		·			Monitored IPs		16	16 5,120	16 5,120 65,536	16 5,120 65,536 327,680
Shodan Images to browse screenshots gathered n devices around the world.		\checkmark	\checkmark	\checkmark	Available search filters	A	All except vuln and tag	All except vuln and tag All except vuln and tag	All except vuln and tag All except vuln and tag All except tag	Allexcept vuln and tag Allexcept vuln and tag Allexcept tag All
					Number of users	1		1	1 1	1 1 1
nple Website Downloads ith the click of a button you can download search		7			Shodan Search pages	20		20	20 200	20 200 200
sults to your local computer.		*	Ŷ	Ť	Shodan Monitor	~		~	✓ ✓	v v v
eep IP Enrichment					Shodan Trends	~		~	× ×	✓ ✓ ✓
bur network by looking them up in Shodan.		~	\checkmark	\checkmark	Private firehose	~		\checkmark	× ×	v v v
n-Demand Scanning					IP lookups	~		~	✓ ✓	у у у У
Ask Shodan to scan your Internet-facing devices to validate your firewall and make sure existing issues have					Batch IP lookups					×
been fixed.			•		Bulk Data					
Real-Time Network Monitoring					InternetDB					
Keep track of the latest services discovered on your external network in real-time.				\checkmark	Full firehose					
					Internet scanning API					

該如何使用Shodan搜尋?



搜尋方法一:參考官方範例



搜尋方法二:參考Explore範例



網頁可使用的過濾器列表



 hostname 		 ssLcipher.bits
■ ip	Bitcoin	 ssLcipher.name
■ isp	 bitcoin.ip 	 ssLcipherversion
■ link	 bitcoin in count 	∎ sslja3s
∎ net	 bitcoin port 	■ ssLjarm
■ org	 bitcoinversion 	 sslversion
■ OS	- Ditconiversion	
■ port		
 postal 		NITD
product	Restricted	NIP
 region 		■ ntp.ip
■ scan	available to users of higher API plans.	 ntp.ip_count
shodan module		 ntp.more
■ state	■ tag	 ntp.port
 version 	 vuln 	
- 10131011		
		Telnet
	SNMP	
Screenshots	snmp.contact	 telnet.do
 screenshot.label 	 snmplocation 	 telnet.dont
	 snmp.name 	 telnet.option
		 telnet.will
Cloud		 telnet.wont
Cioua		
 cloud.provider 		
 cloud.region 		SSH
cloud.service		- cch bacch
		 SSNIndSSN
		SSNIVDE

常用的過濾器說明

過濾器	說明	範例
net	搜尋指定的ip 位置或是網段	net :59.120.179.0/24
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:us
org	搜尋指定的組織或公司	org:google
hostname	搜尋指定的網域名稱	hostname:azure

網頁搜尋範例-問題篇

- ●假設現在要搜尋具備下列條件的IoT設備:
 - 1. 設備在台灣
 - 2. 有開啟FTP服務

🔗 Shodan	Explore	Downloads	Pricing 🗗	請問這裡(搜尋欄位)要輸入甚麼?	٩	

網頁搜尋範例-解答篇

- ●假設現在要搜尋具備下列條件的IoT設備:
 - 1. 設備在台灣 ----->country:tw
 - 2. 有開啟FTP服務 ----->port:21 (FTP服務預設埠號)

🔗 Shodan	Explore	Downloads	Pricing 🖻	country:tw port:21	Q

●備註一:在網頁搜尋時,可以搭配多種過濾器使用,來限縮目標範圍
 ●備註二:過濾器使用先後次序無關,不會影響找到設備數量

Shodan	Explore	Downloads	Pricing 🛃	country	r:tw por	t:21			Q	Account
otal results 7 5,148 op cities		窳 View Report New Service out Shodan	t 🕹 Downloa e: Keep track of Monitor	d Results what you	i His have co	storical	Trend ed to the	Interne	w on Ma t. Check	p
Taipei Taichung Banqiao Taoyuan City Tainan More	29,140 7,559 6,620 4,702 4,647	211.21.155.49 211.21.155.4 9 hinet-ip.hine t.net Data Communication Business Group, d Taiwan, Taipei	220-FileZilla Se 220-written by T 220 Please visit 530 Login or pas 214-The followir ABOR ADAT DELE EPRT	erver 0.9.6 im Kosse (https://f sword inco g commands ALLO AF EPSV	50 beta (tim.koss Filezilla prrect! ; are rec PPE AUT	se@file a-proje cognize TH CD	zilla-pr ct.org/ d: UP CLN	2021- oject.or T CWD	12-07T23: g)	18:07.211127
OP ORGANIZATI Chunghwa Tele Co.,Ltd. Ministry of Education Con Center Data	0005 ecom 45,810 nputer 11,803	61.247.173.38 static-ip-39-17 3-247-61.rev.d yxnet.com Diykian.com(TW)Lt	220 ProFTPD 1.3. 530 Login incorr 214-The followir CWD XCWD EPRT EPSV XRM	2 Server (rect. og commands CDUP) ALLO* F	(ProFTPD s are rec CCUP S RNFR F	Defaul cognize SMNT* RNTO	t Instal d (* =>' QUIT DELE	2021- lation) s unimpl PORT MDTM	12-07T23: [61.247.1 emented): PASV RMD	17:42.561137 173.39] :



前言

- 如果在短時間內分析大量資料、找到特定目標,不可能單靠網頁就可以辨到
 資料分析前,最重要的步驟就是收集資料
- ●接下來會逐步解說如何從Shodan搜尋引擎下載資料

😪 Shodan	Explore	Downloads	Pricing 💋	Server: WEBCAM	٩	106.75	.71.81 (Regular View) >_ Raw Data (*)	Na History	inmofang) Guanz	huang © C	Diarte OpenMapTi	les Satellite	e © MapTi	er © Open	TreetMap contributors
						// TAGS: honeypo							// LA	STUPDA	TE: 2021-12-10
				🛍 View Report 🛛 🕹 Downlo	ad Results 🔟 Historical Trend 🕮 Browse Images 🖽 View on Map										
8,087				New Service: Keep track of	of what you have connected to the Internet. Check out Shodan Monitor	General	Information	놂이	oen Por	ts					
				BIG-IP®- Redirect BIG.75.71.81 Shanghai UCloud Information Technology Company Limited	HTTP/1.1 200 OK Content-Length: 60260	Country	China	84	222	264	503	995	1200	2050	2081
				China, Beijing	X Gogda Cola: Inf. X-Powered Py: Servlet 2.4; Servlet/2.5 JSP/2.1 ,JBoss-4.2.3.GA (build: SWNTag=J0 X-Jenkins: 2.0 X-Jenkins-Cli2-Port	City	Beijing	2121	2222	2323	2560	3108	3403	3690	4282
China Switzerland	€.	2,5 1,8	76 39	164.128.164.65	HTTP/1 1 200 OK	Organization	Shanghai UCloud Information Technology Company Limited	4664	4782	5000	5005	5801	6511	8087	8106
United States Singapore		1,5 4	99 37	ent.cust.swisscom.ch Swisscom (Schweiz) AG	ert oust swisscom ch Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A1045. Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A1045.	China Mobile Communications Group Co., Ltd.	8111	8443	8822	8834	8836	8990	9014	9443	
More			,,	honeypot		ASN	AS9808	11300	16010	20256	27015	28017	32400	32764	44158
TOP PORTS 8081 443		4) 31)4)8	190.131.40.94 C hfce-190-131-40-94.customer.cl aro.com.ec Ecuadorlelecom S.A.	HTTP/1.1 200 OK Server Cross Meb Server Content-length: 1385			50000	50070	52869	54138	62078			
8080 80 9000		2: 2. 1:	35 23 30		Chiene (yp): Cetymon (html) (head)		ILARJS	// 84 / TC	PC			56993	31889 2	821-12-07	17:50:44.680657
More TOP ORGANIZATION Swisscom (Schw	S Biz) AG	1,8	56		<pre>clif(e)weetaw(rite) cscript language="JavaScript") if(navigator.platform.tolowerCase().indexOf("blackberry") != -1) { document.location.href = "BlackBerry.htm"</pre>			HTTP/1. Content X-Drupa X-Power	1 200 OK -Length: (1-Cache: F	50269 HIT rylet 2 4:	Servlet	/2 5 15P/	2 1 1Bos	s_4 2 3 6) (build: SV
Asia Pacific Netw Tencent cloud co	ork Information mputing (Beijin	Center, Pty. Ltd. g) Co., Ltd. 903 ^{1,21}	33		} else if(navigato	🖄 Vulnera	bilities	NTag=JB lRewrit	oss_4_2_3 er.NET 1.7	_GA date=2 7.0,Pleski	200807181 in,ARR/2	417)/JBoss .5,ZendSer	sWeb-2.0, rver/9.1.	PHP/5.4.3	5,ASP.NET,Ur

下載資料的方法

- ●Shodan有雨種方式可以下載資料
 - 1. 在網頁上直接下載
 - 2. 使用命令列(CLI)並透過Shodan API下載

●但是下載Shodan資料需要點數

🔏 Shodan	Explore	Downloads	Pricing 🖉	Search	٩	Account	achillean@demo:~\$ shodan download -h Usage: shodan download [OPTIONS] <filename> <search query=""></search></filename>
Dow	nload	ls					Download search results and save them in a compressed JSON file. Options:
8	Note: You	haven't yet creat	ed any downlo	ads.	HELP 10,000 Query Credits Available 1 query credit lets you download up to 100 results. The query credit usage resets at the star of every month. To get more query credits che out our plans at:	it t ck	limit INTEGER The number of results you want to download1 to download all the data possible. -h,help Show this message and exit. achillean@demo:~\$ achillean@demo:~\$ achillean@demo:~\$ achillean@demo:~\$ achillean@demo:~\$ achillean@demo:~\$ shodan downloadlimit 1000 mongodb.json.gz product:mongodb Search query: product:mongodb Search query: product:mongodb Total number of results: 21493 Query credits left: 100000 Output file: mongodb.json.gz [] 0%

如何查詢帳號內持有的點數?





官方點數消耗說明

Shodan Credits Explained

At Shodan, the amount of access you get to data and other features of the infrastructure depend on how many **credits** your account has available. There are 2 types of credits available at Shodan:

- Query credits
- Scan credits

Note: Export credits are deprecated and can nolonger be purchased.

Query Credits

Query credits are used to download data via the <u>website</u>, <u>command-line interface</u> or the API. If you're using the CLI or API then query credits are deducted if one of the following 2 conditions is met:

- A search filter is used
- Page 2 or beyond is requested

Query credits **renew at the start of the month** and provide the following amount of data:

1 query credit lets you download 100 results

Here are a few search queries and how many query credits they consume:

- apache: search query without any filters and 1st page of results no query credits used
- product:mongodb: searches for MongoDB database servers and uses 1 query credit
- 3rd page of **apache**: requesting the 3rd page costs **1 query credit**
- 5th page of product:mongodb: requesting the 5th page of search results for MongoDB: 1 query credit

網頁下載的變化: 捨棄 export credits



過去的購買Export Credits金額



下載方法一:從網頁直接下載

●假設現在要下載port:502的資料

SHODAN E	Explore Dow	vnloads Prici	ing 🗗 port:502	Q Account	🔏 Shodan	Explore	Downloads	Pricing 🗗	port:502		٩	Account
total results 57,597		窳 View Report New Service:	Download Results I Historical Trend Browse Ima Keep track of what you have connected to the Internet. Check	ages	Do	wnloa	d Resu	lts		FAQ		
		116.58.181.128 116.58.181.128.st atic.zoot.jp INTERLINK Co.,LTD. Japan, Nagoya ics	B Unit ID: Ø Slave ID Data: Illegal Data Address (Error) Device Identification: Illegal Data Address (Error) Unit ID: 1 Slave ID Data: Illegal Function (Error) Device Identification: Illegal Function (Error)	2021-12-08T23:37:29.144440	(Search Qu Number o 9600 96 query cre	iery: port:502 f results dits available.			 Downloads consume query credits which reset start of every month. The maximum numbe results that can be downlo for a search query is 300. 	at the er of oaded 000	
United States 9 Korea, Republic of 3 Germany 3	1,962 1,922 1,093		Unit ID: 255 Slave ID Data: Illegal Data Address (Error) Device Identif		I		Dov	VNLOAD		 Query credits are only deducted for data that wa actually downloaded. 	y IS	
France 3	,066											
Italy 2 More	,627	220.125.118.9 Korea Telecom Korea, Republic of, Cheongju-si	5 Unit ID: 0 Slave ID Data: Illegal Function (Error) Device Identification: Illegal Function (Error)	2021-12-08T23:37:05.632998		Note:	Downloads ma	y take several h	ours to complete	using the official Shodan command-line interface ((cli):	
Korea Telecom 2	,607	ics	Unit ID: 1 Slave ID Data: Illegal Function (Error) Device Identification: Illegal Function (Error)							LEARN MORE		



Shodan <no-reply@shodan.io> 寄給</no-reply@shodan.io>	上午11:05 (38 分鐘前)
🗙 英文 ▾ 🔰 中文 (繁體) ▼ 副講影件	
Download Finished	
Your recent download request for the search query "port:502" has finished	
Please download it from the following location:	
Download	
Be sure to check out these link if you need any help.	
All your recent downloads: https://beta.shodan.io/download How to work with Shodan data files: https://help.shodan.io/mastery/working-with-shodan-data- How to convert to Excel: https://help.shodan.io/mastery/working-with-shodan-data- How to convert to Excel: https://help.shodan.io/mastery/working-with-shodan-data- How to convert to Excel: https://help.shodan.io/mastery/working-with-shodan-data-	files

下載作業進度完成後,官方會寄信通知

如何重新下載資料?



下載方法二:使用命令列下載

Shodan官方(創辦人)有提供python套件,讓使用者在命令列上操作Shodan 服務,或自行寫python程式碼import Shodan套件
下載網址: https://github.com/achillean/shodan-python

●後續安裝教學會以Ubuntu做示範

	About –		ı 🤇
Device Name	nasoc-ubuntu-server 〉	>	
Memory	3.8 Gil	в	
Processor	Intel® Core™ i5-4570 CPU @ 3.20GHz × 2	2	
Graphics	llvmpipe (LLVM 12.0.0, 256 bits	5)	
Disk Capacity	42.9 GI	В	

Ubuntu 20.04.3 LTS
64-bit
3.36.8
X11
VMware
>

安裝Shodan套件

- 可以依照Github上的說明指示安裝
- Ubuntu有整合Shodan安裝套件,可以直接安裝套件

Installation	□
To install the Shodan library, simply:	<pre>nasoc@nasoc-ubuntu-server:~\$ shodan</pre>
\$ pip install shodan	Command 'shodan' not found, but can be installed with:
Or if you don't have pip installed (which you should seriously install):	sudo apt install python3-shodan
<pre>\$ easy_install shodan</pre>	nasoc@nasoc-ubuntu-server:~\$

查詢個人帳號的APIKey

●雨種方式取得API Key

1. 點選Account,進入後會寫在API Key

2. 在Developer頁面的右上角,點擊Show API Key



初始化Shodan服務

- 請保管好個人帳號的API Key,否則可能會被外人偷用帳號內的點數
 使用Shodan服務前,要先經過初始化設定
 - shodan init <api-key>

Æ	nasoc@nasoc-ubuntu-server: ~	Q	≡	-		8
<pre>nasoc@nasoc-ubuntu-server:~\$ Usage: shodan init [OPTIONS] Try "shodan init -h" for hel</pre>	shodan init <api key=""> p.</api>					
Error: Missing argument " <ap< td=""><th>vi key>". </th><td></td><td></td><td></td><td>7</td><td>I</td></ap<>	vi key>". 				7	I
Successfully initialized	shodan chee j					
nasoc@nasoc-ubuntu-server:~\$						

查詢點數數量

▶ 下載資料前,要先知道個人帳號剩下多少下載點數 ▶ shodan info



Query credits renew at the start of the month and provide the following amount of data:

1 query credit lets you download 100 results

查詢目標數量

•下載資料前,要先知道目標有多少筆資料

➢ shodan count <搜尋條件>*



nasoc@nasoc-ubuntu-server:~\$ shodan count

nasoc@nasoc-ubuntu-server:~\$ shodan count

nasoc@nasoc-ubuntu-server:~\$



下載Shodan資料

- ●確認目標數量和下載點數後,就可以進行資料下載
 > shodan download [OPTIONS] <儲存檔案名稱> <搜尋條件>
- •使用命令列下載或網頁下載的檔案內容都相同

Ē	nasoc@nasoc-ubuntu-server: ~	Q		_		
		\sim				
nasoc@nasoc-ubunt Usage: shodan dow	x u-server:~\$ shodan download -h wnload [OPTIONS] <filename> <search quer<="" td=""><td>y></td><td></td><td></td><td></td><td></td></search></filename>	y>				
Download search	results and save them in a compressed	JSON f	ile.			
Options:						
limit INTEGER	The number of results you want to dow	nload.	-1 to	o dowr	nload	1
skin INTEGER	The number of results to skin when st	arting	the c	lown] (had	
-hhelp	Show this message and exit.	arceng	che c	Jownet		
		(and the second s				
	nasoc@nasoc-ubuntu-server: ~	Q	Ξ			×
nasoc@nasoc-ubunt	u-server:~S shodan downloadlimit -1	NTU FT	P DAT	A		
Search query:						
fotal number of r	esults: 575					
Query credits lef	t: 70					
Output file: [####################################	NTU_FTP_DATA.json.gz					
Notice: fewer res	ults were saved than requested					
Saved 554 results	into file NTU FTP DATA, ison.gz	J				
nasoc@nasoc-ubunt	u-server:~\$					

:	DOWNLOAD
554 records	DOWNLOAD
	e 554 records

下載資料的說明

下載資料時,Shodan會先把資料壓縮成「.gz」的壓縮檔格式
原始資料要經過解壓縮後才能取出

•Shodan資料儲存的資料型態為「.json」

NTU_FTP_I		OATA.json.gz Properties	×
Basic	Per	rmissions Open Wit	h
	Name:	NTU ETP DATA ison az	
	Name.	NTO_TTP_DATA.json.gz	
	Туре:	Gzip archive (application/gzip)	
	Size:	173.8 kB (173,808 bytes)	
	Parent folder:	/home/nasoc	
	Accessed:	Thu 09 Dec 2021 09:00:41 AM UT	2
	Modified:	Thu 09 Dec 2021 09:01:40 AM UT	2

Extract +	NTU_I	FTP_DATA.jso	n.gz	Q	Ξ	-		8
⟨ ⟩ Δ Location:	٥/							
Name	*	Size	Тур	e		М	odifie	d
NTU_FTP_DATA.json		1.0 MB	JSO	N docum	ent	09	Dece	mb

簡易的Shodan資料分析

前言

- ●前一章節講解資料的下載,緊接著要進入到資料分析部分
- ●資料分析的工具可以自行開發或使用商業軟體
- ●本章節將使用Shodan套件、Excel做說明

資料分析步驟



引用的資料來源: https://www.largitdata.com/blog_detail/20190725 https://blog.tibame.com/?p=17894

Shodan資料收集說明

Introduction

Data Collection

Frequency

The Shodan crawlers work 24/7 and update the database in real-time. At any moment you query the Shodan website you're getting the latest picture of the Internet.

Distributed

Crawlers are present in countries around the world, including:

- · USA (East and West Coast)
- China
- Iceland
- France
- Taiwan
- Vietnam
- Romania
- Czech Republic

Data is collected from around the world to prevent geographic bias. For example, many system administrators in the USA block entire Chinese IP ranges. Distributing Shodan crawlers around the world ensures that any sort of country-wide blocking won't affect data gathering.

▶ 限制

3

 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
 每次更新時,上次的資料不一

定馬上刪除

爬蟲(crawlers)基本演算法

Randomized

The basic algorithm for the crawlers is:

- 1. Generate a random IPv4 address
- 2. Generate a random port to test from the list of ports that Shodan understands
- 3. Check the random IPv4 address on the random port and grab a banner
- 4. Goto 1

This means that the crawlers don't scan incremental network ranges. The crawling is performed completely random to ensure a uniform coverage of the Internet and prevent bias in the data at any given time.

Shodan資訊元素—Banner & Metedata

Banner

The basic unit of data that Shodan gathers is the **banner**. The banner is textual information that describes a service on a device. For web servers this would be the headers that are returned or for Telnet it would be the login screen.

The content of the banner varies greatly depending on the type of service. For example, here is a typical HTTP banner:

HTTP/1.1 200 OK Server: nginx/1.1.19 Date: Sat, 03 Oct 2015 06:09:24 GMT Content-Type: text/html; charset=utf-8 Content-Length: 6466 Connection: keep-alive

Device Metadata

In addition to the banner, Shodan also grabs meta-data about the device such as its geographic location, hostname, operating system and more (see Appendix A). Most of the meta-data is searchable via the main Shodan website, however a few fields are only available to users of the developer API.

Appendix A: Banner Specification

For the latest list of fields that the banner contains please visit the online documentation³². A banner may contain the following properties/ fields:

General Properties

Name	Description	Example
asn	Autonomous system number	AS4837
data	Main banner for the service	HTTP/1.1 200
ip	IP address as an integer	493427495
ip_str	IP address as a string	199.30.15.20
ipv6	IPv6 address as a string	2001:4860:4860::8888
port	Port number for the service	80
timestamp	Date and time the information was	2014-01-15T05:49:56.283713
hash	collected Numeric hash of the <i>data</i> property	
hostnames	List of hostnames for the IP	["shodan.io", "www.shodan.io
domains	List of domains for the IP	["shodan.io"]
link	Network link type	Ethernet or modem
location	Geographic location of the device	see below
opts	Supplemental/ experimental data	
org	not contained in main banner Organization that is assigned the IP	Google Inc.
isp	ISP that is responsible for the IP	Verizon Wireless
-	space	
os	Operating system	Linux
uptime	Uptime of the IP in minutes	50
tags	List of tags that describe the purpose of the device	["ics", "vpn"]
	(Enterprise-only)	
transport	Type of transport protocol used to	tcp



JSON (JavaScript Object Notation, /<u>dgersen</u>/)是由道格拉斯·克羅克福特構想和設計的一種輕量級資料交換格式。其內容由屬 性和值所組成,因此也有易於閱讀和處理的優勢。JSON是獨立於程式語言的資料格式,其不僅是JavaScript的子集,也採用了C 語言家族的習慣用法,目前也有許多程式語言都能夠將其解析和字串化,其廣泛使用的程度也使其成為通用的資料格式。 "timestamp":"2021-12-09T14:44:55.289866", "isp":"DaDa Broadband LTD.", "asn":"AS18419", "port":80, "transport":"tcp", "domains":["da.net.tw"], "ip_str":"61.60.203.179"

簡介 [編輯]

JSON格式是1999年《JavaScript Programming Language, Standard ECMA-262 3rd Edition》的子集合,所以可以在JavaScript以eval()函式 (javascript通過eval()呼叫解析器) 讀入。不過這並不代表JSON無法使用於其他語言,事實上幾乎所有與網路開發相關的語言都有JSON函式庫。

JSON的基本資料類型:

- 數值:十進位數,不能有前導0,可以為負數,可以有小數部分。還可以用 e 或者 E 表示指數部分。不能包含非數,如NaN。不區分整數與浮點數。JavaScript用雙精度浮點數表示所有數值。
- 字串:以雙引號 "" 括起來的零個或多個Unicode碼位。支援反斜槓開始的跳脫字元序列。

• 布林值:表示為 true 或者 false 。

• 陣列: 有序的零個或者多個值。每個值可以為任意類型。序列表使用方括號 [,] 括起來。元素之間用逗號, 分割。形如: [value, value]

•物件:若干無序的「鍵-值對」(key-value pairs),其中鍵只能是字串^[1]。建議但不強制要求物件中的鍵是獨一無三的。物件以花括號 {開始,並以}結束。鍵-值對之間使 用逗號分隔。鍵與值之間用冒號:分割。

• 空值:值寫為 null

引用資料來源:<u>https://zh.wikipedia.org/zh-tw/JSON</u>

原始Shodan資料範例





🔚 20211210.json 🔀

{"hash": -1001764030, "timestamp": "2021-12-09T14:51:06.689291", "isp": "Data Cc^ {"ftp": {"features": {"LANG": {"parameters": ["bq-BG", "en-US", "es-ES", "fr-FR" {"ip": 2357762502, "port": 22, "transport": "tcp", "version": "8.0", "location": {"hash": 0, "http": {"robots hash": null, "redirects": [], "securitytxt": null, {"ip": 1990924217, "port": 22, "transport": "tcp", "version": "0.46", "location" {"hash": 693696860, "http": {"html hash": 919359363, "robots hash": null, "redir {"hash": 27629689, "tags": ["vpn"], "timestamp": "2021-12-09T14:47:39.899282", " {"hash": -1184745084, "tags": ["cloud"], "timestamp": "2021-12-09T14:47:39.35086 8 {"hash": 181568868, "timestamp": "2021-12-09T14:47:38.981635", "isp": "Data Comm 9 {"product": "Microsoft Exchange smtpd", "hash": 1216985983, "timestamp": "2021-1 {"hash": 0, "timestamp": "2021-12-09T14:47:38.378009", "isp": "Data Communicatic 11 {"hash": -940471364, "timestamp": "2021-12-09T14:47:37.475573", "isp": "Data Com 12 13 {"hash": 448214121, "timestamp": "2021-12-09T14:47:37.400660", "isp": "Data Comm 14 {"hash": -550438196, "timestamp": "2021-12-09T14:47:37.216158", "isp": "Data Com {"hash": 1048646653, "timestamp": "2021-12-09T14:47:36.973094", "org": "Chunghwa 15 16 {"hash": -1437137619, "product": "Chromecast", "http": {"robots hash": null, "re 17 {"hash": 954428700, "http": {"robots hash": null, "redirects": [], "securitytxt" 18 {"hash": 2100702304, "timestamp": "2021-12-09T14:47:35.024964", "isp": "Data Com 19 {"hash": 1188488153, "http": {"robots hash": null, "redirects": [], "securitytxt 20 {"hash": 1271903746, "http": {"robots hash": null, "redirects": [], "securitytxt {"ip": 3399072700, "port": 22, "transport": "tcp", "version": "7.4", "location": 21 {"hash": 744790496, "http": {"robots hash": null, "redirects": [], "securitytxt" ["hash". 0 "timetamo". "2021_12_00#14.47.33 701327" "isn". "Taiwan Infrastruc" 23 < JSON file length : 6,290,227 lines : 1,001 Ln:7 Col:101 Pos:15,175 Unix (LF) UTF-8 INS



Json Parser Online You like it? Support it! Donate

{"hash": 1364076727, "timestamp": "2021-12-09T14:46:45.173433", "isp": "Data Communication Business Group", "transport": "top", "data": "\u0000", "asn": "AS3462", "port": 515, "hostnames": ["218-166-234-160.dynamic-ip.hinet.net"], "location": {"city": "Fengshan", "region_code": "KHH", "area_code": null, "longitude": 120.36126, "latitude": 22.62659, "postal_code": null, "country_code": "TW", "country_name": "Taiwan"}, "ip": 3668372128, "domains": ["hinet.net"], "org": "Chunghwa Telecom Co.,Ltd.", "os": null, "_shodan": {"crawler": "bf213bc419cc3491376c12af3le32623c1b6f467", "module": "line-printer-daemon", "pt": true}, "opts": {}, "ip_str": "218.166.234.160"}

	Try out Beta! Samples ▼ Options ▼											
	• • • •											
String parse	JS eval											
"hash":1364076727,	"hash":1364076727,											
"timestamp":"2021-12-09T14:46:45.173433",	"timestamp":"2021-12-09T14:46:45.173433",											
"isp":"Data Communication Business Group",	"isp": "Data Communication Business Group",											
"transport":"tcp",	"transport": "tcp",											
"data":"\u0000",	"data":"",											
"asn":"AS3462",	"asn": "AS3462",											
"port":515,	"port":515,											
"hostnames":	"hostnames":											
"218-166-234-160.dvnamic-ip.hinet.net"	"218-166-234-160.dvnamic-ip.hinet.net"											
1.	1.											
"location":	"location":											
"city": "Fengshan",	"city": "Fengshan",											
"region code":"KHH",	"region code":"KHH".											
"area code":null,	"area code":null,											
"longitude":120.36126,	"longitude":120.36126,											
"latitude":22.62659,	"latitude":22.62659,											
"postal_code":null,	"postal code":null,											
"country code": "TW",	"country code":"TW",											
"country_name":"Taiwan"	"country_name":"Taiwan"											
},	},											
"ip":3668372128,	"ip":3668372128,											
"domains": 🗖 ["domains": 🗖 [
"hinet.net"	"hinet.net"											
1,	1,											
"org":"Chunghwa Telecom Co.,Ltd.",	"org":"Chunghwa Telecom Co.,Ltd.",											
"os":null,	"os":null,											
"_shodan": 🖂 {	"_shodan": 🗆 {											
"crawler":"bf213bc419cc8491376c12af31e32623c1b	"crawler":"bf213bc419cc8491376c12af31e32623c1b											
6f467",	6f467",											
"options": 🖂 {	"options": 🖂 {											
},	},											
"id":"c185df3a-bb6d-4490-ba58-5b20f5a042b4",	"id":"c185df3a-bb6d-4490-ba58-5b20f5a042b4",											
"module":"line-printer-daemon",	"module":"line-printer-daemon",											
"ptr":true	"ptr":true											
},	},											
"opts": 🗆 {	"opts": 🗆 {											
},	},											
"ip_str":"218.166.234.160"	"ip_str":"218.166.234.160"											

單一Shodan資料範例(續)



218.166.234.160
랾 Open Ports
515 516
>_ Raw Data Expand All Collapse All Copy to Clipboard
{
area_code : null,
asn : <u>"AS3462</u> ",
city : <u>"Fengshan"</u> ,
country_code : "Thi",
country_name : "Taiwan",
🗆 data : [
□0:{
🗆 _shodan : {
crawler : "bf213bc419cc8491376c12af31e32623c1b6f467",
id : "c185df3a-bb6d-4490-ba58-5b20f5a042b4",
<pre>module : "line-printer-daemon",</pre>
options : {},
ptr : true
Ъ
asn : <u>"A53462</u> ",
data : " ",
🗆 domains : [

資料分析說明

●進行分析前,需要做資料前處理

●資料前處理完成後,才開始從細節上對資料進行分析



資料來源: https://ithelp.ithome.com.tw/articles/10231293

簡化後的資料分析步驟



內建套件的資料格式轉換

- 原始資料有太多資訊,比較難以直接檢視資料
- 套件中有包含資料格式的轉換功能,讓使用者方便轉換格式資料 → shodan convert < 要轉檔的檔案> < 轉換後的格式>

轉換後的資料比較容易查閱內容

Л nasoc@nasoc-ubuntu-server: ~ **_** Desktop Documents Downloads Music Pictures Public iasoc@nasoc-ubuntu-server:~\$ shodan convert -h Usage: shodan convert [OPTIONS] <input file> <output format> x Convert the given input data file into a different format. The following Templates Videos 20211210. 20211210. 20211210. file formats are supported: xlsx CSV json.gz kml, csv, geo.json, images, xlsx nasoc@nasoc-ubuntu-server: ~ Q ΓŦ. Example: shodan convert data.json.gz kml nasoc@nasoc-ubuntu-server:~\$ shodan convert 20211210.json.gz xls> Successfully created new file: 20211210.xlsx Options: nasoc@nasoc-ubuntu-server:~\$ shodan convert 20211210.json.gz csv --fields TEXT List of properties to output. Successfully created new file: 20211210.csv Show this message and exit. -h. --help nasoc@nasoc-ubuntu-server:~\$ nasoc@nasoc-ubuntu-server:~S

轉換後的資料範例(csv)

L					-		**	-			·
data 🔽 hostnames 🔽	ip 🔽 ip_str 🔽	іруб 🔽 огд	🔽 isp	🔽 location	Iocation.cit	locatio 💌	location 💌 l	ocation 🔽 os	🔽 asn	💌 port 💌 tags	🔽 timestamp 💽
+OK Dovecot ready. +OK mail.fast.org.tw	998085218 59.125.146.98	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Fengshan	Taiwan	22.62659	120.36126	AS3462	110	2021/12/9 14:51
220 FTP Server ready. 530 59-124-162-194	998023874 59.124.162.194	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Taipei	Taiwan	25.04776	121.53185	AS3462	21	2021/12/9 14:49
SSH-2.0-OpenSSH_8.0 Key	2357762502 140.136.153.198	Ministry of E	ducation (Fu Jen Catholic Uni	iversity TW	Bangiao	Taiwan	25.01427	121.46719	AS38845	5 22	2021/12/9 14:47
120-114-141-20	2020773320 120.114.141.200	Ministry of E	ducation (National Cheng Ku	ng UniveTW	Tainan	Taiwan	22.99083	120.21333	AS18177	7 8010	2021/12/9 14:47
SSH-2.0-dropbear_0.46 Ke 118-171-23-185	1990924217 118.171.23.185	Chunghwa Te	lecom Co Data Communicatio	on Busin(TW	Tainan	Taiwan	22.99083	120.21333	AS3462	22	2021/12/9 14:47
HTTP/1.1 200 OK Date: T 114-39-177-218	1915204058 114.39.177.218	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Tainan	Taiwan	22.99083	120.21333	AS3462	80	2021/12/9 14:47
Firmware: 1 Hostname: Vig61-222-88-148.}	1037981844 61.222.88.148	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Taoyuan City	Taiwan	24.99368	121.29696	AS3462	1723 vpn	2021/12/9 14:47
HTTP/1.1 302 FOUND Cc 93.151.236.35.b	602707805 35.236.151.93	Google LLC	Google LLC	TW	Taipei	Taiwan	25.04776	121.53185	AS15169	9 8443 cloud	2021/12/9 14:47
\xff\xfd\x01\xff\xfd\x1f\xff 59-127-33-64.hi	998187328 59.127.33.64	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Taitung	Taiwan	22.75991	121.14457	AS3462	2323	2021/12/9 14:47
220 TWTPS201.tpvaoc.contpex.tpvaoc.com	3544769455 211.72.227.175	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Banqiao	Taiwan	25.01427	121.46719	AS3462	465	2021/12/9 14:47
114-34-63-212.1	1914847188 114.34.63.212	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Yilan	Taiwan	24.757	121.753	AS3462	9530	2021/12/9 14:47
RTSP/1.0 200 OK CSeq: 1218-161-112-11	3668013166 218.161.112.110	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Tainan	Taiwan	22.99083	120.21333	AS3462	554	2021/12/9 14:47
RTSP/1.0 200 OK Server: 125-227-71-77.)	2112046925 125.227.71.77	Data Commur	ication B Data Communicatio	on Busin TW	Taichung	Taiwan	24.1469	120.6839	AS3462	554	2021/12/9 14:47
head\x03\x00\x00\x00\x00	3699681095 220.132.167.71	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Taichung	Taiwan	24.1469	120.6839	AS3462	6036	2021/12/9 14:47
NetBIOS Response: Serve: 114-40-120-226	1915255010 114.40.120.226	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Kaohsiung	Taiwan	22.61626	120.31333	AS3462	137	2021/12/9 14:47
HTTP/1.1 403 Forbidden (112-105-56-45.a	1885943853 112.105.56.45	New Century	InfoCom Taiwan Infrastructu	are Netw TW	Fengyuan	Taiwan	24.25	120.71694	AS18049	9 8008 iot	2021/12/9 14:47
HTTP/1.1 200 OK Content 1-161-69-208.dy	27346384 1.161.69.208	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Taipei	Taiwan	25.04776	121.53185	AS3462	80	2021/12/9 14:47
HTTP/1.1 400 Bad Request 210-65-240-7.hi	3527536647 210.65.240.7	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Taipei	Taiwan	25.04776	121.53185	AS3462	1723	2021/12/9 14:47
HTTP/1.1 200 OK Date: T211-22-230-144	3541493392 211.22.230.144	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Tainan	Taiwan	22.99083	120.21333	AS3462	82	2021/12/9 14:47
HTTP/1.1 302 Found Loca 124-108-171-12	2087496572 124.108.171.124	Taiwan Fixed	Network Taiwan Fixed Netw	vork, Tel TW	Taipei	Taiwan	25.04776	121.53185	AS9924	8008	2021/12/9 14:47
SSH-2.0-OpenSSH_7.4 Kej 188-187-153-20	3399072700 202.153.187.188	UnigateNet, I	nternet Se AboveNet Commun	nications TW	Taipei	Taiwan	25.04776	121.53185	AS17408	3 22	2021/12/9 14:47
HTTP/1.1 302 Found Loca	2020423316 120.109.54.148	Ministry of E	ducation (Taiwan Academic N	Network TW	Taichung	Taiwan	24.1469	120.6839	AS1659	8008	2021/12/9 14:47
123-205-57-165	2077047205 123.205.57.165	New Century	InfoCom) Taiwan Infrastructu	are Netw TW	Zhongxing Ne	w Taiwan	23.95908	120.68516	AS18049	8009	2021/12/9 14:47
HTTP/1.1 400 Bad Request visit.keznews.co	2823859236 168.80.172.36	Cooperative I	nvestmentQT Inc.	TW	Taipei	Taiwan	25.04776	121.53185	AS24567	7 8200	2021/12/9 14:47
HTTP/1.1 200 OK X-Powe	2356615211 140.119.24.43	Ministry of E	ducation (Taiwan Academic N	Network TW	Xindian	Taiwan	24.96005	121.53892	AS1659	3000	2021/12/9 14:47
HTTP/1.1 200 OK Content 220-132-123-14	3699669902 220.132.123.142	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Tainan	Taiwan	22.99083	120.21333	AS3462	80	2021/12/9 14:47
VPN (IKE) Initiator SPI: 7114-32-219-221	1914756061 114.32.219.221	Chunghwa Te	lecom Co Data Communicatio	on Busin TW	Taipei	Taiwan	25.04776	121.53185	AS3462	500 vpn	2021/12/9 14:47
CCU 20 0000 27 10110 160 125 7	1000756102 110 160 125 7	Chunchur To	laaam Co Data Cammuniaatia	Durin TIU	Tainai	Taiman	25.04776	101 52105	Y 437460	22	2021/12/0 17:42

轉換後的資料範例(xlsx)

IP	Port	- Timestamn	_ Data		- Hostnames	Organizatio	n ISP	Conntry	Conntry ISO Code	Cit v	05	ASN	 Тталерот	Product	Version	Web Server	Wohsita	Title
210 242		143 2021-12-09T	1 * OK ICAPAR	BILITY	210-242-91-7	h Chunghwa Te	elecc Data Comu	Taiwan	TW	Miaoli	00	AS3462	ten	IIVuut	¥ CI 3104		HCDJILC	TIME
220.141.	1	135 2021-12-09T	1 Microsoft RPC	C Endra	220-141-196-	17Chunghwa Te	elecc Data Comi	Taiwan	TW	Taovian (City	AS3462	tep	Microsoft RPC	Endpoint	Mapper		
125.227.3	2	465 2021-12-09T	1220 ESMTP N	MAILS	Simail.ietvox.co	mChunghwa Te	elecc Data Comi	Taiwan	TW	Taipei		AS3462	tep		- <u></u>	in appoi		
125.227.	5	80 2021-12-09T	1HTTP/1.1 401	l Unauti	h 125-227-67-19	9. Data Commu	nica1Data Com1	Taiwan	TW	Taichung		AS3462	tcp	mini httpd	1.19 19dec	mini httpd/1.19	401 Unaut	thorized
1.171.11	58	800 2021-12-09T	14:47:25.34168	1	1-171-116-85	d Chunghwa Te	elecc Data Comi	Taiwan	TW	Taipei		AS3462	top			, , , , , , , , , , , , , , , , ,		
125.228.	9	554 2021-12-09T	1RTSP/1.0 401	Unauth	h 125-228-91-80). Chunghwa Te	elecc Data Comi	Taiwan	TW	Taipei		AS3462	tcp					
1.170.54		443 2021-12-09T	14:47:25.07574	4	1-170-54-144	d Chunghwa Te	elecc Data Comi	Taiwan	TW	Fengyuan		AS3462	tcp					
114.33.1	0	80 2021-12-09T	1HTTP/1.1 200	O OK D	. 114-33-100-10	59 Chunghwa Te	elecc Data Comi	Taiwan	TW	Douliu		AS3462	tcp	Boa Web Serv	\$1	Boa/0.94.14rc2		
116.241.3	2	80 2021-12-09T	1 HTTP/1.1 200	O OK D	116-241-217-4	49 TBC	TBC	Taiwan	TW	Taoyuan (City	AS131596	tcp	Boa Web Serv	\$1	Boa/0.94.14rc2	1	
114.32.3	9	554 2021-12-09T	1 RTSP/1.0 200	OK C	\$114-32-39-24). Chunghwa Te	elecc Data Comi	Taiwan	TW	Taipei		AS3462	tcp					
1.162.57	. 2	2000 2021-12-09T	1 \x01\x00\x00\	x00	1-162-57-146.	.d Chunghwa Te	elecc Data Comi	Taiwan	TW	Taipei		AS3462	tcp	MikroTik ban	dwidth-test	server		
34.81.71		22 2021-12-09T	1 SSH-2.0-Oper	nSSH_7	7.220.71.81.34.	beGoogle LLC	Google LL	. Taiwan	TW	Taipei		AS396982	tcp	OpenSSH	7.4			
59.127.1	0	80 2021-12-09T	1 HTTP/1.1 200	OOK S	€ 59-127-102-8.	h Chunghwa Te	eleccData Comi	Taiwan	TW	Hualien C	ity	AS3462	tcp	Cross Web Sei	ver	Cross Web Serv	DVR Com	ponents
111.241.3	2	81 2021-12-09T	14:47:23.66671	2	111-241-218-	12Chunghwa Te	eleccData Comi	Taiwan	TW	Taipei		AS3462	tcp					
120.107.	1 8	008 2021-12-09T	1 HTTP/1.1 302	2 Found	Location: http	s Ministry of E	duc: Taiwan Ac	Taiwan	TW	Chang-hua	a	AS1659	tcp					
168.80.1	7 3	3001 2021-12-09T	1 HTTP/1.1 400) Bad R	e visit.keznews.	ccCooperative I	nvesQT Inc.	Taiwan	TW	Taipei		AS24567	top					
220.135.	1	123 2021-12-09T	1 NTP protocoly	version:	: 220-135-19-14	4(Chunghwa Te	elecc Data Comi	Taiwan	TW	Taitung		AS3462	udp					
210.71.1	9 2	2323 2021-12-09T	1 HTTP/1.0 404	4 FAIL	210-71-196-19	98Data Commu	nicatData Comi	Taiwan	TW	Taipei		AS3462	top					
103.10.2	0	80 2021-12-09T	1 HTTP/1.1 200	OOK S	erver: 01_1632	00141 Yang Gu	an Ji 141 Yang (Taiwan	TW	Tainan		AS45599	top			01_1632062562	;	
183.182.	7 9	998 2021-12-09T	14:47:22.21553	9		Asia Pacific N	Vetw 60 Market	Taiwan	TW	Taichung		AS55303	tcp					
61.223.1	3	445 2021-12-09T	1 SMB Status:	Authen	n 61-223-187-2/	45Chunghwa Te	elecc Data Comi	Taiwan	TW	Chang-hua	a Windows	1AS3462	tcp					
49.158.2	1	123 2021-12-09T	1 NTP protocoly	version:	: 49-158-216-72	2. TFN MEDIA	. CO UNION BI	Taiwan	TW	Hualien C	ity	AS24164	udp					
140.126.	1 8	3008 2021-12-09T	1 HTTP/1.1 302	2 Found	Class5-27.cc-p	oc Ministry of E	duc National C	Taiwan	TW	Miaoli		AS9916	tcp					
36.230.2	5	81 2021-12-09T	14:47:21.82906	1	36-230-26-82	d Chunghwa Te	eleccData Comi	Taiwan	TW	Taoyuan (City	AS3462	tcp					
114.33.1	3	80 2021-12-09T	1HTTP/1.1 200	O OK C	114-33-189-2	4(Chunghwa Te	eleccData Comi	Taiwan	TW	Tainan		AS3462	tcp					
114.42.2	0	80 2021-12-09T	1HTTP/1.1 301	1 Move	d 114-42-209-12	26Chunghwa Te	eleccData Comi	Taiwan	TW	Chang-hua	a	AS3462	tcp	lighttpd	1.4.45	lighttpd/1.4.45		
114.33.2	£	80 2021- <u>12-09T</u>	14:47:21.37870	2	114-33-2-88.h	ii Chunghwa Te	elecc Data Comi	Taiwan	TW	Taichung		AS3462	tcp					













•	11			0		-	1	0	11	1		17	-	141	11	V	
IP		Port	💌 Ti 🛙	nest 🔻	Data	Hostna	Organi -	ISP	- Countr -	Countr -	City 💌	OS 🤄	ASN 🗖	Transp 🔻	Produc -	Versio 💌 Web	S Websit fitle
2		50	00 202	1-12-0	HTTP/1.	1 220-135-	2 Chunghwa	Data C	omr Taiwan	TW	Fengshan	Synology	IAS3462	tcp	nginx	6.2.3-2542 nginx	DS918 - Synology DiskStation
1		50	00 202	1-12-0	HTTP/1.	1 114-35-2	4' Chunghwa	Data C	omr Taiwan	TW	Banqiao	Synology	IAS3462	tcp	nginx	6.2.2-2492 nginx	Family-NAS - Synology DiskStation
. 1:		50	00 202	1-12-0	HTTP/1.	1 180-177-	l(kbro CO.	I kbro C	O. I Taiwan	TW	Hsinchu	Synology	IAS38841	tcp	nginx	7.0.1-4221 nginx	SkyDisk - Synology DiskStation
2		50	00 202	1-12-0	HTTP/1.	1 pc169-16	5 Taiwan A	c Taiwan	Ac Taiwan	TW	Taitung	Synology	IAS1659	tcp	nginx	6.2.4-2555 nginx	NTTU - Synology DiskStation
б		50	01 202	1-12-0	HTTP/1.	1 33-238.6	3. Savecom 1	l:SaveCo	m l Taiwan	TW	Taichung	Synology	IAS9676	tcp		6.2.2-2492 nginx	OFFICE - Synology DiskStation
1:		50	01 202	1-12-0	HTTP/1.	1 122-116-	5(Chunghwa	Data C	omr Taiwan	TW	Taipei	Synology	IAS3462	tcp		6.2.3-2542 nginx	EDG2550 - Synology DiskStation
. 2		50	00 202	1-12-0	HTTP/1.	1 210-244-	1.New Cent	u Digital	Un Taiwan	TW	Tainan	Synology	IAS4780	tcp	nginx	6.2.4-2555 nginx	MKX5 - Synology NAS
1		50	00 202	1-12-0	HTTP/1.	1 111-246-	3.Chunghwa	Data C	omr Taiwan	TW	Yuanlin	Synology	IAS3462	tcp	nginx	6.2.4-2555 nginx	stfrancis - Synology NAS

NoSQL資料庫簡介

什麼是 NoSQL 資料庫?

NoSQL 資料庫也稱為「非關聯式」、「NoSQL DB」或「非 SQL」,以強調它們能夠以不同於關聯式 (SQL) 資料庫 (利用 資料列和資料表)的方式,來處理大量快速變化的非結構化資料。

NoSQL 技術大約從 1960 年代開始就已存在,但由於資料環境變化,開發人員必須做出調整才能處理雲端、行動裝置: 社交媒體和巨量資料所產生數量龐大且種頻繁多的資料,因此突然大受歡迎。

從熱門名人推文到電子病歷中的救生資訊,迅速就能產生新的資料和資料類型。NoSQL資料庫已發展成可協助開發人員 快速建立資料庫系統,以儲存新的資訊,並讓該項資訊立即可供搜尋、彙總和分析。



彈性處理資料

NoSQL 可讓開發人員更自由、快速且彈性地變更結構描述 和查詢,以配合資料需求。儲存為彙總的資訊可更輕鬆快 速地反覆改善,而不需要事先設計結構描述。



資料來源: https://azure.microsoft.com/zh-tw/overview/nosql-database/

資料視覺化說明

資料視覺化是將複雜的資訊以視覺圖像呈現、簡化的過程

 把生硬的資料變成簡單易懂的圖片、動畫、以及其他有效的溝通媒介,將 艱涩理性的資訊變有趣、感性的內容



引用資料來源:https://relab.cc/blog/%E8%B3%87%E6%96%99%E8%A6%96%E8%A6%BA%E5%8C%96

結論

●Shodan是一個專門蒐集IoT設備資訊的搜尋引擎

●如何在資安事件發生前或大規模漏洞攻擊前,利用Shodan找出學術網路中 有漏洞的設備並進行通報,是目前北區ASOC團隊正在努力的方向

資料來源-1

- 1. CNN報導: https://money.cnn.com/2013/04/08/technology/security/shodan/
- 2. System Shock圖片來源: <u>https://en.wikipedia.org/wiki/System_Shock</u>
- 3. 巴哈電玩瘋報導: <u>https://www.youtube.com/watch?v=n1ChelLmQIc</u>
- 4. iT邦幫忙: <u>https://ithelp.ithome.com.tw/articles/10218769</u>
- 5. Bleepingcomputer報導: <u>https://www.bleepingcomputer.com/news/security/compromised-</u> docker-hosts-use-shodan-to-infect-more-victims/
- 6. PCMagazine報導: <u>https://in.pcmag.com/security/146125/att-reveals-malware-targeting-</u> <u>millions-of-routers-iot-devices</u>
- 7. 維基百科—JSON: <u>https://zh.wikipedia.org/zh-tw/JSON</u>
- 8. JSON線上解析器: <u>http://json.parser.online.fr/</u>

資料來源-2

- 1. Shodan官方網站: <u>https://cli.shodan.io/</u>
- 2. Github-Shodan 套件: <u>https://github.com/achillean/shodan-python</u>
- 3. 大數據分析步驟-1: <u>https://www.largitdata.com/blog_detail/20190725</u>
- 4. 大數據分析步驟-2: <u>https://blog.tibame.com/?p=17894</u>
- 5. 微軟—NoSQL 資料庫: <u>https://azure.microsoft.com/zh-tw/overview/nosql-database/</u>
- 6. 資料分析說明: <u>https://ithelp.ithome.com.tw/articles/10231293</u>
- 7. 資料視覺化是什麼?: https://relab.cc/blog/%E8%B3%87%E6%96%99%E8%A6%96%E8%A6%BA%E5%8C%96
- 8. John Matherly (2017), Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work for You, Leanpub.



謝謝大家