

盤點常用的資安工具

蔡一郎



Google Me.

現任

- ✓ 來毅數位科技股份有限公司 資安長
- ✓ 台灣數位安全聯盟 榮譽理事長
- ✓ 台灣網際空間與安全策略發展協會 理事長
- ✓ 台灣資訊暨資安服務聯盟 理事長
- ✓ 台灣數位鑑識發展協會 理事
- ✓ 中華民國資訊安全學會 監事
- ✓ 中華民國數位金融交易暨資料保護協會 理事
- ✓ 中華民國人壽保險商業同業公會 資安顧問/資安工作小組委員
- ✓ InfoSec Taiwan 國際資安組織大會 創辦人、大會主席
- ✓ OWASP 台灣分會長
- ✓ The HoneyNet Project 台灣分會長
- ✓ Cloud Security Alliance 台灣分會長
- ✓ CSCIS 亞太區副總裁
- ✓ 政府部會資安稽核委員
- ✓ 自由作家，資訊圖書著作 37 本，技術專欄文章 100+ 篇
- ✓ 部落格 <https://blog.yilang.org>
- ✓ 專業證照：
 - ✓ RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC、BS10012 LAC、ISO 17065、ISO 42001 LAC、CSA STAR Auditing、CCSK、CMMC Essential、CSM



蔡一郎 Steven Tsai

國立成功大學 電腦與通信工程研究所 博士候選人
國立成功大學 電機工程研究所 碩士

曾任

- ✓ 微智安聯股份有限公司 創辦人兼執行長
- ✓ 財團法人國家實驗研究院國家高速網路與計算中心 研究員
- ✓ 台灣數位安全聯盟 理事長
- ✓ 中華民國資料保護協會 監事
- ✓ 數位經濟暨產業發展協會 理事
- ✓ 中華民國南部科學園區產學協會 理事 監事
- ✓ 台灣資訊安全聯合發展協會 監事

課程大綱

- 資安工具盤點
- 網路與系統安全測試
- 案例分享

資安工具盤點



前言

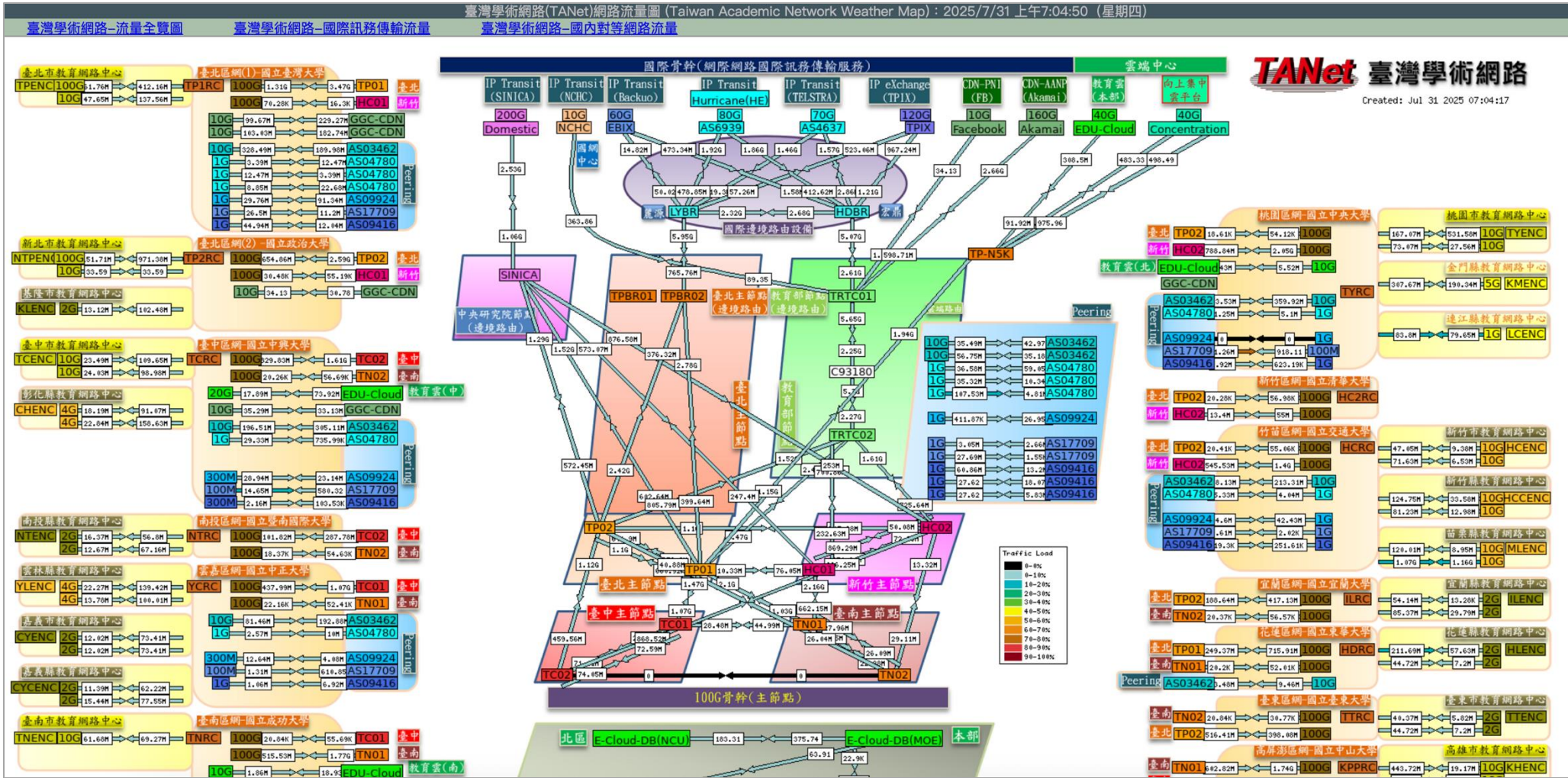
- 資安工具隨手可得，如何選擇好用的工具軟體，協助我們進行資安的檢測工作，是許多資訊與資安人員不可不知的技能
- 本場次將介紹網路分析、系統安全以及應用服務安全測試上常用的工具軟體，透過案例的分享掌握工具的使用技巧
- 找出自己工作上需要的資安工作，將可以事半功倍

資安相關的工具軟體多嗎？



Cyber Security Tools

TANet Traffic



TANet Whois



The image shows the TANet Whois Database interface. At the top left is the logo of the Ministry of Education, Taiwan, with the text "教育部" and "資訊及科技教育司". The main title "TANet Whois Database" is prominently displayed in the center. Below the title, there is a search section labeled "IP Whois 查詢:". It includes a text input field, a "送出" (Submit) button, and a "重設" (Reset) button. At the bottom left, there is a link labeled "聯絡我們" (Contact Us). The background features a network diagram with nodes and lines, and the word "Internet" is visible in the upper left area of the interface.

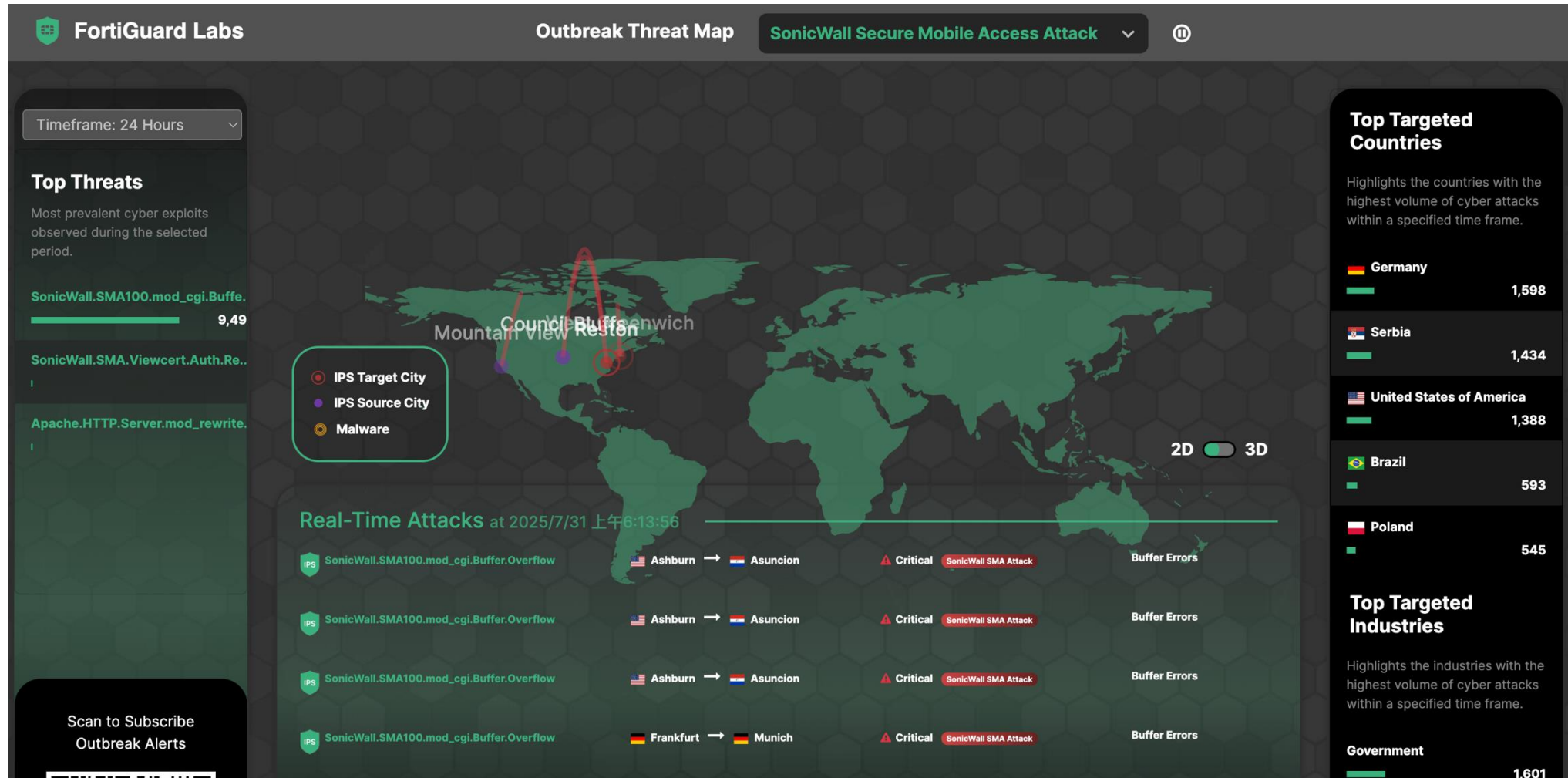
MINISTRY OF EDUCATION
教育部 資訊及科技教育司

Internet

TANet Whois Database Internet IP Whois 查詢 : 送出 重設 [聯絡我們](#)

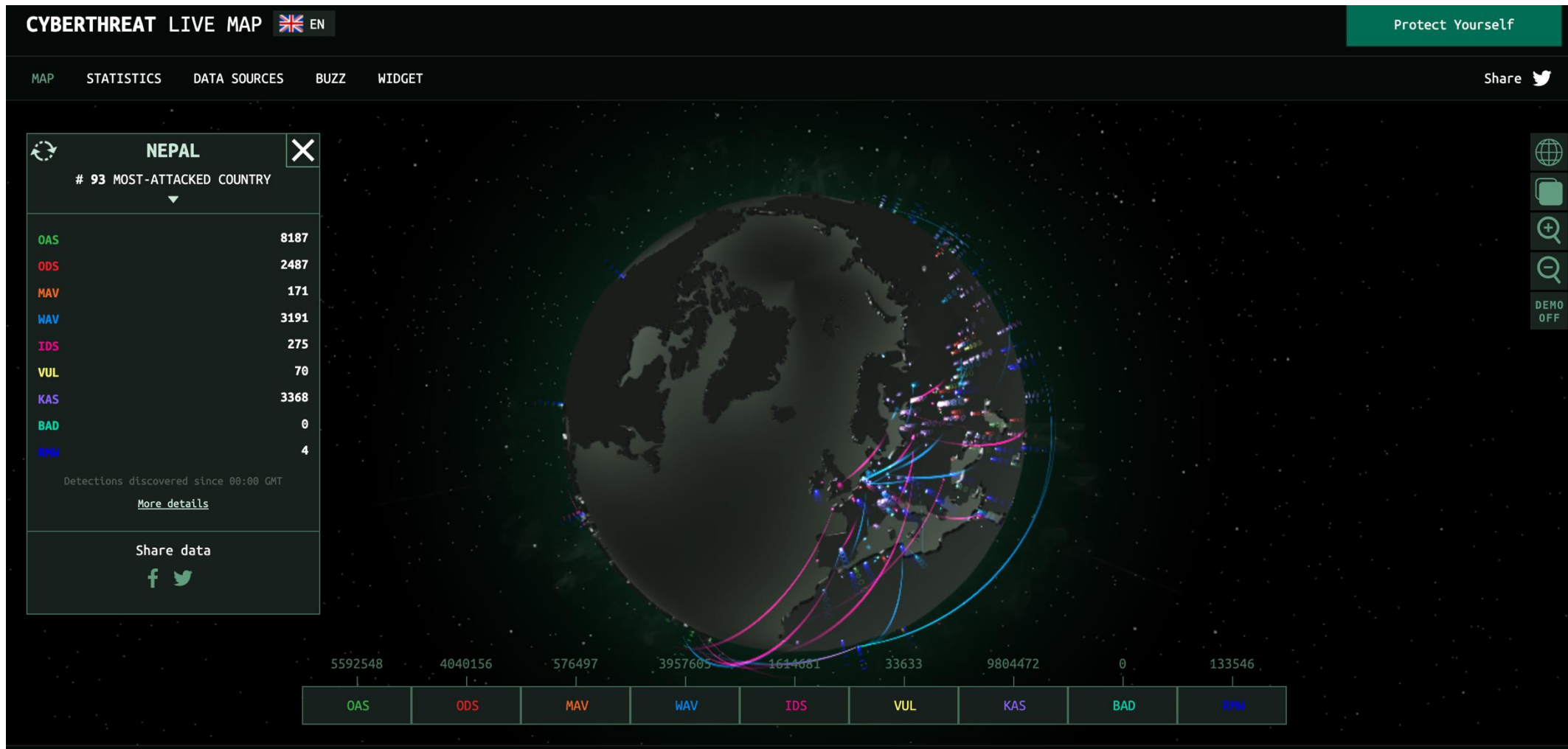
<https://whois.tanet.edu.tw/>

FortiGuard Labs



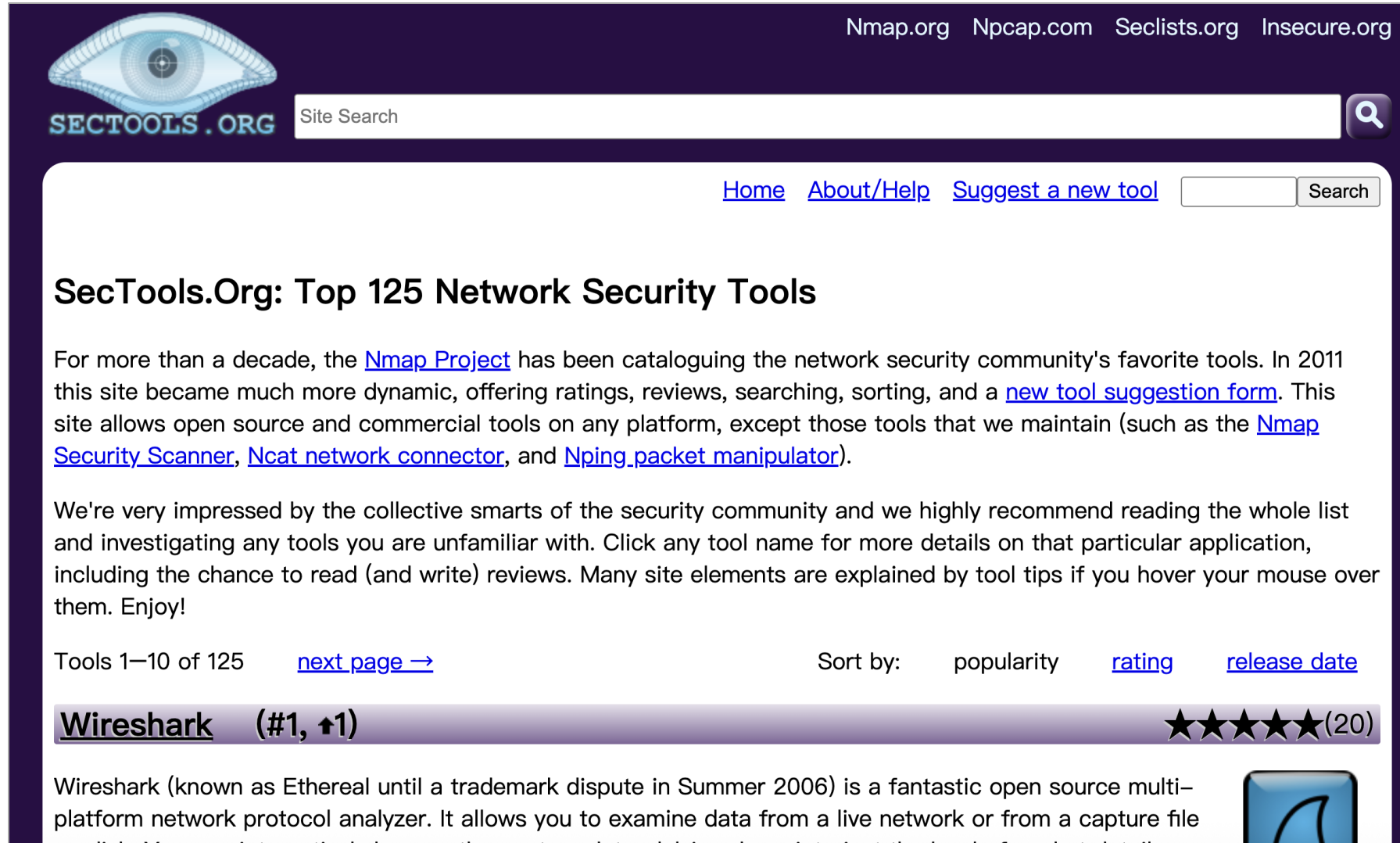
<https://fortiguard.fortinet.com/threat-map>

Cyberthreat Live Map



<https://cybermap.kaspersky.com/>

從 sectools.org 談起



The screenshot shows the Sectools.org website interface. At the top, there's a navigation bar with links to Nmap.org, Npcap.com, Seclists.org, and Insecure.org. Below this is a search bar with the text "Site Search" and a magnifying glass icon. The main content area features a header with links to Home, About/Help, and Suggest a new tool, followed by a search box. The main heading is "SecTools.Org: Top 125 Network Security Tools". The text below explains that the site has been cataloging network security tools for over a decade, offering ratings, reviews, and a new tool suggestion form. It lists several tools: Nmap Project, Nmap Security Scanner, Ncat network connector, and Nping packet manipulator. A paragraph expresses appreciation for the security community and encourages users to explore the tools. Below this, there's a section for "Tools 1—10 of 125" with a "next page →" link. The sorting options are "popularity", "rating", and "release date". The first tool listed is "Wireshark" with a rating of 5 stars (20 reviews) and a position of (#1, ↑1). A brief description of Wireshark is provided, stating it's a multi-platform network protocol analyzer. A small icon of the Wireshark logo is visible on the right.

Nmap.org Npcap.com Seclists.org Insecure.org

SECTOOLS.ORG Site Search

[Home](#) [About/Help](#) [Suggest a new tool](#) Search

SecTools.Org: Top 125 Network Security Tools

For more than a decade, the [Nmap Project](#) has been cataloguing the network security community's favorite tools. In 2011 this site became much more dynamic, offering ratings, reviews, searching, sorting, and a [new tool suggestion form](#). This site allows open source and commercial tools on any platform, except those tools that we maintain (such as the [Nmap Security Scanner](#), [Ncat network connector](#), and [Nping packet manipulator](#)).

We're very impressed by the collective smarts of the security community and we highly recommend reading the whole list and investigating any tools you are unfamiliar with. Click any tool name for more details on that particular application, including the chance to read (and write) reviews. Many site elements are explained by tool tips if you hover your mouse over them. Enjoy!

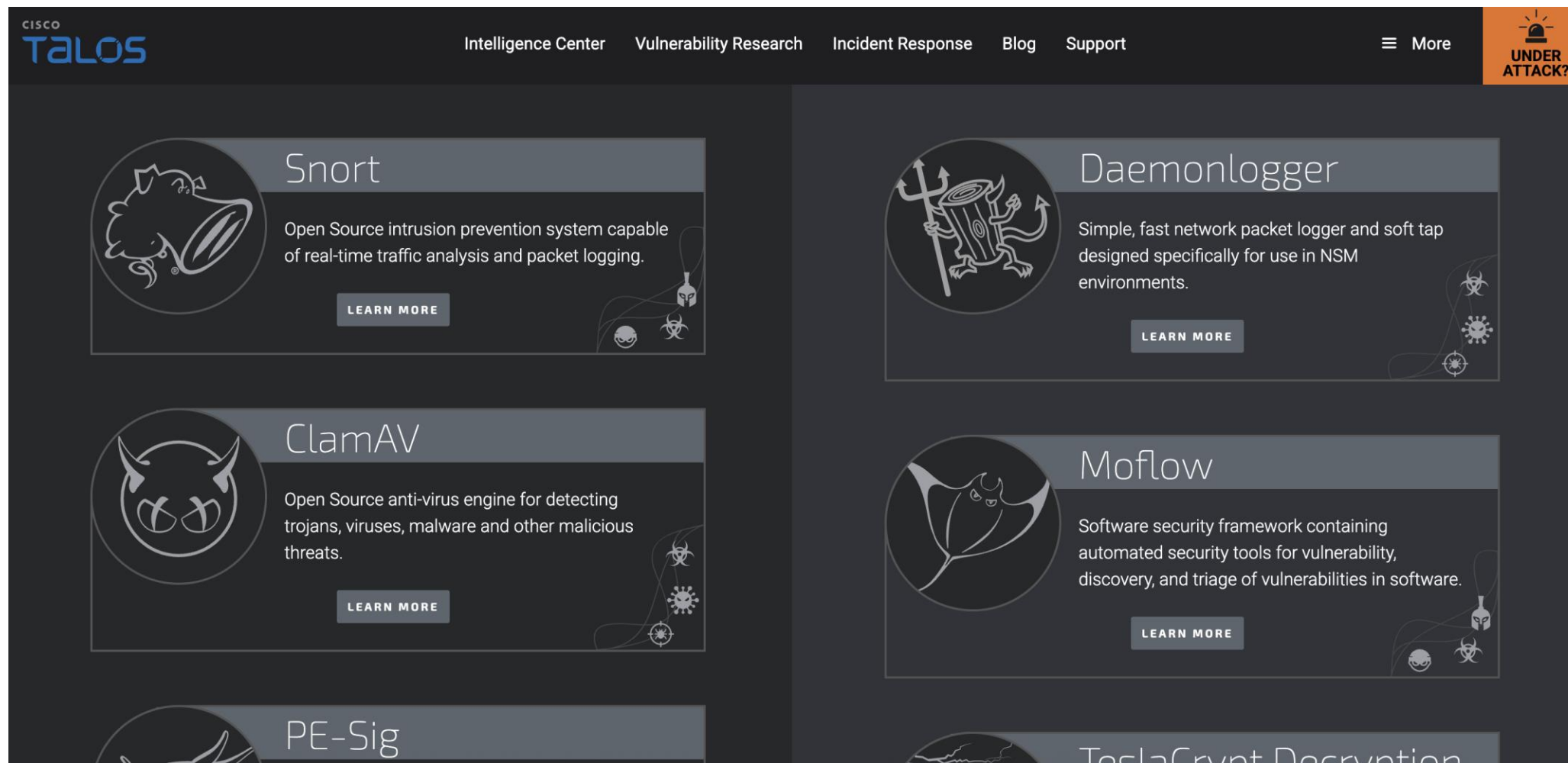
Tools 1—10 of 125 [next page →](#) Sort by: popularity [rating](#) [release date](#)

Wireshark (#1, ↑1) ★★★★★(20)

Wireshark (known as Ethereal until a trademark dispute in Summer 2006) is a fantastic open source multi-platform network protocol analyzer. It allows you to examine data from a live network or from a capture file

<https://sectools.org/>

OpenSource Tools



The screenshot shows the Cisco Talos website's 'Open Source Tools' section. The header includes the Cisco Talos logo and navigation links: Intelligence Center, Vulnerability Research, Incident Response, Blog, and Support. A 'More' menu icon is also present. A red banner in the top right corner reads 'UNDER ATTACK?'. The main content area features four tool cards, each with a circular icon, the tool name, a brief description, and a 'LEARN MORE' button. The tools listed are Snort, Daemonlogger, ClamAV, and Moflow. A fifth tool, PE-Sig, is partially visible at the bottom left, and TeslaCrypt Decryption is partially visible at the bottom right.

CISCO TALOS

Intelligence Center Vulnerability Research Incident Response Blog Support

UNDER ATTACK?

Snort
Open Source intrusion prevention system capable of real-time traffic analysis and packet logging.
[LEARN MORE](#)

Daemonlogger
Simple, fast network packet logger and soft tap designed specifically for use in NSM environments.
[LEARN MORE](#)

ClamAV
Open Source anti-virus engine for detecting trojans, viruses, malware and other malicious threats.
[LEARN MORE](#)

Moflow
Software security framework containing automated security tools for vulnerability, discovery, and triage of vulnerabilities in software.
[LEARN MORE](#)

PE-Sig

TeslaCrypt Decryption

<https://talosintelligence.com/software>

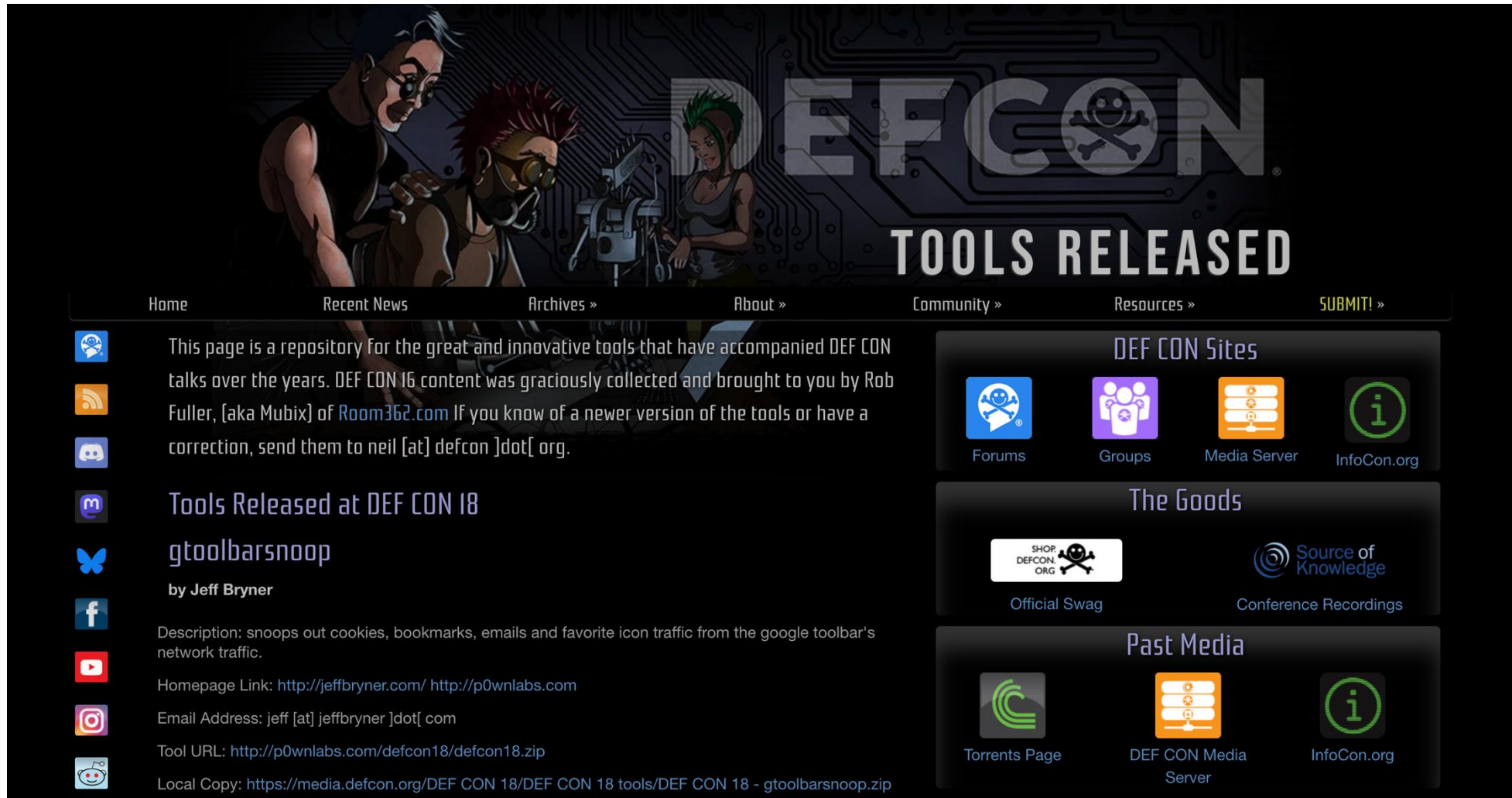
Kali Linux



<https://www.kali.org/>





DEFCON Tools





The image is a screenshot of the DEFCON Tools Released page. At the top, there is a banner with an illustration of three characters (two men and one woman) in a cyberpunk style, with the text 'DEFCON TOOLS RELEASED' in large, bold, white letters. Below the banner is a navigation bar with links: Home, Recent News, Archives », About », Community », Resources », and SUBMIT! ». The main content area is divided into two columns. The left column features a list of social media icons (Twitter, RSS, Discord, Medium, Facebook, YouTube, Instagram, and GitHub) and a section titled 'Tools Released at DEF CON 18' with the tool 'gtoolbarsnoop' by Jeff Bryner. The right column has sections for 'DEF CON Sites' (Forums, Groups, Media Server, InfoCon.org), 'The Goods' (Official Swag, Conference Recordings), and 'Past Media' (Torrents Page, DEF CON Media Server, InfoCon.org).


Home Recent News Archives » About » Community » Resources » SUBMIT! »


 This page is a repository for the great and innovative tools that have accompanied DEF CON talks over the years. DEF CON 16 content was graciously collected and brought to you by Rob Fuller, [aka Mubix] of Room362.com. If you know of a newer version of the tools or have a correction, send them to [neil \[at\] defcon \[dot\] org](mailto:neil@defcon.org).







 Tools Released at DEF CON 18

 **gtoolbarsnoop**

 by Jeff Bryner

 Description: snoops out cookies, bookmarks, emails and favorite icon traffic from the google toolbar's network traffic.





 Homepage Link: <http://jeffbryner.com/> <http://p0wnlabs.com>

Email Address: [jeff \[at\] jeffbryner \[dot\] com](mailto:jeff@jeffbryner.org)



Tool URL: <http://p0wnlabs.com/defcon18/defcon18.zip>

Local Copy: [https://media.defcon.org/DEF CON 18/DEF CON 18 tools/DEF CON 18 - gtoolbarsnoop.zip](https://media.defcon.org/DEF%20CON%2018/DEF%20CON%2018%20tools/DEF%20CON%2018%20-%20gtoolbarsnoop.zip)




DEF CON Sites

 Forums  Groups  Media Server  InfoCon.org

The Goods

 Official Swag  Source of Knowledge

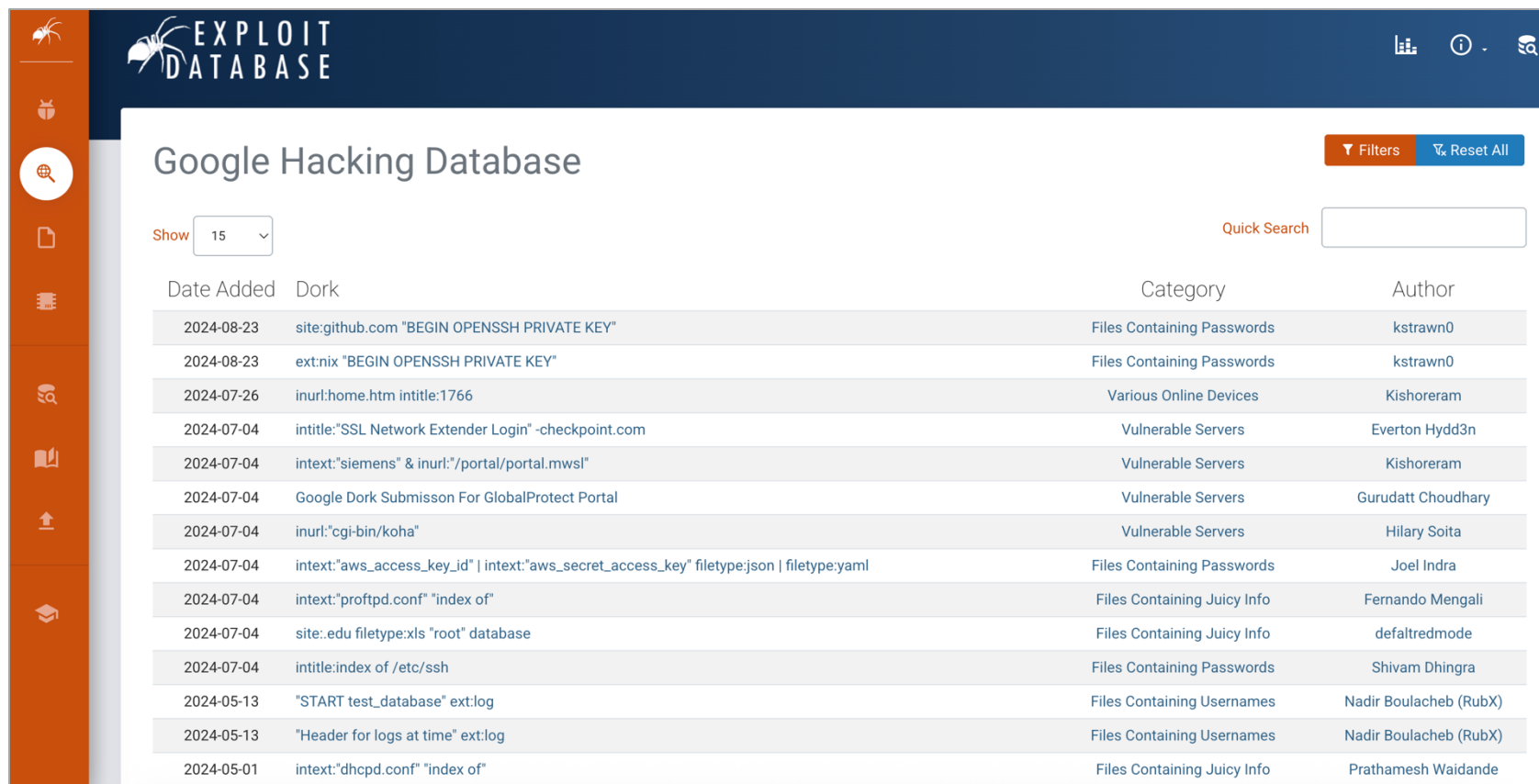
Past Media

 Torrents Page  DEF CON Media Server  InfoCon.org

<https://defcon.org/html/links/dc-tools.html>

Google Hacking

- Google 是資訊人員的好幫手，而Google Hacking 亦是如此，只是我們利用了一些特殊的語法及關鍵字，找到一些遺留在網路上的資料



Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl: "/portal/portal.mwsl"	Vulnerable Servers	Kishoreram
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id" intext:"aws_secret_access_key" filetype:json filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	Files Containing Juicy Info	defaultredmode
2024-07-04	intitle:index of /etc/ssh	Files Containing Passwords	Shivam Dhingra
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-13	"Header for logs at time" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-01	intext:"dhcpd.conf" "index of"	Files Containing Juicy Info	Prathamesh Waidande

<https://www.exploit-db.com/google-hacking-database>

Google Hacking

- 資料量夠大
- 回應速度快
- 最佳化輸出結果
- 頁庫存檔
- 豐富的運算元



Google Search

- 常見Agent
 - Googlebot, Yahoo!Slurp, bingbot
 - AhrefsBot, Baiduspider, Ezooms, MJ12bot, YandexBot
- Robots.txt
 - User-agent : 可以指定哪一種User-agent
 - Allow/Disallow : 設定檔案或是資料夾，允許不允許被爬取
 - Crawl-delay : 設定抓取的延遲時間
 - Sitemap : 用來告知搜尋爬蟲網站結構
- 詞彙/關鍵字(term)

```
User-agent: *  
Disallow: /cgi-bin/  
Disallow: /images/  
Disallow: /tmp/  
Disallow: /private/
```

Google Hacking相關語法

語法	用途
intitle/allintitle	搜尋網頁標題的內容
intext/allintext	搜尋網頁的本文
inurl/allinurl	搜尋網頁的URL內容
filetype	搜尋特定類型的檔案
link	搜尋網站中的鏈結
site	限制搜尋的對象必須來自指定網域
cache	搜尋Google 頁面存檔中最近歸檔的網頁
inanchor/allinanchor	搜尋網站上的鏈結文字，而回傳該鏈結所指向的網頁
related	查詢和指定的網址或URL有關聯的網頁(搜尋類似內容)
info	顯示指定的網域或URL之摘要資訊(網頁相關資訊)
daterange	過濾在特定時間內被google編入索引的網頁(限定時間範圍)
numrange	搜尋有指定範圍內數值的網頁(數字範圍)
define	搜尋名詞的定義
stocks	搜尋某家公司的股票資訊
location/source	縮減新聞資料的搜尋範圍

常用指令

Google Search 基本搜尋運算子

- **+**: 用在詞彙的前面，表示此詞彙必須要出現在網頁之中
- **-**: 用在詞彙的前面，表示排除此詞彙
- **""**: 雙引號刮起來，強制文字之順序
- **.**: 表示任一字元，如 bl.ck box
- *****: 表示任一單字，如 Apache/* Server
- **..**: 搜尋範圍內之數字或是金錢，如 1900..2019、\$300..\$900
- **OR |**: 表示其中之一，如 台灣("科技" | "首府")
- **:** Google 會自行判斷輸入文字之語系，做最好之處理。中文會有自行一套斷詞規則，
 - EX: 搜尋 國網中心台灣衫
- 那**AND**呢？

利用 Google Hacking 尋找資訊洩漏

- 傳統資訊洩漏
- 管理介面的洩漏如同告知歹徒保險箱位置
 - 暴力破解管理帳號
 - 後台防禦較弱
 - 套件管理介面
- 常見路徑
 - /admin, /administrator, /phpmyadmin, /manage
- 管理介面不對外開放存取
- 隱藏管理介面目錄(複雜目錄名稱)
- 加強後台防禦

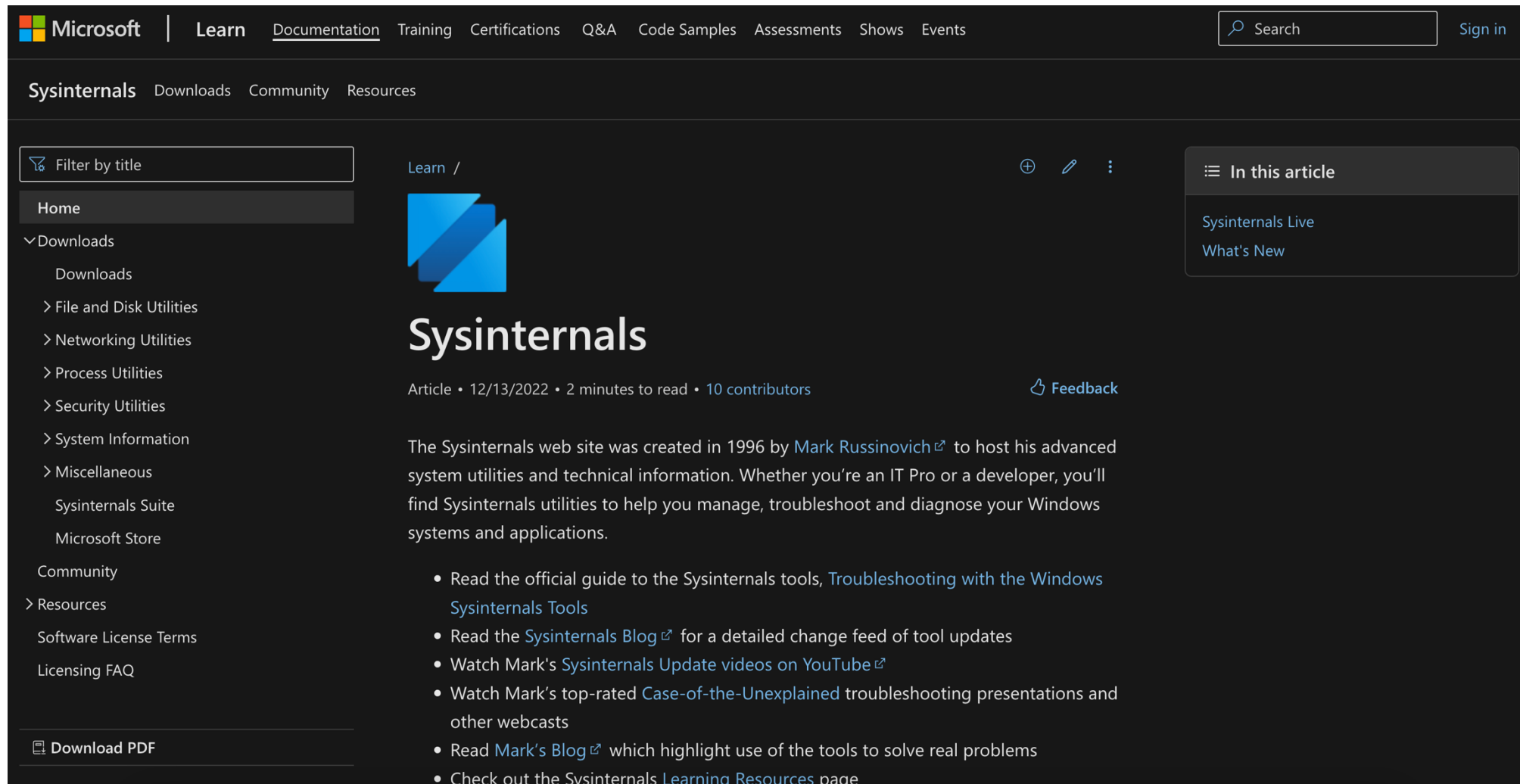
利用Google Hacking尋找資訊洩漏

- 目錄瀏覽
 - 洩漏網站目錄結構
 - 有機會存取機敏檔案
 - 有機會存取設定檔

Index of /teachers

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 config.php	2004-08-07 09:42	263	
 course.php	2003-12-04 21:05	2.3K	
 faculty.php	2009-06-15 00:42	18K	
 faculty_e.php	2005-09-21 17:24	18K	
 functions.php	2003-11-19 01:16	1.4K	
 images/	2003-11-26 19:28	-	
 pics/	2006-10-21 14:59	-	
 teachers_backup_20120229.tar.gz	2012-02-29 10:11	1.6M	

Microsoft Sysinternals



The screenshot shows the Microsoft Sysinternals website. The top navigation bar includes links for Microsoft, Learn, Documentation, Training, Certifications, Q&A, Code Samples, Assessments, Shows, and Events. A search bar and a 'Sign in' link are on the right. Below the navigation bar, the 'Sysinternals' section is highlighted, with links for Downloads, Community, and Resources. On the left, a sidebar contains a 'Filter by title' search box and a list of categories: Home, Downloads (with sub-items like File and Disk Utilities, Networking Utilities, etc.), Community, and Resources. The main content area features the Sysinternals logo, the title 'Sysinternals', and a brief description of the website's purpose. It also includes a list of links to various resources, such as the official guide, Sysinternals Blog, and YouTube videos. A 'Feedback' link is located at the bottom right of the main content area.

Microsoft | Learn | Documentation | Training | Certifications | Q&A | Code Samples | Assessments | Shows | Events

Search Sign in

Sysinternals Downloads Community Resources

Filter by title

Home

▼ Downloads

- Downloads
- > File and Disk Utilities
- > Networking Utilities
- > Process Utilities
- > Security Utilities
- > System Information
- > Miscellaneous
- Sysinternals Suite
- Microsoft Store

Community

> Resources

- Software License Terms
- Licensing FAQ

Download PDF

Learn /

Sysinternals

Article • 12/13/2022 • 2 minutes to read • 10 contributors

Feedback

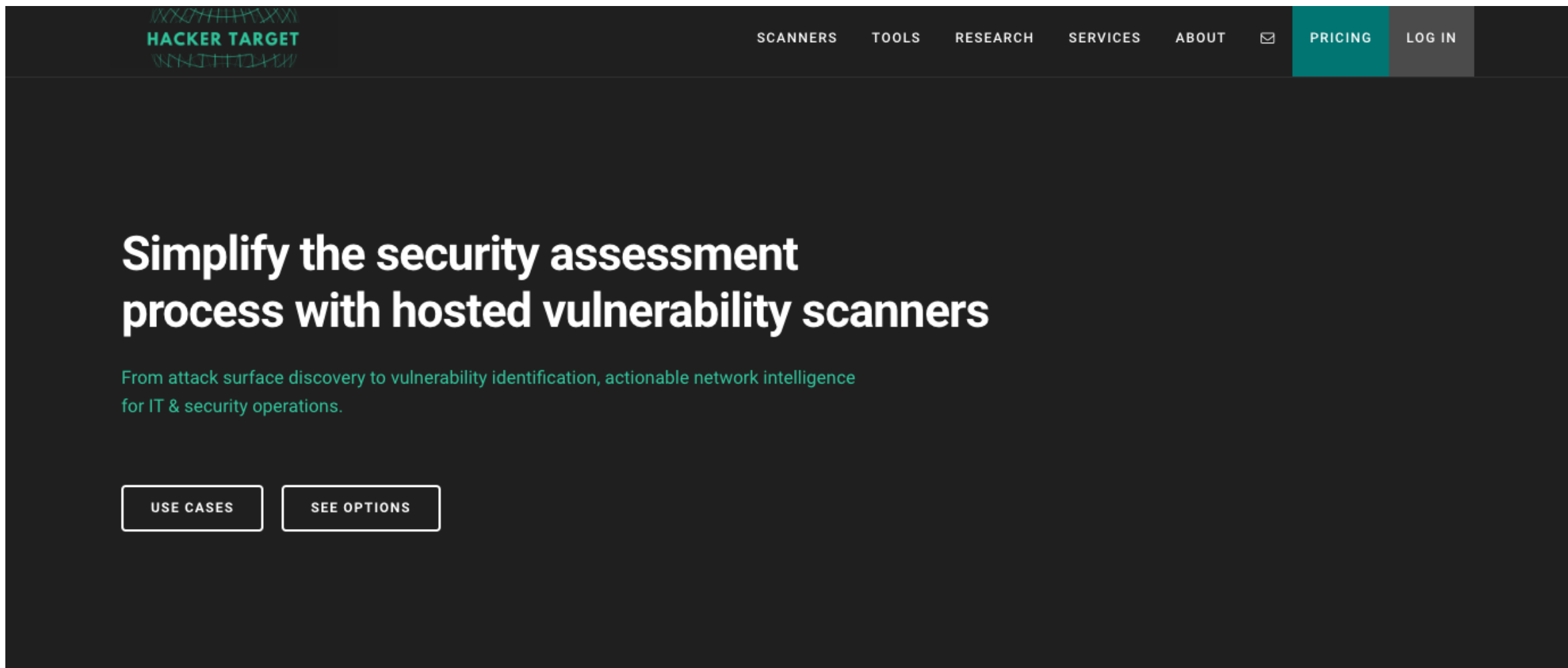
The Sysinternals web site was created in 1996 by [Mark Russinovich](#) to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.

- Read the official guide to the Sysinternals tools, [Troubleshooting with the Windows Sysinternals Tools](#)
- Read the [Sysinternals Blog](#) for a detailed change feed of tool updates
- Watch Mark's [Sysinternals Update videos on YouTube](#)
- Watch Mark's top-rated [Case-of-the-Unexplained](#) troubleshooting presentations and other webcasts
- Read [Mark's Blog](#) which highlight use of the tools to solve real problems
- Check out the Sysinternals [Learning Resources](#) page

In this article


- Sysinternals Live
- What's New

<https://learn.microsoft.com/en-us/sysinternals/>



The screenshot shows the Hacker Target website. The header is dark with the logo on the left and navigation links on the right. The main content area has a large heading and a subheading. At the bottom of the main area are two buttons.

HACKER TARGET

SCANNERS TOOLS RESEARCH SERVICES ABOUT  **PRICING** LOG IN

Simplify the security assessment process with hosted vulnerability scanners

From attack surface discovery to vulnerability identification, actionable network intelligence for IT & security operations.

[USE CASES](#) [SEE OPTIONS](#)

<https://hackertarget.com/>

On-Line Tools

Pentest Tools YOUR SCANS ▾ Tools ▾ Features ▾ Pricing Services Resources ▾ Company ▾ Sign in Register

The essential penetration testing tools, all in one place

Pentest-Tools.com is the leading cloud-based toolkit for offensive security testing. Focused on web applications and network security testing, the platform helps you **reduce repetitive work** and saves you time for more creative hacking, custom testing, and security research.

[Try the live demo](#) [Compare pricing plans](#)

Found 671 subdomains

Subdomain	IP address	Netname (whois)
skyline.github.com	13.107.226.42	MSFT
examregistration.github.com	20.40.202.15	MSFT

Found 7 open ports (1 host)

Port Number	State	Service Name	Service Product
445	open	microsoft-ds	Microsoft Windows 7
8080	open	http	Apache Tomcat

SQL Injection CONFIRMED

Vulnerable URL	Method	Vulnerable Parameter
https://bank.pentest-ground.com/find-customers	GET	search_str

Vulnerability summary

Target is vulnerable to CVE-2021-34473 - Microsoft Exchange ProxyShell RCE!
[*] Trying to gain an exploit session...
Target successfully exploited

Scan activity: 5 IP ADDRESSES, 6 HOSTNAMES, 41 PORTS

<https://pentest-tools.com/>

Google Hacking » 0 Credits Free

Target domain

- Q Directory listing vulnerabilities
- Q Configuration files exposed
- Q Database files exposed
- Q Log files exposed
- Q Backup and old files
- Q Login pages
- Q SQL errors
- Q Publicly exposed documents
- Q phpinfo()

Find Subdomains » 20 Credits Free

Domain name

☒ Include subdomain details

Start

Reset

Whois Lookup » 0 Credits Free

Whois

Start

Reset

Wireshark


Official certification from the Wireshark Foundation is available! Learn about becoming a Wireshark Certified Analyst. ↗


WIRESHARK Download ▾ Learn ▾ Resources ▾ Tools ▾ Community ▾ Develop ▾ Members Certifications [Donate](#)

The world's leading network protocol analyzer

Wireshark lets you dive deep into your network traffic – free and open source.

[Download Now](#)




 Find out more about the new WCA certification

<https://www.wireshark.org/>

網路與系統安全測試



檢查一下網站的狀態



We give you X-Ray Vision for your Website

In just 20 seconds, you can see *what attackers already know*

Enter a URL to start 📌

E.g. google.com

Analyze URL

DNS Records

2a04:4e42:600::81
2a04:4e42:400::81
2a04:4e42:200::81
2a04:4e42::81
CNAME
ddns1.bbc.com
dns0.bbc.co.uk
dns0.bbc.com
dns1.bbc.co.uk
dns1.bbc.com
ddns0.bbc.co.uk
ddns0.bbc.com
ddns1.bbc.co.uk

Cookies

SOCS	CAAA8giAzqKlBg
expires	Tue, 06-Aug-2024 16:42:15...
path	/
domain	.google.com
SameSite	lax
AEC	Ad49MVEtQVG6LH6KJy7oJI@cK...
CONSENT	PENDING+192

Crawl Rules

User-agent	*
Disallow	/bitesize/search?
Disallow	/bitesize/study-support
Disallow	/cbbc/search\$
Disallow	/cbbc/search/
Disallow	/cbeebies/search\$
Disallow	/chwilio/
Disallow	/chwilio\$
Disallow	/chwilio?
Disallow	/iplayer/bigscreen/
Disallow	/iplayer/cbbc/episodes/
Disallow	/iplayer/cbbc/search
Disallow	/iplayer/cbeebies/episode...
Disallow	/iplayer/cbeebies/search
Disallow	/iplayer/search
Disallow	/indepthtoolkit/smallprox\$

Cloudflare bot management solution identifies and mitigates automated traffic to protect websites from bad bots.

Learn more at: <https://www.cloudflare.com/en-...>

Priority Hints

Priority Hints exposes a mechanism for developers to signal a relative priority for browsers to consider when fetching resources.

Pages

/	Last Modified	16 October 2018
	Change Frequency	monthly
	Priority	1.00
/about		
/donations		
/app		
/hiring		
/privacy		
/press		
/newsletter		
/spread		
/bangs		
/settings		

Security.Txt


Present	<input checked="" type="checkbox"/> Yes
File Location	/.well-known/security.txt
PGP Signed	<input checked="" type="checkbox"/> Yes
Hash	SHA512
Contact	/cloudflare
Contact1	mailto:security@cloudflar...
Contact2	/abuse/
Preferred-Languages	en
Encryption	/gpg/security-at-cloudfla...
Canonical	/.well-known/security.txt
Policy	/disclosure
Hiring	/careers/jobs/
Expires	22 March 2023


Linked Pages

Summary	
Internal Link Count	329
External Link Count	8

<https://web-check.xyz/>

以外部的觀點

 **Web Check**


 ncku.edu.tw

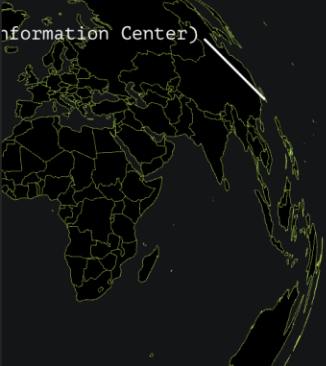
27 jobs successful 2 jobs skipped 8 jobs failed Finished in 6200 ms

[Show Details](#) [Dismiss](#)

[Show Filters](#) [Export Data](#) [Learn About The Results](#) [More Tools](#) [View GitHub](#)

Server Location

City	null, East District, Tain...
Country	Taiwan 
Timezone	Asia/Taipei
Languages	zh-TW,zh,nan,hak
Currency	Dollar (TWD)



SSL Certificate

Subject	*.ncku.edu.tw
Issuer	Sectigo Limited
Expires	1 August 2026
Renewed	30 June 2025
Serial Num	66662E7BFD8E73C932C...
Fingerprint	77:86:9B:C5:39:75:B...

Extended Key Usage

- TLS Web Server Authentication
- TLS Web Client Authentication

Domain Whois

Headers

date	31 July 2025
content-type	1 August 2001
transfer-encoding	chunked
vary	Accept-Encoding
set-cookie	PageLang=zh-tw; path=/; s...
expires	31 December 2017
last-modified	28 July 2025
cache-control	no-store
pragma	no-cache
x-frame-options	SAMEORIGIN
x-xss-protection	1; mode=block
x-content-type-options	nosniff
strict-transport-security	max-age=63072000

Cookies

PageLang	zh-tw
PageLang	zh-tw
_counter	84608172
PageLang	zh-tw

<https://web-check.xyz/>

DNS 狀態檢查



Creative Cloud
首年享低於 55 折優惠
須遵守適用條款。

立即購買

Adobe
Creative Cloud

HomeAll ToolsDNS LookupPublic DNS List

220.138.192.130

DNS CHECK

A

Search

CD Flag

Refresh: 20 sec.

San Francisco CA, United States
OpenDNS

Mountain View CA, United States
Google

Berkeley, US
Quad9

Kansas City, United States
WholeSale Internet, Inc.

San Jose, United States
Corporate West Computer Systems

San Francisco, US

CHECK DNS PROPAGATION


Whether you have recently changed your DNS records, switched web host, or started a new website - checking whether the DNS records are propagated globally is essential. DNS Checker provides a free DNS propagation check service to check Domain Name System records against a selected list of DNS servers in multiple regions worldwide. Perform a quick DNS propagation lookup for any hostname or domain, and check DNS data collected from all available DNS Servers to confirm that the DNS records are fully propagated.

使用完整應用程式創造
您的世界

立即試用









Adobe
Creative Cloud

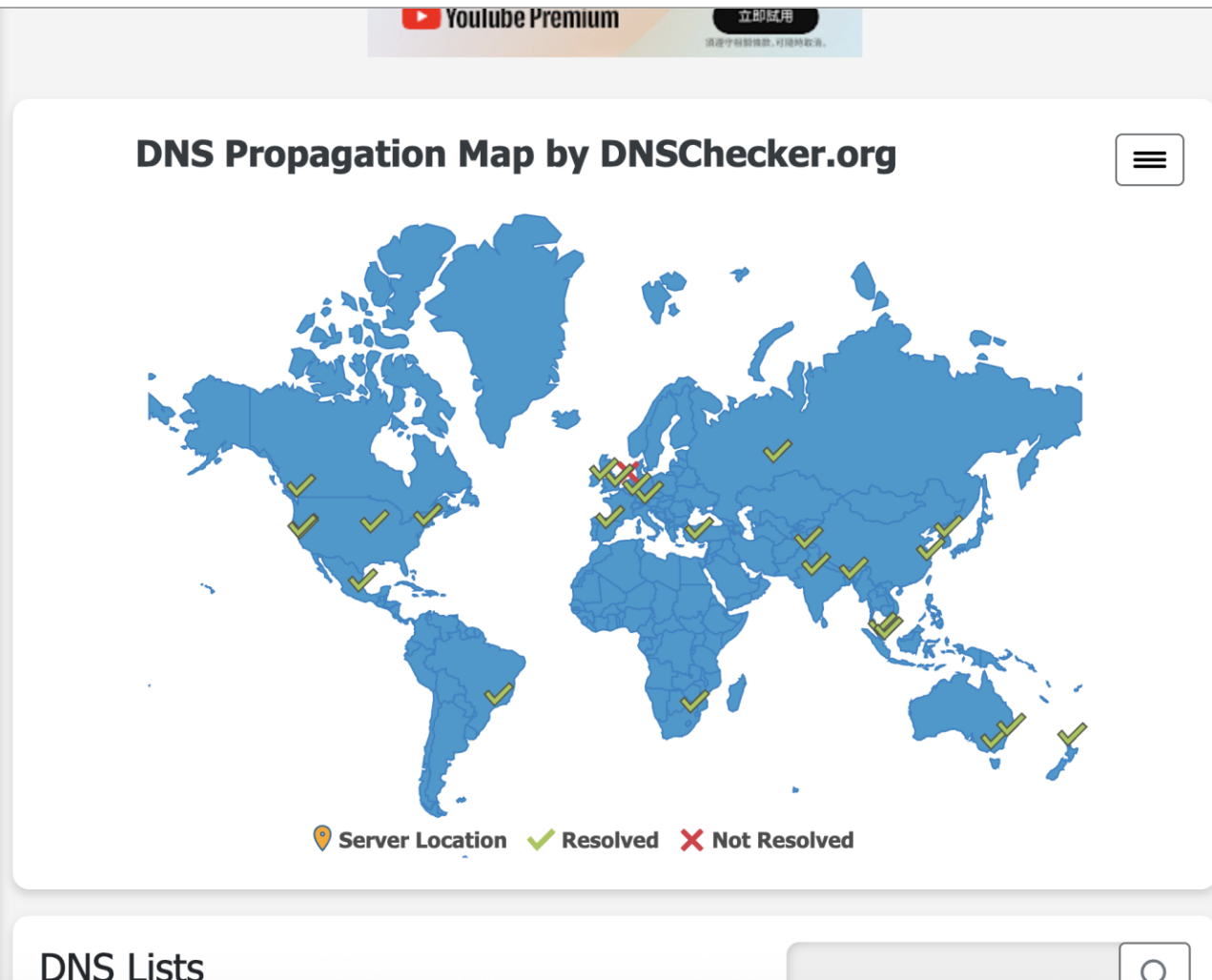
DNS Propagation Map by DNSChecker.org



<https://dnschecker.org/>

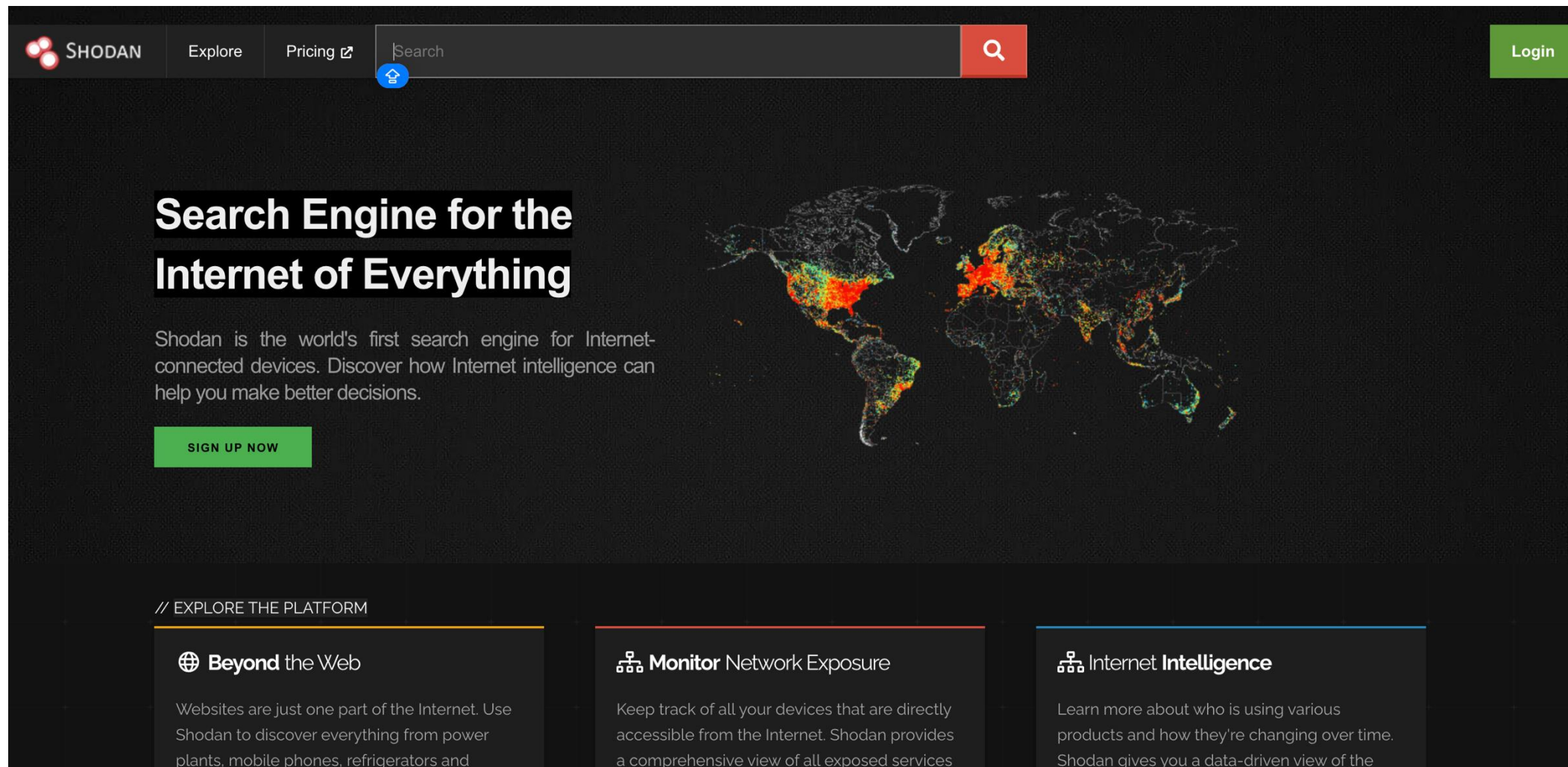
從不同的區域進行測試

 Mountain View CA, United States	172.65.90.67 172.65.90.66	✓
Google ⓘ		
 Berkeley, US	172.65.90.67 172.65.90.66	✓
Quad9 ⓘ		
 Kansas City, United States	172.65.90.67 172.65.90.66	✓
WholeSale Internet, Inc. ⓘ		
 San Jose, United States	172.65.90.67 172.65.90.66	✓
Corporate West Computer Systems ⓘ		
 San Francisco, US	172.65.90.66 172.65.90.67	✓
Quad9 ⓘ		
 New York, United States	172.65.90.66 172.65.90.67	✓
Oracle Corporation ⓘ		
 Burnaby, Canada	172.65.90.66 172.65.90.67	✓
Fortinet Inc ⓘ		
 Yekaterinburg, Russian Federation	172.65.90.66	



<https://dnschecker.org/>

物聯網安全搜尋引擎



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with the Shodan logo, links for 'Explore' and 'Pricing', a search bar with a magnifying glass icon, and a 'Login' button. Below the navigation bar, the main heading reads 'Search Engine for the Internet of Everything'. To the right of the heading is a world map with various colored dots representing data points. Below the heading, a paragraph states: 'Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.' A green button labeled 'SIGN UP NOW' is positioned below this text. At the bottom, there is a section titled '// EXPLORE THE PLATFORM' with three columns. The first column is titled 'Beyond the Web' and describes discovering everything from power plants to mobile phones. The second column is titled 'Monitor Network Exposure' and describes keeping track of all devices directly accessible from the Internet. The third column is titled 'Internet Intelligence' and describes learning more about who is using various products and how they're changing over time.

SHODAN Explore Pricing Search Login

Search Engine for the Internet of Everything

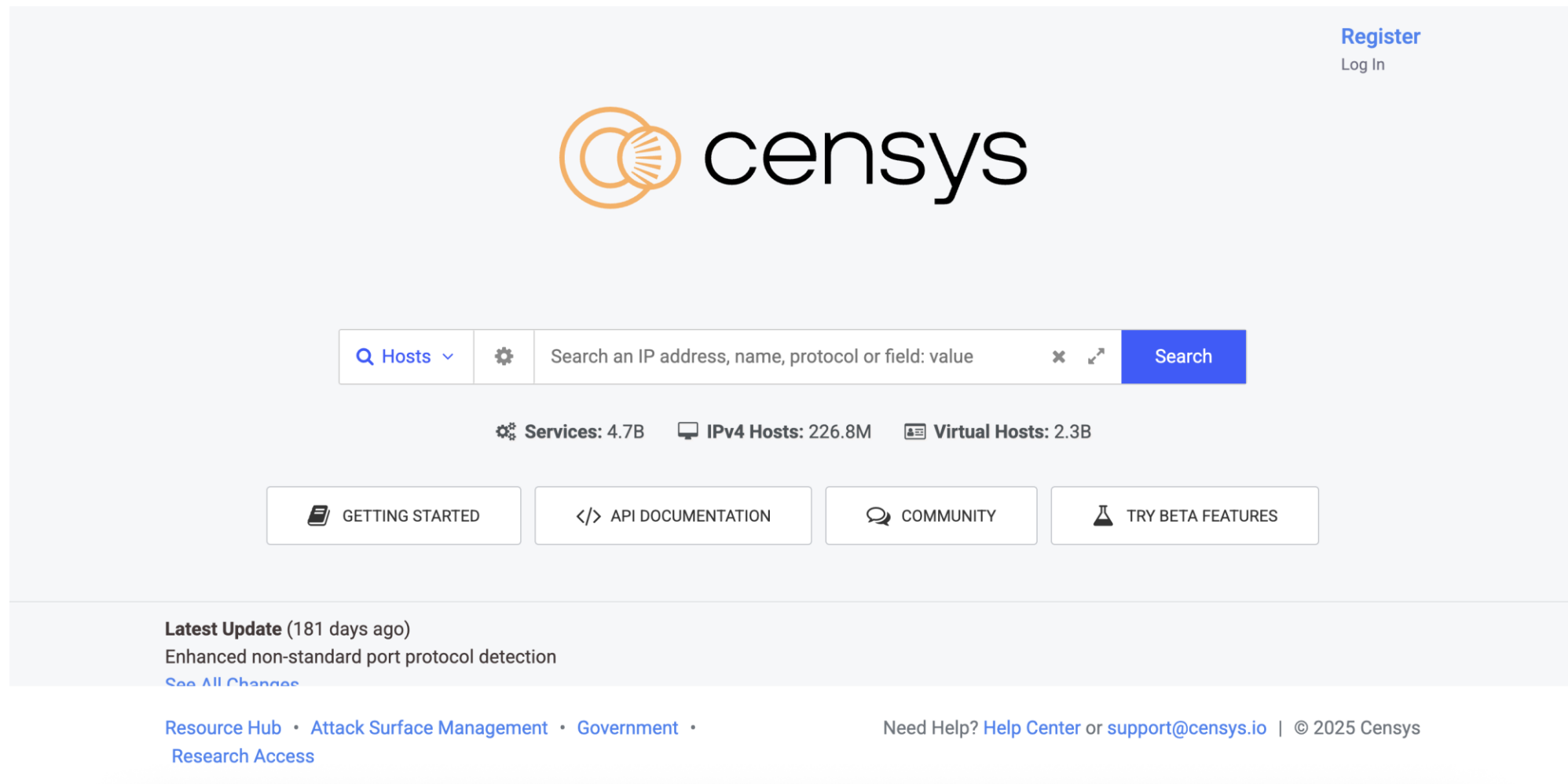
Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

[SIGN UP NOW](#)


// EXPLORE THE PLATFORM

- Beyond the Web**
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and
- Monitor Network Exposure**
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services
- Internet Intelligence**
Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the

<https://www.shodan.io/>



SSL 檢測

 **Qualys** SSL Labs

HomeProjectsQualys Free TrialContact

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

Submit

☐ Do not show the results on the boards

Recently Seen

- [safetydepositary.net](#)
- [cipherdrop.app](#)
- [mock-api-hmg.certisign.com.b...](#)
- [adelphi.de](#)
- [www.civfund.org](#)

Recent Best

coupa.com	A+
gruposaudebrasil.com	A+
massive.ag	A
s3.us-east-1.amazonaws.com	A
indyapa.net	A

Recent Worst

ftp.no.co	T
vestiguimconsulting.co.za	T
www.beandoser.com	T
subscription.rhsm.redhat.com	T
mail.lukseh.org	T

<https://www.ssllabs.com/ssltest/analyze.html>



Zed Attack Proxy (ZAP)

by **Checkmarx**

The world's most widely used web app scanner. Free and open source. A community based GitHub Top 1000 project that anyone can contribute to.

[Intro Video](#)

[Quick Start Guide](#)

[Download Now](#)

ZAP is an independent Open Source project - learn more.



<https://www.zaproxy.org/>

程式安全、網址安全檢測



<https://www.virustotal.com/>

國內的 Virus Check



訊息公告
Notice

檔案上傳
Upload File

檢測進度查詢
Progress

系統介紹
Introduction

使用說明與常見問題
Manual & FAQ

使用規範
Terms of Use

惡意檔案檢測服務

Virus Check

Integrate static and dynamic cybersecurity analyzing skills;
Detect hidden malware in a comprehensive manner

檔案上傳 File Upload

選擇檔案 未選擇任何檔案

提醒您，檔案上傳功能僅限電腦版，手機版僅提供查詢功能。

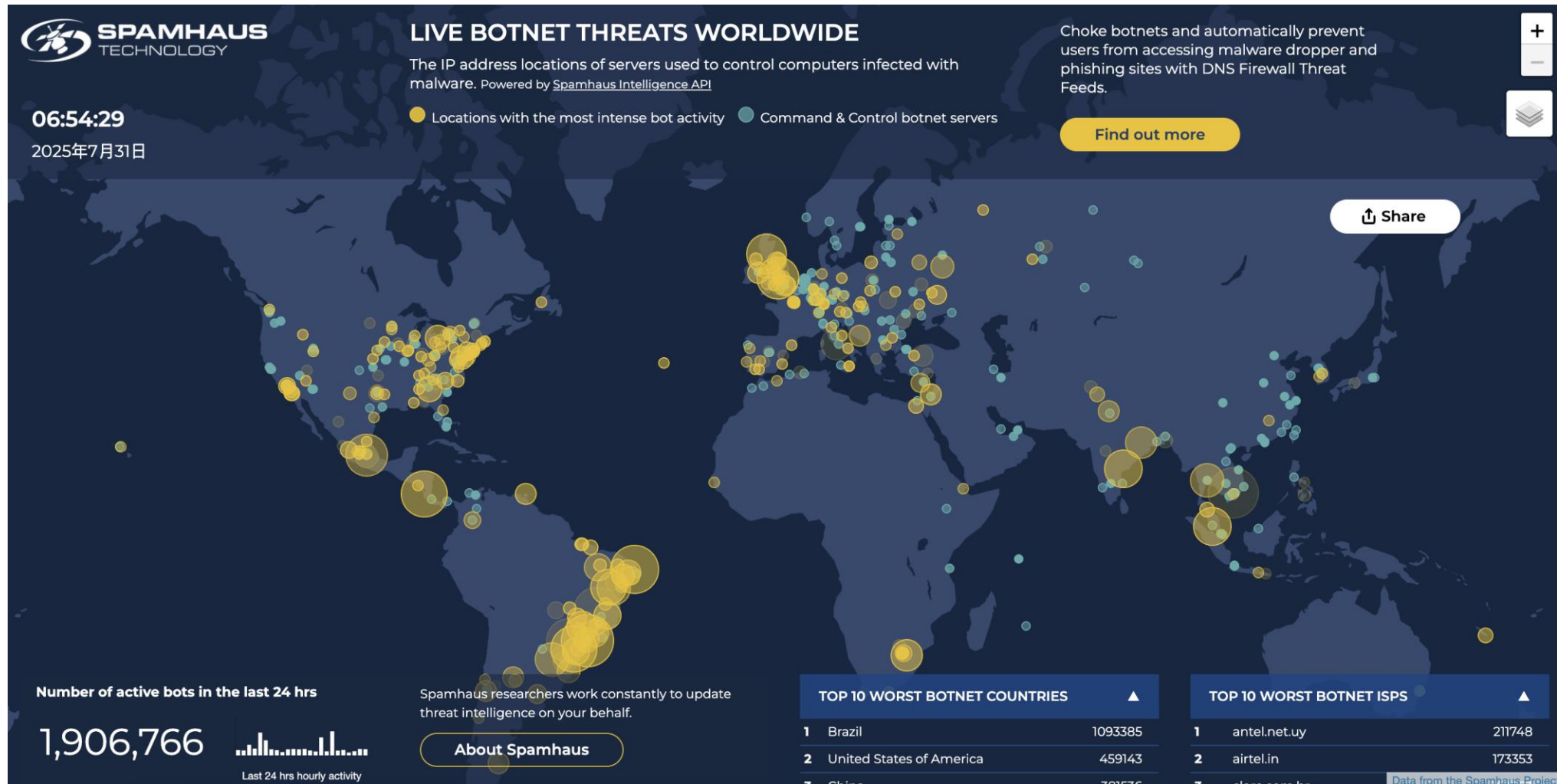
壓縮檔密碼 Unzip password

限長度為 10 碼以內的英文字母與數字

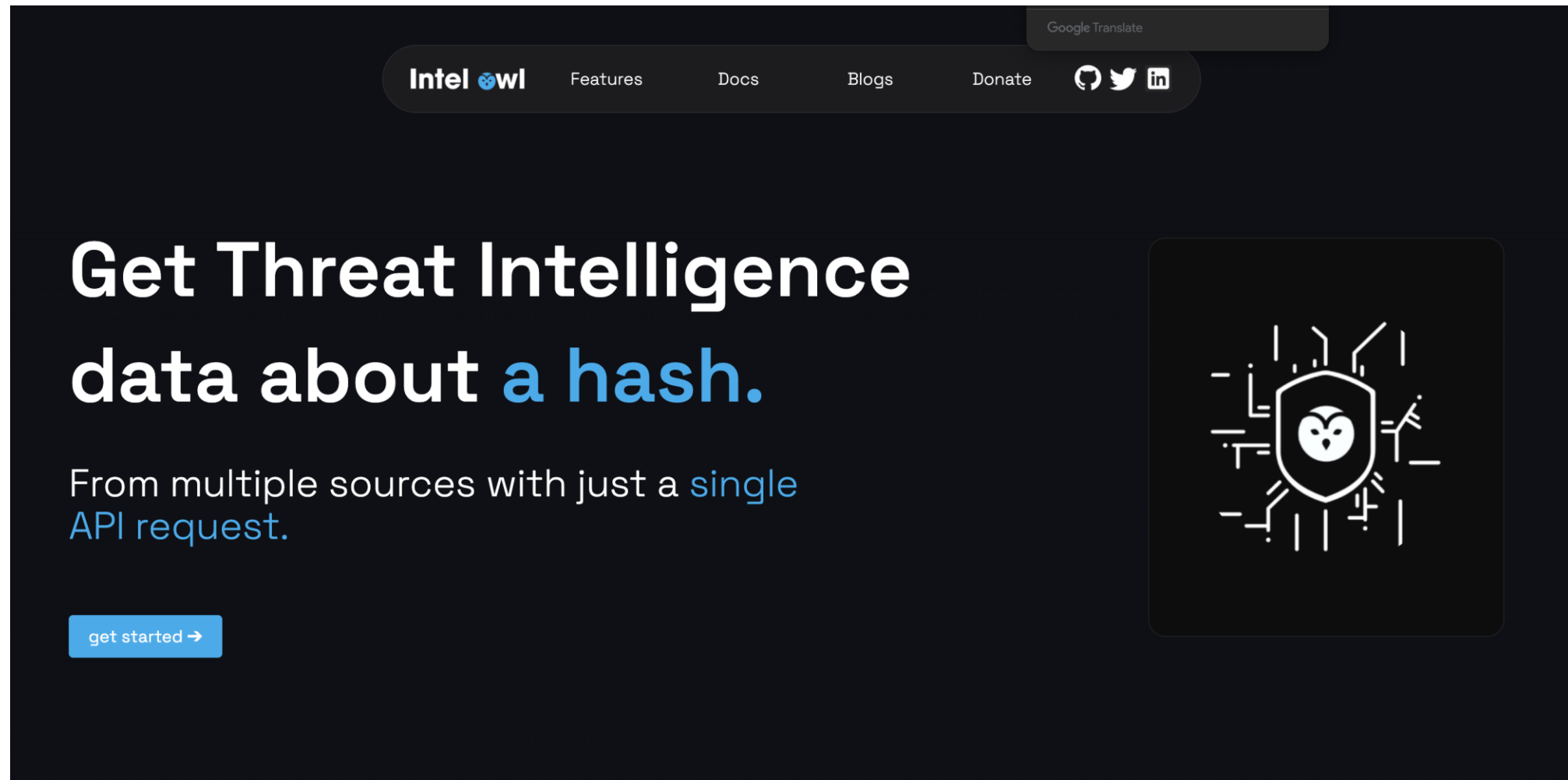
隱私權 · 條款

<https://viruscheck.tw/>

Live Botnet Threats Worldwide



<https://www.spamhaus.com/threat-map/>



案例分享



IBM X-Force Exchange

The screenshot displays the IBM X-Force Exchange dashboard. At the top, a navigation bar includes the IBM X-Force Exchange logo, a hamburger menu, and links for 'Create IBMid' and 'Log In'. Below the navigation bar, a header section reads 'Research, Collaborate and Act on threat intelligence'. A search bar is prominently featured, with a dropdown menu open showing instructions: 'Search or submit a file to scan. Check for IOCs, keywords, malware intelligence, or even Collections that other users have contributed.' To the right of the search bar, there are links for 'Scan file' and a 'Trending' section listing various threat indicators such as IP addresses and hashtags. The main dashboard area is divided into three columns. The left column, titled 'IBM X-Force OSINT Advisories', lists several advisories with dates and 'New' tags. The middle column, titled 'IBM X-Force Threat Group Reports', lists reports on specific threat groups like Qilin Ransomware and Scattered Spider. The right column contains a 'Skip Tour' button and a 'Next' button. At the bottom right, there is an 'AlertCon™ Threat Level' indicator showing a level of 1.

IBM X-Force Exchange

Research, Collaborate and Act on threat intelligence

Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...

Search

Search or submit a file to scan. Check for IOCs, keywords, malware intelligence, or even Collections that other users have contributed.

Next

IBM X-Force OSINT Advisories

Curated by the IBM X-Force team

Leveraging Compromised Service Account... **New**

2025年7月31日

Microsoft SharePoint Zero-Day Actively... **New**

2025年7月24日

The Growing CRYPTO24 Ransomware Group

2025年7月23日

Mispadu Resurfaced

2025年7月19日

View more

SafePay ransomware threatens to leak 3.5TB of ... **New**

2025年7月31日

Malware Discovered in Endgame Gear Gaming Mous... **New**

2025年7月31日

Amazon's Coding Tool Hacked — Experts Warn of ... **New**

2025年7月31日

Darktrace's Cyber AI Analyst in Action: 4 Real... **New**

2025年7月31日

View more

IBM X-Force Threat Group Reports

Curated by the IBM X-Force team

Qilin Ransomware Group Profile

2025年7月25日

Scattered Spider Threat Group Profile

2025年7月4日

View more

AlertCon™ Threat Level 1

<https://exchange.xforce.ibmcloud.com/>

AlienVault OTX - LevelBlue

LevelBlue/Labs

Dashboard

Browse

Scan Endpoints


Create Pulse

Submit Sample

API Integration

All Search OTX

YILANGTSAI



YILANGTSAI

Profile

0 pulses

0 contributions

STATISTICS

0

FOLLOWERS

1

SUBSCRIBERS

0

CONTRIBUTED INDICATORS

GROUPS

No Groups

FOLLOWERS

FOLLOWING

No Followers

SUBSCRIBERS

SUBSCRIBING


TOP COMMUNITY CONTRIBUTORS

Pulses

Activity

Suggested Edits (0)

LevelBlue New Updated Subscribed




PoS Scammers Toolbox

CREATED 11 YEARS AGO | MODIFIED 8 YEARS AGO by AlienVault | Public | TLP: Green

FileHash-MD5: 8 | URL: 10 | YARA: 2 | Domain: 6 | Hostname: 2

Unsubscribe (332,718)




RAZOR BLADES IN THE CANDY JAR

CREATED 11 YEARS AGO | MODIFIED 10 YEARS AGO by AlienVault | Public | TLP: Green

Hostname: 11

Unsubscribe (332,430)




Linking Asprox, Zemot, Rovix and Rerdom Malware Fam...

CREATED 11 YEARS AGO | MODIFIED 8 YEARS AGO by AlienVault | Public | TLP: Green

FileHash-MD5: 4 | Domain: 6

Asprox, Zemot, Rovix

Unsubscribe (332,383)



Operation Double Tap

CREATED 11 YEARS AGO | MODIFIED 8 YEARS AGO by AlienVault | Public | TLP: Green

CVE: 2 | FileHash-MD5: 9 | URL: 2 | Domain: 5 | Hostname: 5

Unsubscribe (332,338)

<https://otx.alienvault.com/>

Security List

SECURELIST by Kaspersky


CompanyAccountGet In TouchDark mode offEnglish

SolutionsIndustriesProductsServicesResource CenterAbout UsGDPR

Content menu


Search...

Subscribe



ToolShell: a story of five vulnerabilities in Microsoft SharePoint

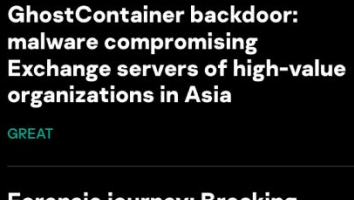
BORIS LARIN, GEORGY KUCHERIN, ILYA SAVELYEV



RESEARCH

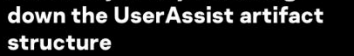
Cobalt Strike Beacon delivered via GitHub and social media

A campaign targeting Russian entities leveraged social media, Microsoft Learn Challenge, Quora, and GitHub as intermediate C2 servers to deliver Cobalt Strike Beacon.




GhostContainer backdoor: malware compromising Exchange servers of high-value organizations in Asia

GREAT




Forensic journey: Breaking down the UserAssist artifact structure

AWAD ALJUAID




Code highlighting with Cursor AI for \$500,000

GEORGY KUCHERIN




Approach to mainframe penetration testing on z/OS. Deep dive into RACF

DENIS STEPANOV, ALEXANDER KOROTIN



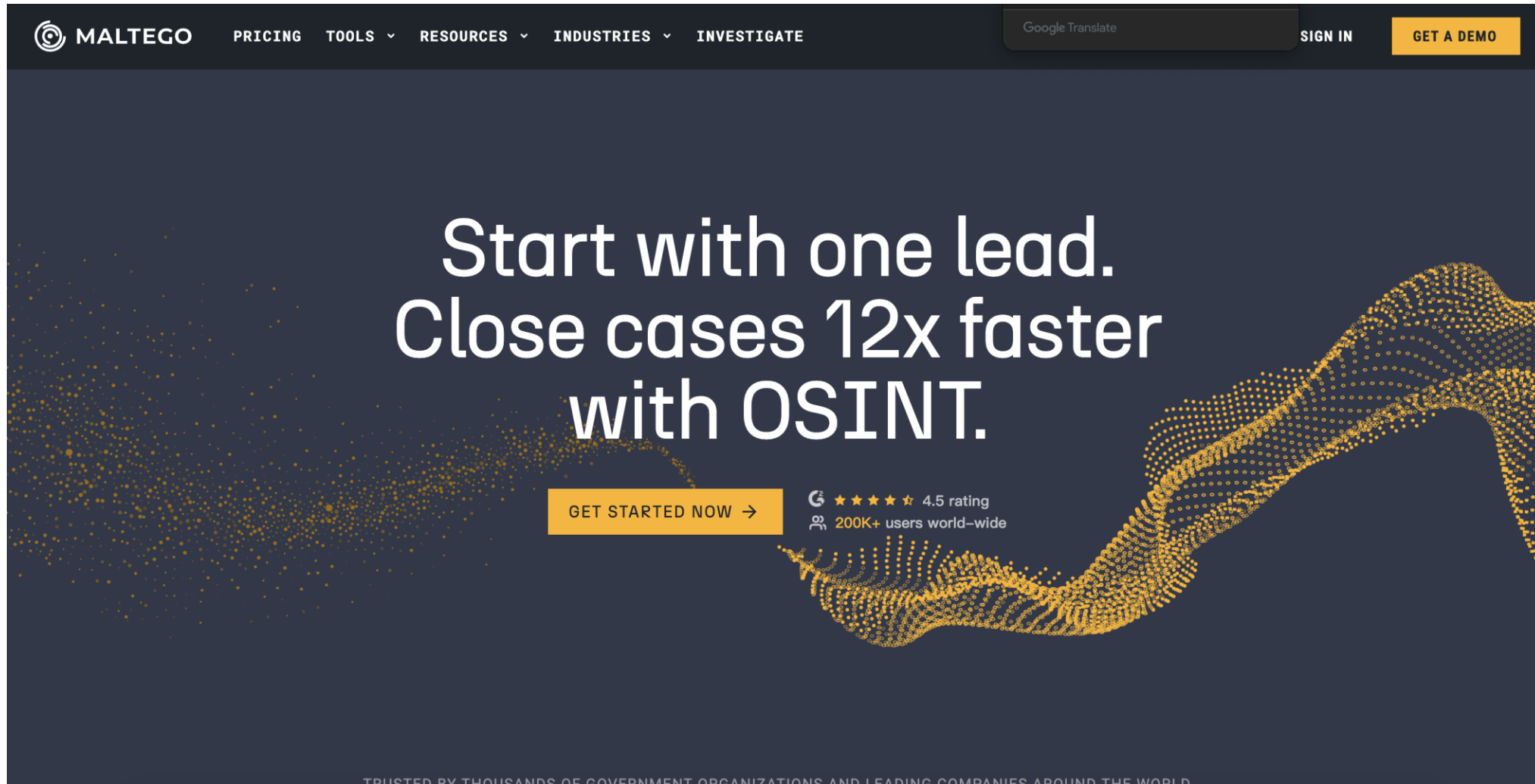
Batavia spyware steals data



The SOC files: Rumble in the jungle or APT41's new target in Africa

<https://securelist.com/>

Maltego CE

The image shows the Maltego CE website landing page. The header is dark with the Maltego logo and navigation links: PRICING, TOOLS, RESOURCES, INDUSTRIES, and INVESTIGATE. There are also links for Google Translate, SIGN IN, and GET A DEMO. The main content area has a dark background with a large white text overlay that reads "Start with one lead. Close cases 12x faster with OSINT." Below this text is a yellow button that says "GET STARTED NOW →". To the right of the button, there is a 4.5 star rating and text indicating "200K+ users world-wide". The background features abstract yellow particle patterns. At the bottom, there is a small line of text: "TRUSTED BY THOUSANDS OF GOVERNMENT ORGANIZATIONS AND LEADING COMPANIES AROUND THE WORLD".

MALTEGO PRICING TOOLS ▾ RESOURCES ▾ INDUSTRIES ▾ INVESTIGATE Google Translate SIGN IN GET A DEMO

Start with one lead. Close cases 12x faster with OSINT.

GET STARTED NOW →

★★★★☆ 4.5 rating
200K+ users world-wide

TRUSTED BY THOUSANDS OF GOVERNMENT ORGANIZATIONS AND LEADING COMPANIES AROUND THE WORLD

<https://www.maltego.com/>

WannaCry大規模來襲

- 惡意程式加上勒索，針對系統重大弱點進行自動化攻擊與散佈



WannyCry造成的影響

- 資安研究，有時候是一體的兩面
- 特殊的網域名稱
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

SINKHOLED!

This domain has been sinkholed by Kryptos Logic.

<https://dq.yam.com/post.php?id=8002>

擋下「想哭」病毒的英國資安專家 被控開發惡意軟體遭逮

2017-09-04 by: 衛衛

10167 10167 10167 10167 10167

你還記得今年五月讓全球人心惶惶的電腦病毒「想哭」嗎？近日，被封為網路英雄、成功擋下「想哭」的英國資安專家遭控開發惡意勒索軟體，在美國遭到FBI的逮捕。



Photo: Press today

圖為今年 23 歲的英國資安專家哈欽斯。近日，他被控開發惡意勒索軟體在美國拉斯維加斯機場遭到 FBI 逮捕。

擋下「想哭」聲名大噪

你還記得今年五月席捲全球 150 個國家、造成超過 100 萬台電腦中毒的惡意勒索軟體「想哭」(WannaCry)嗎？當時，英國 23 歲的資安專家哈欽斯(Marcus Hutchins)找到了「殺手開關」，成功阻擋「想哭」的進一步蔓延而聲名大噪。

DNS記錄與WannaCry

>	17/07/05 23:14:17.000	Jul 05 15:14:17 10.0.1.18 CEF:0 Lastline Enterprise 7.10 signature-match IDS Signature Match 6 act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87026 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14323232?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.38.137 end=Jul 05 2017 23:13:47 CST externalId=14323232 proto=TCP sourceDnsDomain=78-user127.cc.ncut.edu.tw src=140.128.78.127 start=Jul 05 2017 23:13:47 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline
>	17/07/05 21:26:42.000	Jul 05 13:26:42 10.0.1.18 CEF:0 Lastline Enterprise 7.10 signature-match IDS Signature Match 6 act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=86756 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312974?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:26:12 CST externalId=14312974 proto=TCP sourceDnsDomain=95-user169.lib.ncut.edu.tw src=140.128.95.169 start=Jul 05 2017 21:26:12 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline
>	17/07/05 21:21:25.000	Jul 05 13:21:25 10.0.1.18 CEF:0 Lastline Enterprise 7.10 signature-match IDS Signature Match 6 act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87049 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312456?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:20:48 CST externalId=14312456 proto=TCP sourceDnsDomain=t2.ba.dep-appoint.static.012.ippool.cyut.edu.tw src=120.110.27.12 start=Jul 05 2017 21:20:48 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline
>	17/07/05 21:21:13.000	Jul 05 13:21:13 10.0.1.18 CEF:0 Lastline Enterprise 7.10 signature-match IDS Signature Match 6 act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87049 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312456?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:20:48 CST externalId=14312456 proto=TCP sourceDnsDomain=t2.ba.dep-appoint.static.012.ippool.cyut.edu.tw src=120.110.27.12 start=Jul 05 2017 21:20:48 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline

Mirai Botnet

- Mirai可以讓執行Linux的計算系統成為被遠端操控的「殭屍」，以達到通過殭屍網路進行大規模網路攻擊的目的
- Mirai的主要感染物件是可存取網路的消費級電子裝置，例如網路監控攝錄影機和家庭路由器等。
- Mirai構建的殭屍網路已經參與了幾次影響廣泛的大型分散式阻斷服務攻擊，包括2016年9月20日針對電腦保安撰稿人布萊恩·克萊布斯個人網站的攻擊、對法國網站代管商OVH的攻擊，以及2016年10月Dyn公司網路攻擊事件
- Mirai的原始碼已經以開源的形式發布，其中的技術也已被其他一些惡意軟體採用

Mirai Botnet

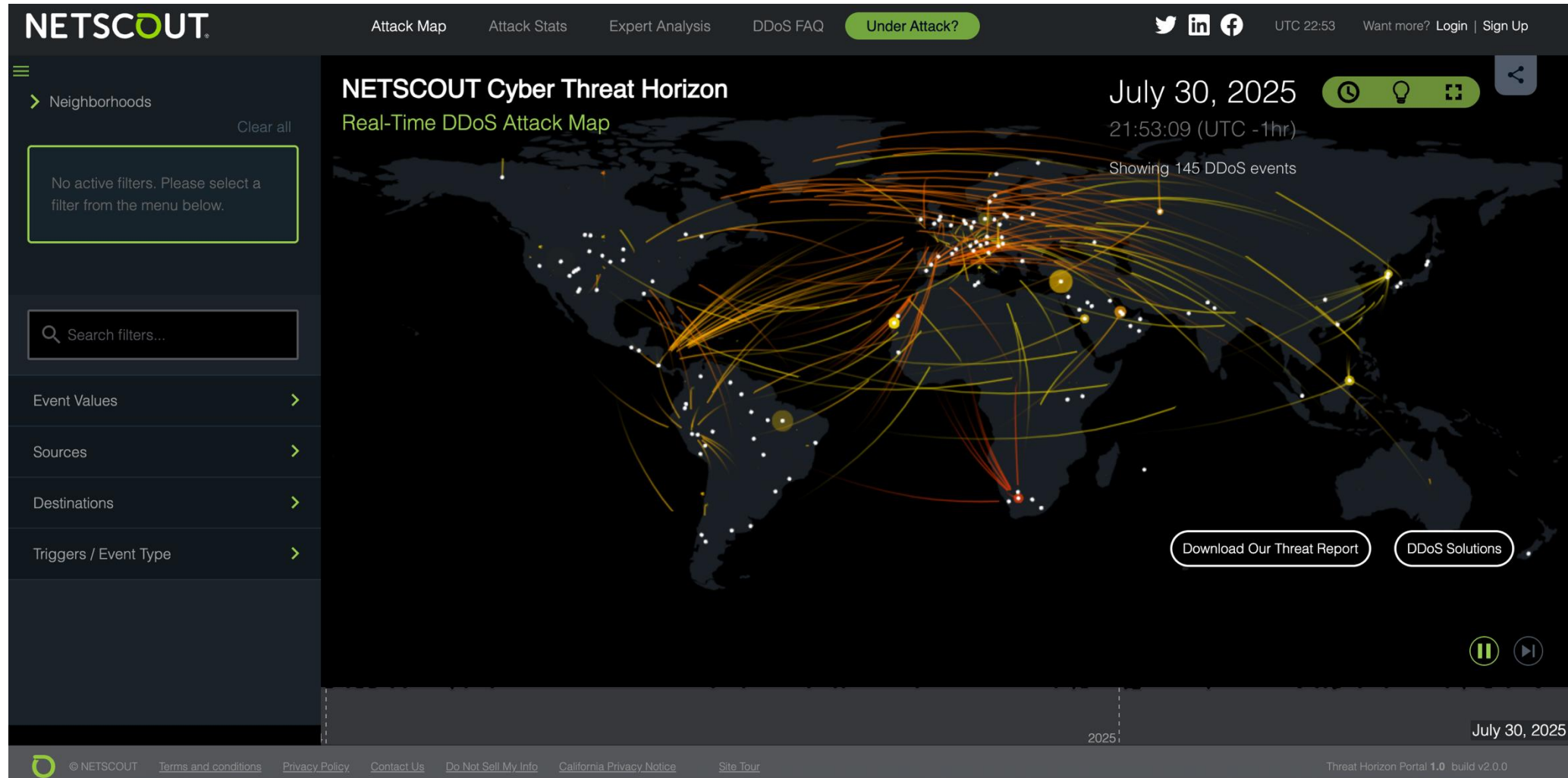
- 當軍火庫被打開時
- 開發攻擊用的惡意程式變得更加容易

jgamblin committed on GitHub Merge pull request #38 from Red54/patch-1 ...		Latest commit 3273043 24 days ago
dlr	Trying to Shrink Size	10 months ago
loader	Trying to Shrink Size	10 months ago
mirai	Trying to Shrink Size	10 months ago
scripts	Transcribe post to markdown while preserving	10 months ago
ForumPost.md	Transcribe post to markdown while preserving	10 months ago
ForumPost.txt	Update ForumPost.txt	9 months ago
LICENSE.md	Trying to Shrink Size	10 months ago
README.md	Fix a typo in README.md	24 days ago

jgamblin Trying to Shrink Size		Latest commit 9779d43 on 25 Oct 2016
..		
bot	Trying to Shrink Size	10 months ago
cnc	Trying to Shrink Size	10 months ago
tools	Trying to Shrink Size	10 months ago
build.sh	Trying to Shrink Size	10 months ago
prompt.txt	Trying to Shrink Size	10 months ago

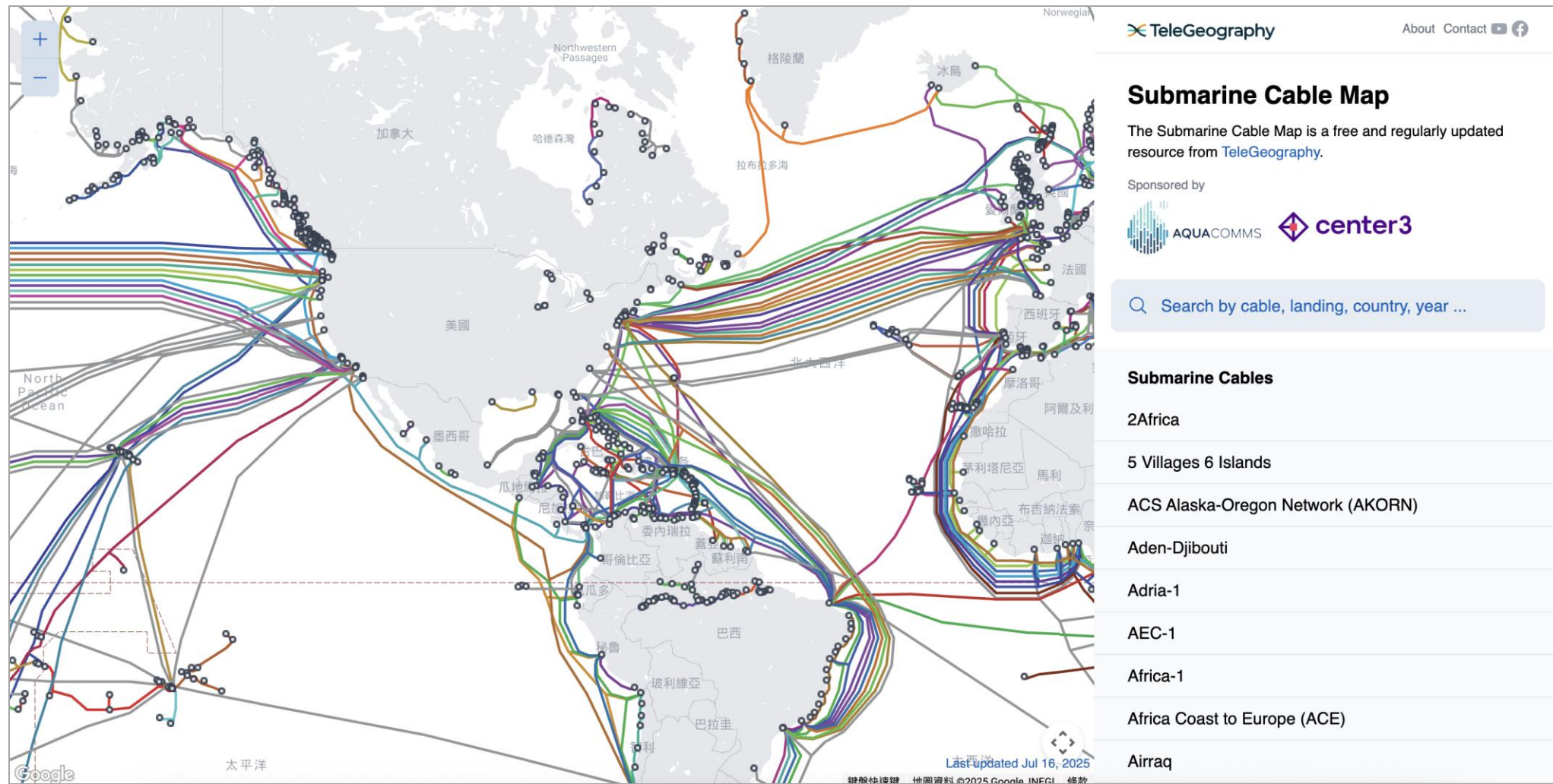
<https://github.com/jgamblin/Mirai-Source-Code>

Cyber Threat Horizon



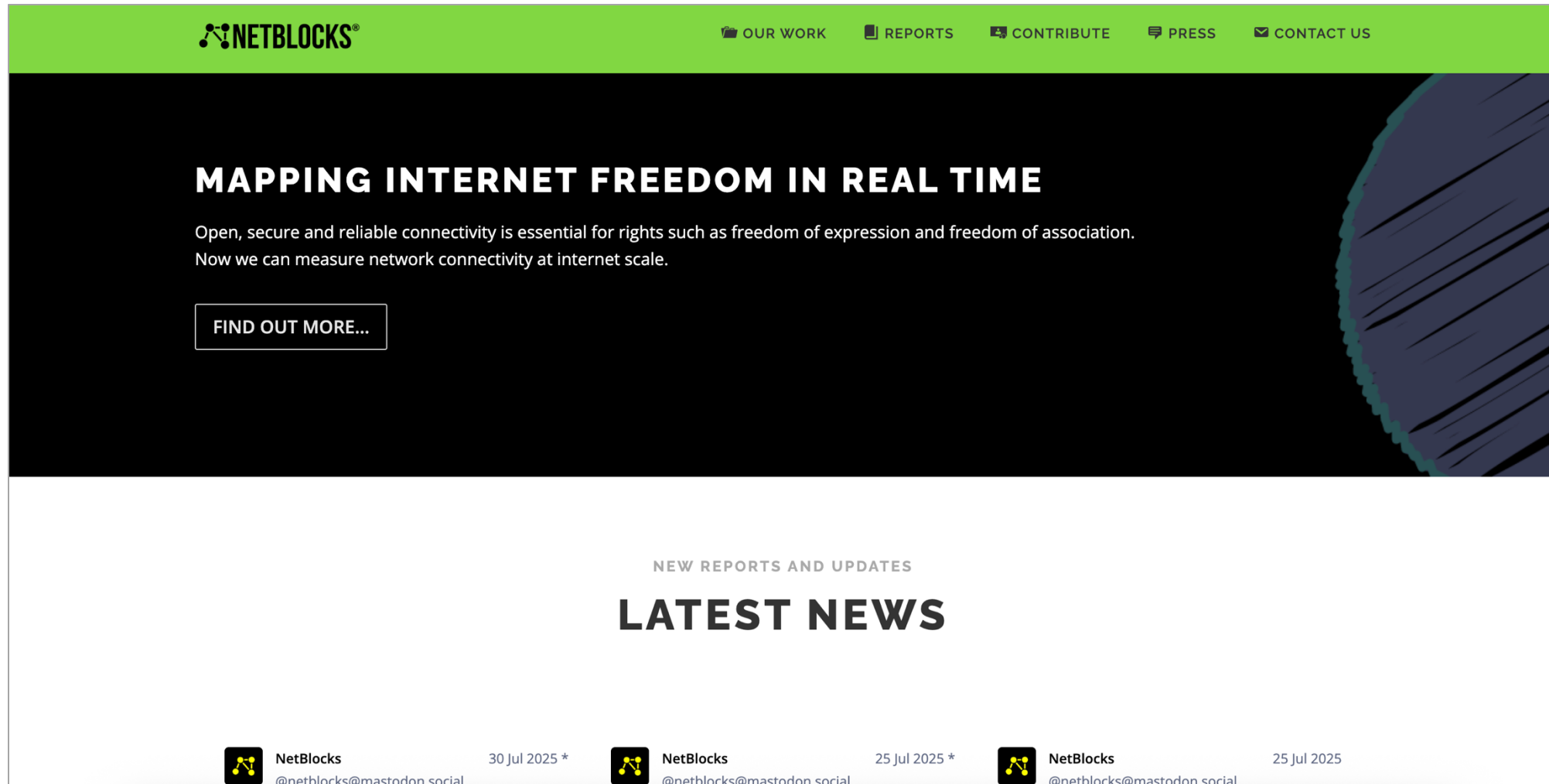
<https://horizon.netscout.com/>

國際海纜地圖

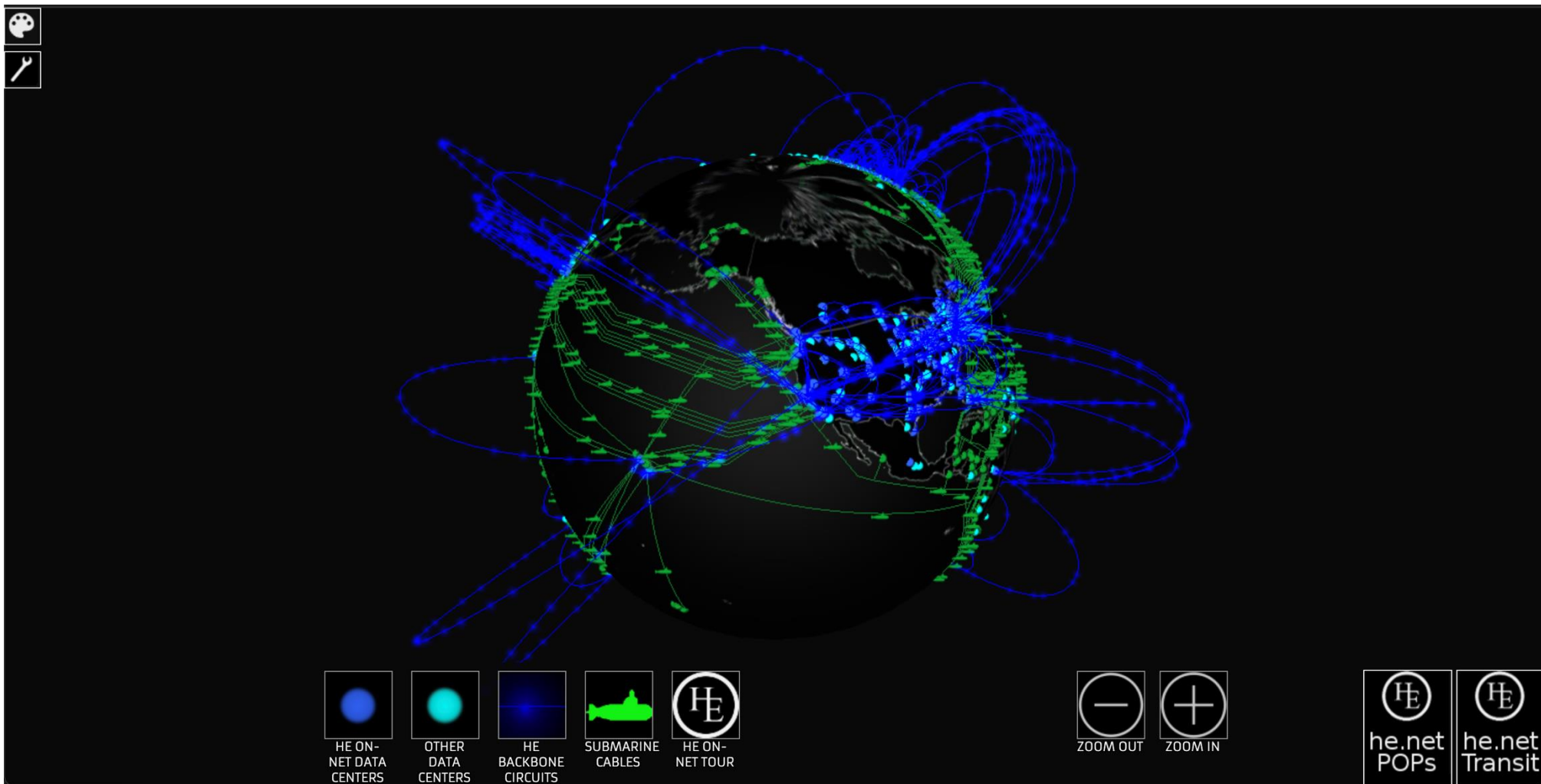


<https://www.submarinecablemap.com/>

Net Blocks



<https://netblocks.org/>



Q&A

