

DNS Sinkhole & RPZ

運作原理與實際應用

台大計中網路組
游子興

davisyou@ntu.edu.tw

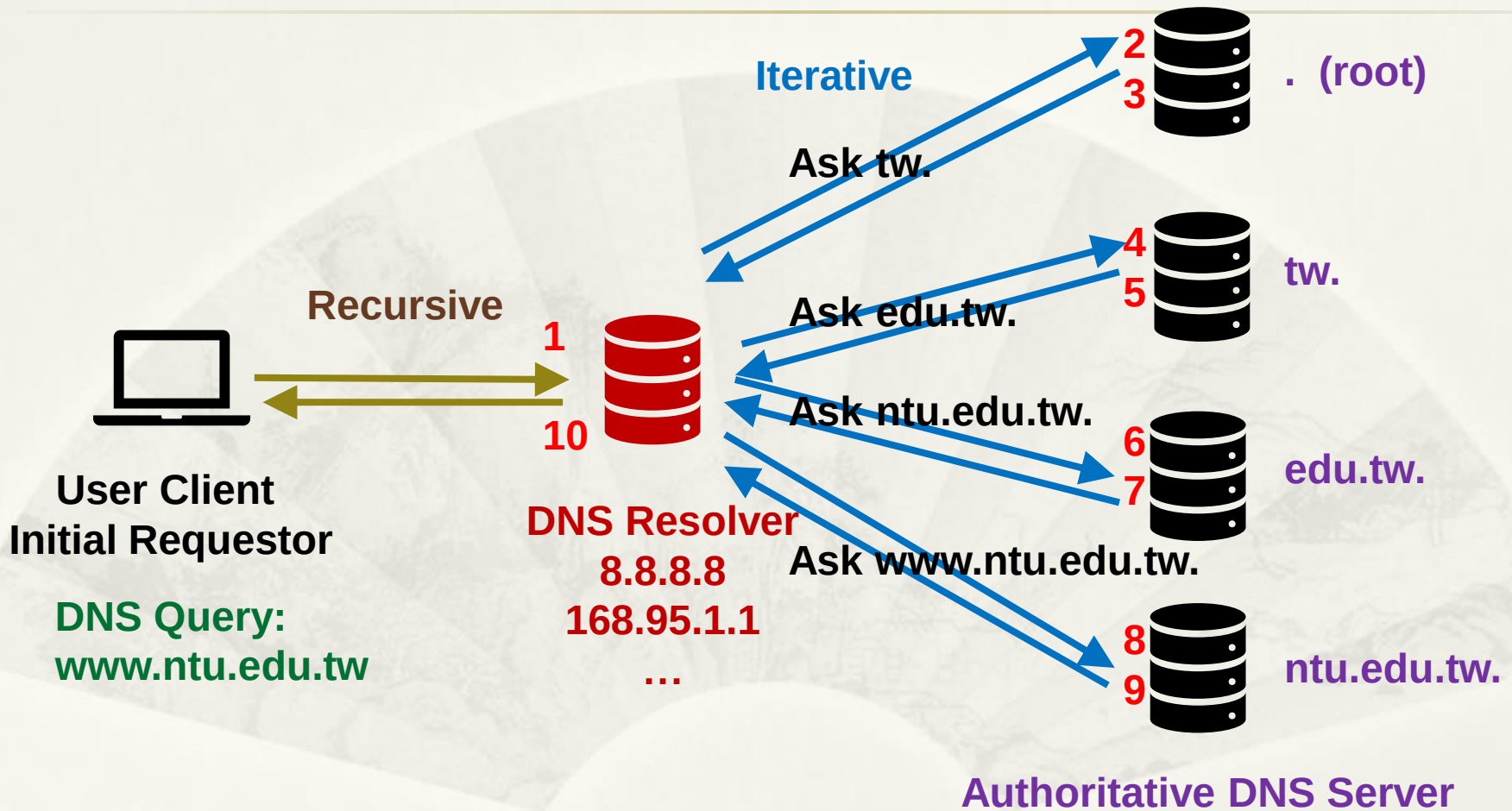
02-33665008

大綱

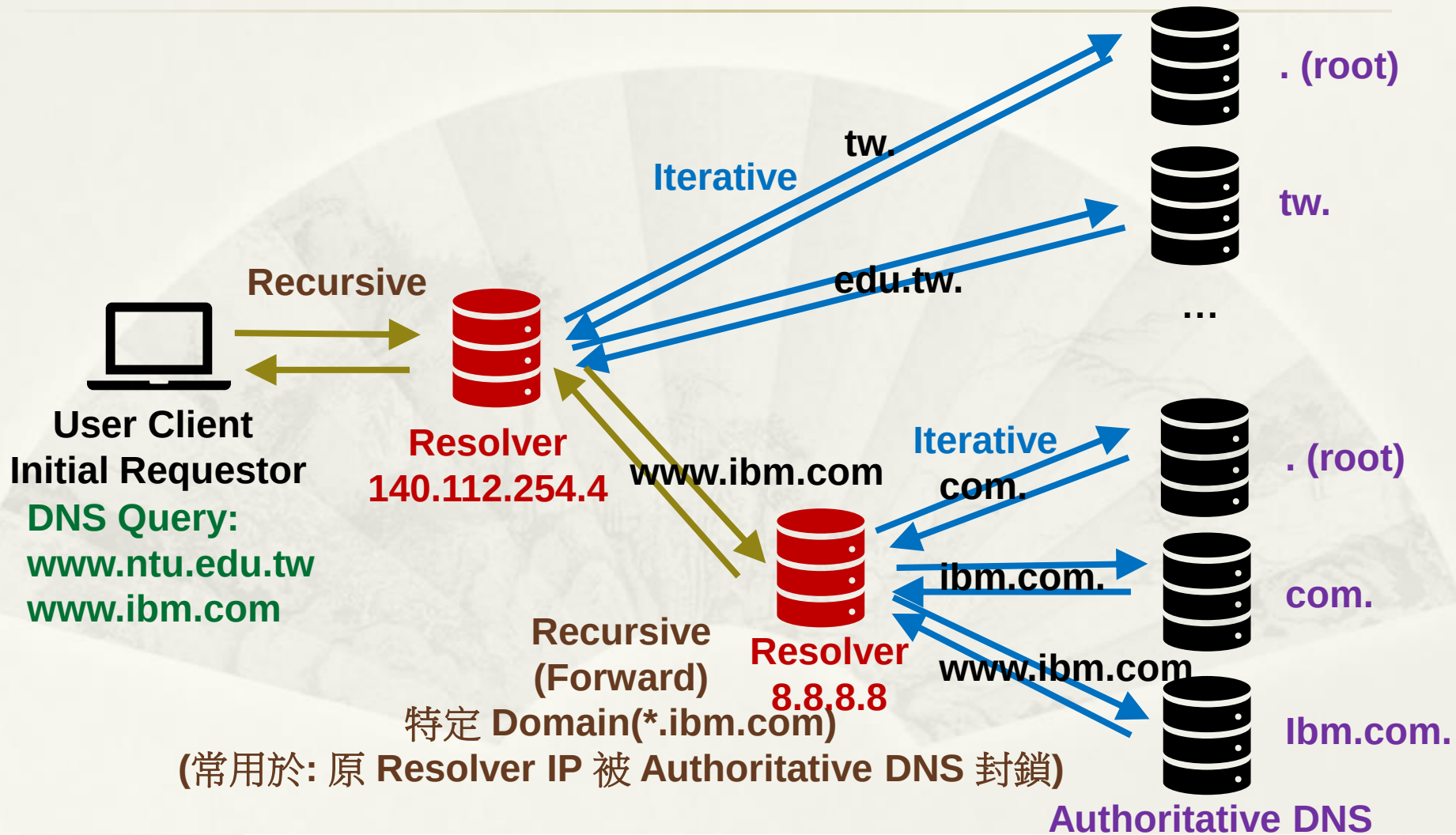
- * DNS 架構與運作原理
- * DNS Sinkhole
- * DNS RPZ

DNS 運作架構

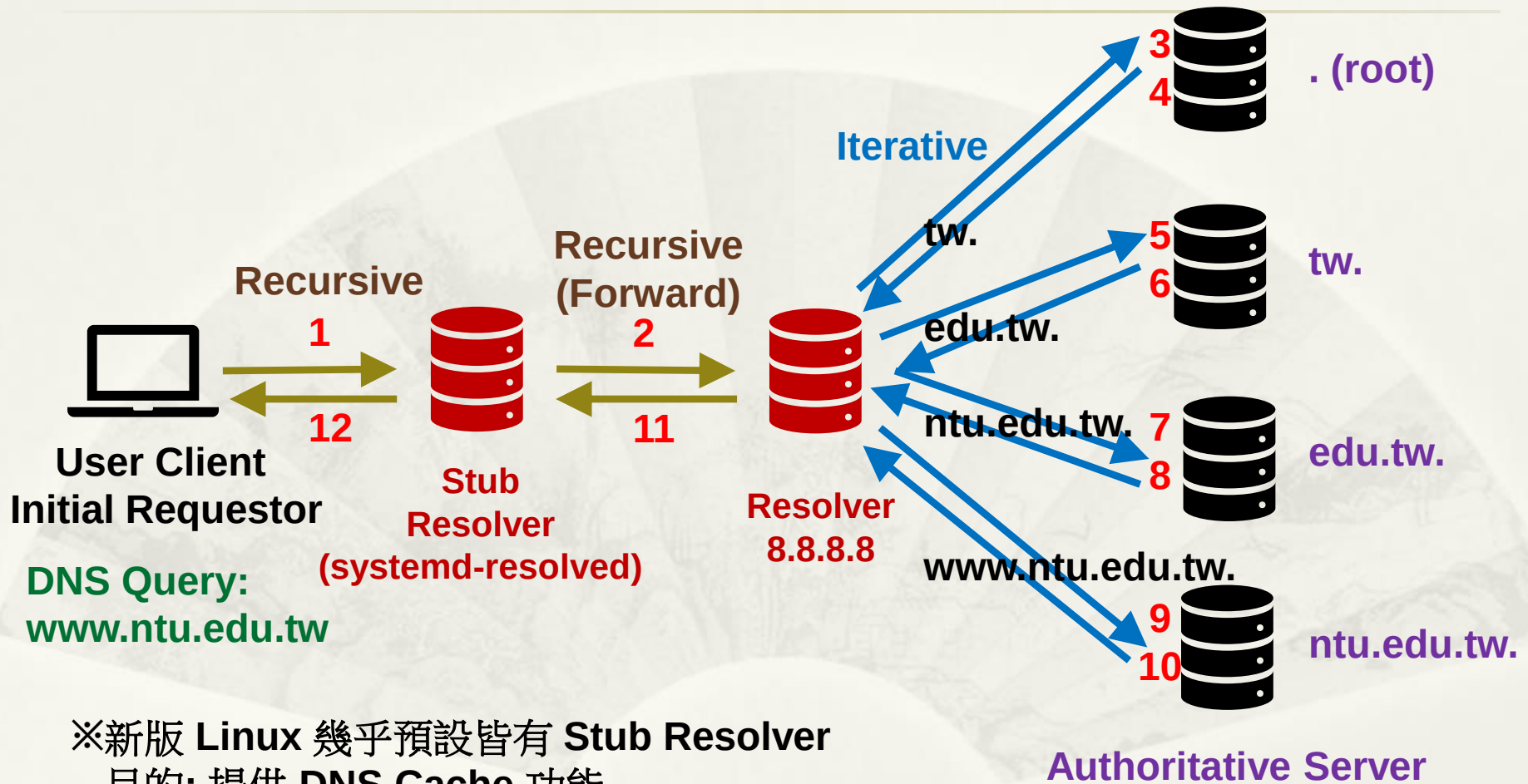
DNS 運作架構



Partial Forward



Stub Resolver (All Forward)



※新版 Linux 幾乎預設皆有 Stub Resolver
目的: 提供 DNS Cache 功能

DNS Sinkhole

大綱

- * 事前阻擋: DNS Sinkhole
 - * DNS Authoritative Server: 正解 and 反解
 - * 資安設備阻擋 or Redirect
 - * Local Hosts File
 - * DNS Resolver: DNS RPZ
- * 事後分析
 - * 資安情資資料庫

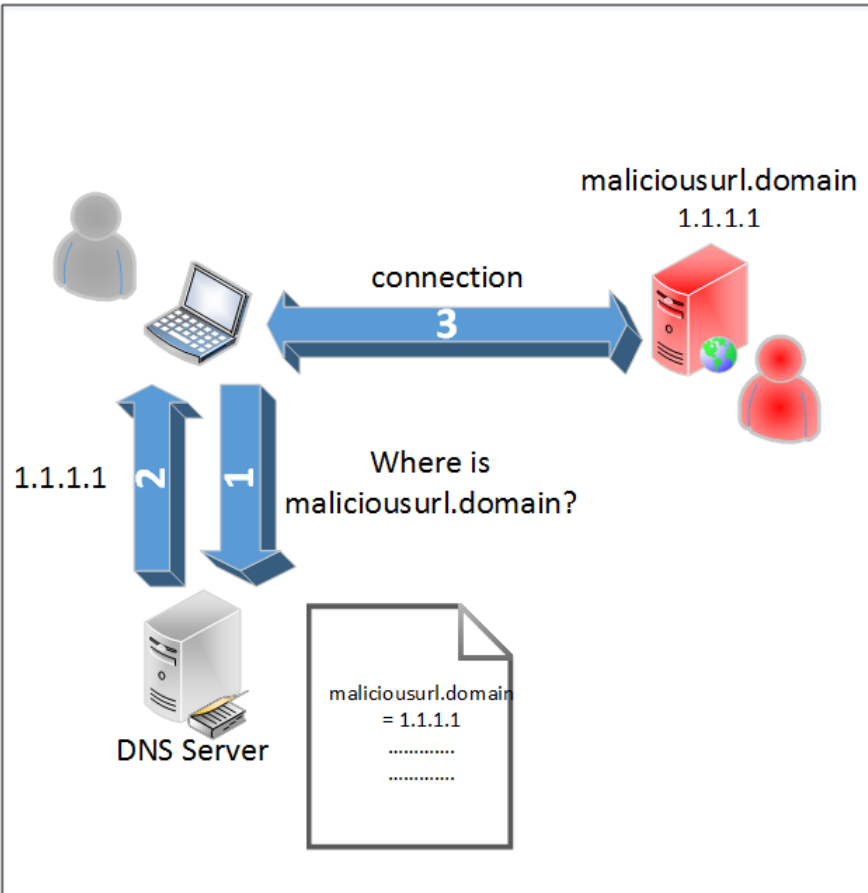
事前阻擋 vs. 事後分析

- * 事前阻擋: DNS Sinkhole
- * 事後分析: 分析 DNS Query Log 是否出現於 DNS 黑名單

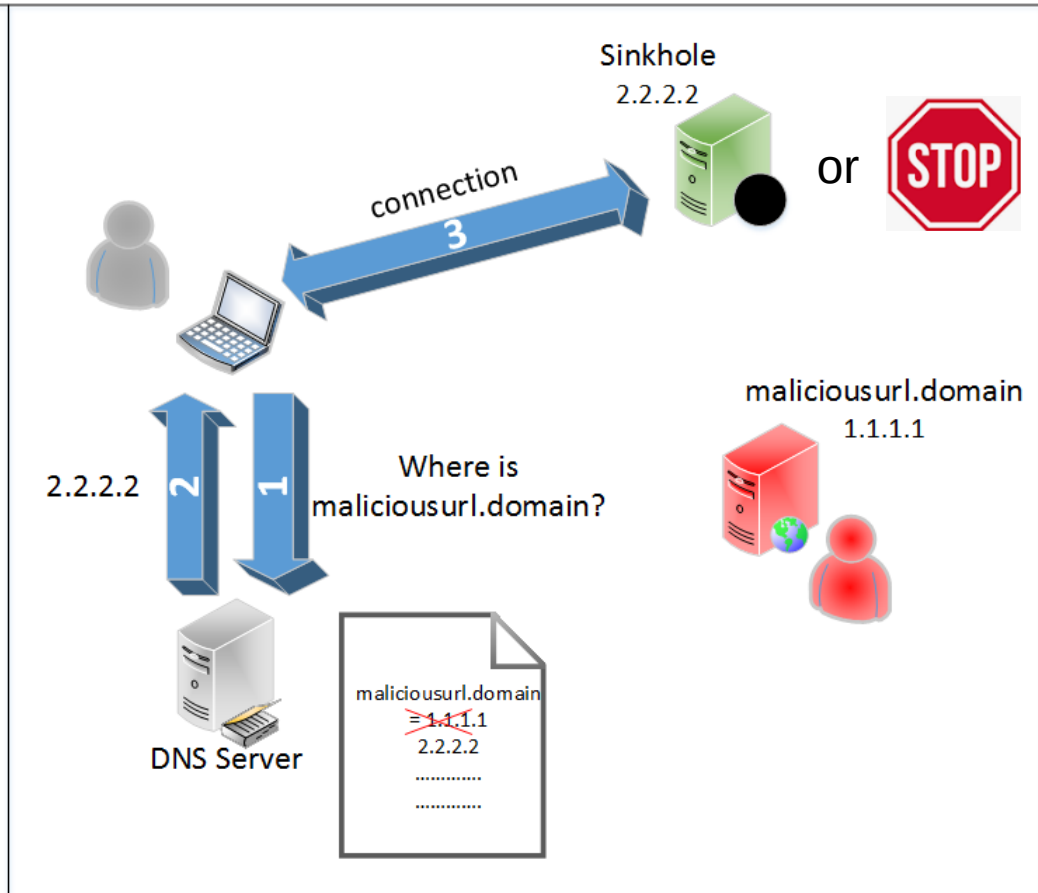
DNS Sinkhole

運作方式

W/O Sinkhole



Sinkhole



DNS Sinkhole

- * Protect users by intercepting DNS request attempting to connect to known malicious domains.
- * 目的: Return NXDOMAIN or False IP
- * 作法:
 - * DNS Authoritative Server: 正解 and 反解
 - * 資安設備阻擋 or Redirect
 - * Local Hosts File
 - Linux: /etc/hosts
 - Windows: C:\Windows\System32\drivers\etc\hosts
 - * DNS Resolver: DNS Firewalls、DNS RPZ

DNS Sinkhole use DNS Authoritative Server

方法 1

DNS Authoritative Server

- * 前提: Botnets have been compromised by Up-level domain.
- * 案例1: 2022年4月7日
 - * 微軟接管了駭客 Fancy Bear（亦稱 APT28、Strontium）用以攻擊烏克蘭的7個網域，並將流量導向微軟控制的 Sinkhole
 - * 此駭客組織在烏克蘭戰爭中，曾鎖定烏克蘭入口網站 Ukr.net 用戶下手，發動網釣攻擊。
 - * Ref. <https://www.ithome.com.tw/news/150323>

DNS Authoritative Server

* 案例2: 2022年4月22日

- * 微軟成功接管 ZLoader 殭屍網路超過 400 個網域，使其暫時在網絡上消失。
- * ZLoader 是惡名昭彰大型殭屍網路之一，最初以金融木馬程式姿態出現，後來逐漸擴充成惡意軟體即服務供應商，與 Ryuk、DarkSide 和 BlackMatter 等勒索軟體分享網路，受害者遍布全球。
- * Ref.
<https://technews.tw/2022/04/22/microsoft-successfully-takes-over-zloader-botnet/>

DNS Authoritative Server

- * 案例3: <https://avcheck.net/>



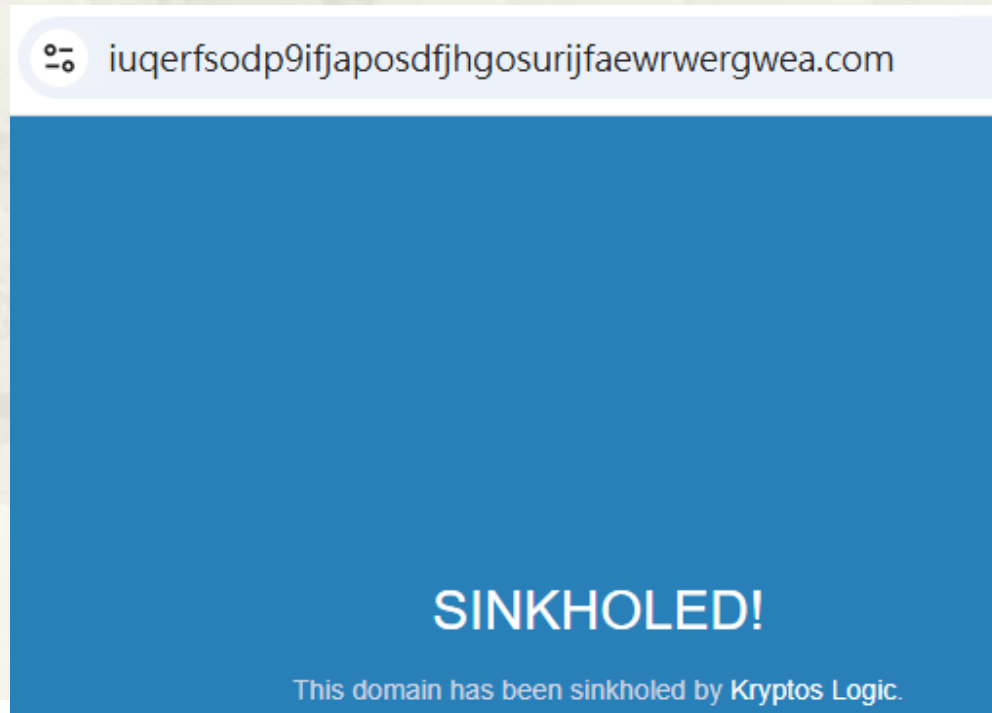
- * 2025-06-02 國際警方關閉被駭客用來對抗防毒軟體的 AVCheck
 - * Ref. <https://www.ithome.com.tw/news/169290>

如何知道網址已經是 DNS Sinkhole ? (Identify Compromised Hosts)

- * 方法1 : Domain 正解
 - * `http://網址/` , 內容顯示 sinkholed by xxxx
- * 方法2: IP addr 反解(PTR)
 - * 出現 Sinkhole 字串

方法1 : Domain 正解

- * 內容顯示 sinkholed by xxxx
- * 案例: WannaCry 勒索病毒運作檢查網址
<https://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>
<https://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>



WannaCry 勒索病毒運作檢查網址

* <https://applealmond.com/posts/5224>

勒索病毒已停止擴散？WannaCry 2.0 更新 版釋出，威脅尚未解除

2017 年 5 月 14 日 / 多頻發送

就在昨天肆虐全台的 WannaCry 勒索病毒，被一名化名 MalwareTech 的資安研究人員發現，WannaCry 會透過一個未被註冊的網域名稱：iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 作為判斷是否擴散的依據，只要該網域不存在，病毒就會繼續擴散。因此這名研究人員把網域註冊起來，意外地阻止了 WannaCry 的擴散。

方法1 : Domain 正解

* Snort Rules 封包內容出現“sinkhole”關鍵字

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"INDICATOR-COMPROMISE Connection to malware sinkhole - CERT.PL"; flow:to_client,established; content:"Content-Length: 24|oD oA|"; http_header; content:"Sinkholed by CERT.PL<br>");
```

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"INDICATOR-COMPROMISE connection to zeus malware sinkhole"; flow:to_client,established; content:"X-Sinkhole|3A| Malware GameOverZeus sinkhole");
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"MALWARE-OTHER connection to malware sinkhole"; flow:to_client,established; isdataat:21; isdataat:!22; content:"Sinkholed by abuse.ch|oA|");
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"MALWARE-OTHER Sinkhole reply - irc-sinkhole.cert.pl"; flow:to_client,established; content:"|3A|irc|2D|sinkhole|2E|cert|2E|pl");
```

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"MALWARE-OTHER connection to malware sinkhole"; flow:to_client,established; content:"X-Sinkhole|3A| Malware");
```

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"MALWARE-OTHER connection to malware sinkhole"; flow:to_client,established; content:"malware-sinkhole|oD oA|");
```

方法2: IP addr 反解(PTR)

出現 Sinkhole 字串

- * 案例: ET TROJAN Ransom.Win32.Birele.gsg
 - * 清大資工所網路安全課程期末惡意程式分析作業
 - * <https://www.sharecourse.net/sharecourse/upload/assign/51/submit/fid72b40f5527b1f2a46eba2788115c6.pdf>
- * 惡意網址: mkkuei4dsz.com
- * DNS 正解 IP: 166.78.144.80
- * 166.78.144.80 反解(PTR):
C:\> nslookup 166.78.144.80
名稱: **so1.snkhole.mal-ware.susp-nded.domain**
Address: 166.78.144.80
- * 補充: sinkhole domain name 無正解 IP 或 無特別意義
 - * C:\Users\user>nslookup so1.snkhole.mal-ware.susp-nded.domain
 - * 找不到 so1.snkhole.mal-ware.susp-nded.domain: Non-existent domain

方法2: IP addr 反解(PTR) 出現 sinkhole 字串

- * 清大資工所網路安全課程期末惡意程式分析作業
- * 封包側錄

101	47.0964890	192.168.113.128	192.168.113.2	DNS	75 Standard query 0x340a A mkkuei4kdsz.com
102	47.3791150	192.168.113.2	192.168.113.128	DNS	91 Standard query response 0x340a A 166.78.144.80
103	47.3805360	192.168.113.128	166.78.144.80	TCP	62 interhdl-e1md > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
104	47.3809450	166.78.144.80	192.168.113.128	TCP	60 http > interhdl-e1md [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
105	47.3809470	192.168.113.128	166.78.144.80	TCP	54 interhdl-e1md > http [ACK] Seq=1 Ack=1 win=64240 Len=0
106	47.3811850	192.168.113.128	166.78.144.80	HTTP	245 GET /683/411.html HTTP/1.1
107	47.3814540	166.78.144.80	192.168.113.128	TCP	60 http > interhdl-e1md [ACK] Seq=1 Ack=192 win=64240 Len=0

- * 連線觀察 netstat

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat

Active Connections

Proto Local Address          Foreign Address         State
TCP    user-9be8d1799b:1422  s01.sinkhole.malware.suspended.domain:http ESTABLISHED
```

方法2: IP addr 反解(PTR) 出現 sinkhole 字串

* 思考:

- * 所有對外連線 IP 進行 DNS 反解後搜尋是否有 sinkhole 字串

DNS Sinkhole

資安設備阻擋 or Redirect

方法 2

資安設備阻擋

Cisco IPS

- * DNS Query 網址為已知之網域黑名單
- * Snort Rule
 - * alert **udp \$HOME_NET any -> any 53** (msg:"INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry"; flow:to_server; byte_test:1,!&,oxF8,2; content:"|29|iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea|03|com|oo"
 - * alert **udp \$EXTERNAL_NET 53 -> \$HOME_NET any** (msg:"INDICATOR-COMPROMISE DNS response points to sinkholed domain"; flow:to_client,established; content:"|oo 02 00 01|"; content:"honeybot|02|us";
 - * alert **udp \$HOME_NET any -> any 53** (msg:"MALWARE-CNC Torpig bot sinkhole server DNS lookup"; flow:to_server; byte_test:1,!&,oxF8,2; content:"torpig-sinkhole|03|org"; (待釐清)

待釐清

torpig-sinkhole.org 為 DNS Sinkhole ?

- * <https://otx.alienvault.com/indicator/domain/torpig-sinkhole.org>
- * <https://www.virustotal.com/gui/domain/torpig-sinkhole.org>
- * <https://www.virustotal.com/gui/domain/mx2.torpig-sinkhole.org>

資安設備 Redirect PaloAlto 使用 CNAME

* 案例1: nslookup dgs.ltedu.com.tw

未經授權的回答:

名稱: sinkhole.paloaltonetworks.com

Address: 72.5.65.111

Aliases: dgs.ltedu.com.tw

* PA 將該 Domain 列入 spyware 威脅類別

* 案例2: 2024isme.skyces.org

```
Non-authoritative answer:
2024isme.skyces.org      canonical name = sinkhole.paloaltonetworks.com.
Name:   sinkhole.paloaltonetworks.com
Address: 72.5.65.111
>
```

資安設備 Redirect With Secure 更改 DNS query 結果

- * 2024isme.skyces.org



- * With Secure: EDR Solution
 - * <https://www.withsecure.com/en/home>

DNS Sinkhole use Local Hosts File

方法 3

Local Hosts File

- * Steven Black

- * <https://github.com/StevenBlack/hosts>

- * 下載後直接放於 Local Hosts File

Linux: /etc/hosts

Windows: C:\Windows\System32\drivers\etc\hosts



Host file recipe	Readme	Raw hosts	Unique domains
Unified hosts = (adware + malware)	Readme	link	165,872
Unified hosts + fakenews	Readme	link	168,066
fakenews	Readme	link	2,194
Unified hosts + gambling	Readme	link	172,368
gambling	Readme	link	6,508
Unified hosts + porn	Readme	link	240,534
porn	Readme	link	75,364
Unified hosts + social	Readme	link	169,060
social	Readme	link	3,217

```
#=====
# Title: Hosts contributed by Steven Black
# http://stevenblack.com

0.0.0.0 ad-assets.futurecdn.net
0.0.0.0 ck.getcookiestxt.com
0.0.0.0 eul.clevertap-prod.com
0.0.0.0 wizhumpgyros.com
0.0.0.0 coccyxwickimp.com
0.0.0.0 webmail-who-int.000webhostapp.com
0.0.0.0 010sec.com
0.0.0.0 01mspmd5yalky8.com
0.0.0.0 0byv9mgbn0.com
0.0.0.0 ns6.0pendns.org
0.0.0.0 dns.0pengl.com
0.0.0.0 12724.xyz
0.0.0.0 21736.xyz
0.0.0.0 www.analytics.247sports.com
0.0.0.0 2no.co
0.0.0.0 www.2no.co
0.0.0.0 logitechlogitechglobal.112.2o7.net
```



事後分析

事後分析

- * 分析 DNS Query Log 是否出現於DNS 黑名單
- * 資安情資資料庫
 - * Open Threat Intelligence Community
 - * <https://otx.alienvault.com/>

如何知道某網址已經是 DNS Sinkhole ?

* 範例: Domain Name (FQDN)

* **iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com**

* <https://otx.alienvault.com/indicator/domain/iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>

DOMAIN

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 

Add to Pulse 

Pulses	Passive DNS	URLs	Files
5	57	0	0

Analysis Overview

Verdict	Malicious	Indicator Facts	OTX telemetry in last 7 days DGA domain
IP Address	104.16.173.80, 104.17.244.81		4 malicious files communicating
Location	 United States		Related URLs found in Alien Labs pulses
ASN	AS13335 cloudflare		Historical OTX telemetry Open directory
Nameservers	ns1.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, ns2.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. More		Running webserver 12 subdomains
WHOIS	Registrar: NAMECHEAP INC, Creation Date: May 12, 2017	Antivirus Detections	Backdoor:Win32/Fynloski.PA!MTB, Worm:Win32/Mofksys.R!MTB
Related Pulses	Alien Labs Pulses (1), OTX User-Created Pulses (4)	AV Detection Ratio	4 / 6
		Certificate Issuer	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc ECC CA-3
		Certificate Subject	CN=api.cloudflare.com



如何知道某網址已經是 DNS Sinkhole ?

* 範例: Domain Name (FQDN)

* **torpig-sinkhole.org**

* <https://otx.alienvault.com/indicator/domain/torpig-sinkhole.org>

The screenshot shows the AlienVault OTX interface for the domain **torpig-sinkhole.org**. At the top, it displays the domain name and an "Add to Pulse" button. Below this, a summary row shows: 1 Pulse, 199 Passive DNS records, 0 URLs, and 0 Files. The "Analysis Overview" section is divided into two columns. The left column lists details: Verdict (Sinkhole), IP Address (87.106.18.122), Location (Germany), ASN (AS8560 1&1 Internet AG), Nameservers (ns2.torpig-sinkhole.org, ns1.torpig-sinkhole.org), WHOIS (Registrar: 1 & 1 Internet AG, Creation Date: Feb 19, 2009), Related Pulses (OTX User-Created Pulses (1)), and Related Tags (8 tags including malware, info, pups, phishing sites, am cst). The right column, "Indicator Facts", lists: DGA domain, Domain is a sinkhole, Domain is sinkholed, Blocked by Quad9, Historical OTX telemetry, Running webserver, 59 subdomains, Domain has its own nameserver, Certificate Issuer (SELF-ISSUED), Certificate Subject (CN=localhost), and External Resources (Whois, UrlVoid, VirusTotal).

DOMAIN	
torpig-sinkhole.org	
Pulses	1
Passive DNS	199
URLs	0
Files	0
Analysis Overview	
Verdict	Sinkhole
IP Address	87.106.18.122
Location	Germany
ASN	AS8560 1&1 Internet AG
Nameservers	ns2.torpig-sinkhole.org, ns1.torpig-sinkhole.org
WHOIS	Registrar: 1 & 1 Internet AG, Creation Date: Feb 19, 2009
Related Pulses	OTX User-Created Pulses (1)
Related Tags	8 Related Tags: malware, info, pups, phishing sites, am cst More
Indicator Facts	DGA domain, Domain is a sinkhole, Domain is sinkholed, Blocked by Quad9, Historical OTX telemetry, Running webserver, 59 subdomains, Domain has its own nameserver
Certificate Issuer	SELF-ISSUED
Certificate Subject	CN=localhost
External Resources	Whois , UrlVoid , VirusTotal

如何知道某網址已經是 DNS Sinkhole ?

- * 範例: Domain Name (FQDN)
 - * **honeybot.us**
 - * <https://otx.alienvault.com/indicator/domain/honeybot.us>

DOMAIN

honeybot.us

Add to Pulse +

Pulses	Passive DNS	URLs	Files
0	57	0	0

Analysis Overview

Verdict	Suspicious	Indicator Facts	Blocked by Quad9	Historical OTX telemetry
IP Address	208.100.26.234		Running webserver	3 subdomains
Location	United States	Certificate Issuer	C=US, O=Let's Encrypt, CN=R3	
ASN	AS32748 steadfast	Certificate Subject	CN=mmmmm.pw	
Nameservers	dns1.registrar-servers.com, dns2.registrar-servers.com.	External Resources	Whois, UrlVoid, VirusTotal	
WHOIS	Registrar: NAMECHEAP, INC., Creation Date: Oct 1, 2015			
Related Pulses	None			



如何知道 IP 已經是 DNS Sinkhole ?

* 範例: IP

* 166.78.144.80

* <https://otx.alienvault.com/indicator/ip/166.78.144.80>

The screenshot displays the AlienVault OTX interface for the IP indicator 166.78.144.80. At the top, the IP is shown with a copy icon and an 'Add to Pulse' button. Below this, four large statistics are presented: 1, 500+, 7, and 0. The main section is titled 'Analysis Overview' and is divided into two columns. The left column lists various attributes such as Verdict (Sinkhole), Classification (Datacenter / Hosting / VPS), Reverse DNS (s01.snkhole.mal-ware.susp-nded.domain), Location (United States of America), ASN (AS33070 rackspace hosting), DNS Resolutions (500+ Domains), Top Level Domains (22 Unique TLDs), Related Pulses (OTX User-Created Pulses (1)), and Related Tags (Nextray, cyber security, loc, phishing, malicious). The right column, titled 'Indicator Facts', highlights that it is a 'Sinkhole address' with 'Historical OTX telemetry', including 6 dynamic DNS domains, 1 domain resolved in the last 7 days, 1 domain resolved in the last 30 days, 500+ domains resolved in all time, and 22 top-level domains. Below this, 'External Resources' like Whois and VirusTotal are listed.

Analysis Overview	
Verdict	Sinkhole
Classification	Datacenter / Hosting / VPS
Reverse DNS	s01.snkhole.mal-ware.susp-nded.domain
Location	United States of America
ASN	AS33070 rackspace hosting
DNS Resolutions	500+ Domains
Top Level Domains	22 Unique TLDs
Related Pulses	OTX User-Created Pulses (1)
Related Tags	5 Related Tags Nextray, cyber security, loc, phishing, malicious

Indicator Facts	
Sinkhole address	Historical OTX telemetry
6 dynamic DNS domains	
1 domains resolved in last 7 days	
1 domains resolved in last 30 days	
500+ domains resolved in all time	
22 top-level domains	

External Resources	
Whois , VirusTotal	

DNS Sinkhole use DNS Resolver (DNS Firewalls 、 DNS RPZ)

大綱

- * 傳統 DNS Sinkhole 作法
- * 回應政策區域 Response Policy Zone (RPZ)
- * RPZ 現有聯防案例
- * RPZ 語法介紹
- * RPZ 是否與 DNSSEC 衝突?
- * RPZ Redirect to 警告頁面受 HSTS 限制

傳統 DNS Sinkhole 作法

不支援 RPZ 之替代方法

傳統 DNS Sinkhole 作法 (不支援 RPZ 之替代方法)

- * 直接將惡意 FQDN 建立單獨的 Zone，並共用一個 Zone File.

- * BIND

- * named.conf

```
zone "onedrive.hayraet.com" IN { type master; file "redirect.nowhere"; };  
zone "cathaylife.garfeas.com" IN { type master; file "redirect.nowhere"; };  
zone "ntu-web.weebly.com." IN { type master; file "redirect.nowhere"; };  
zone "eud.tw." IN { type master; file "redirect.nowhere"; };
```

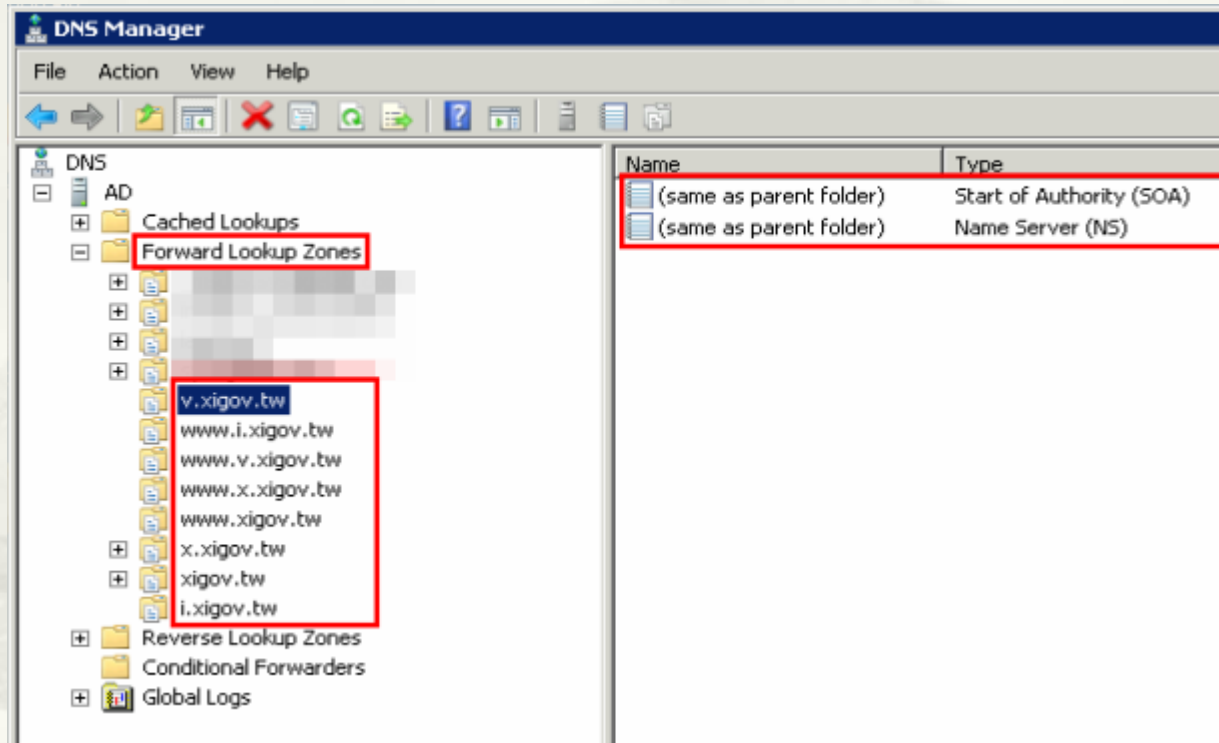
....

- * Zone File: redirect.nowhere

```
@ 1D IN SOA  localhost root ( 20210830 3H 15M 1W 1D )  
1D IN NS   @  
5  IN A    192.168.1.1
```

Windows DNS 黑名單

- * 直接將惡意 FQDN 建立單獨的 Zone

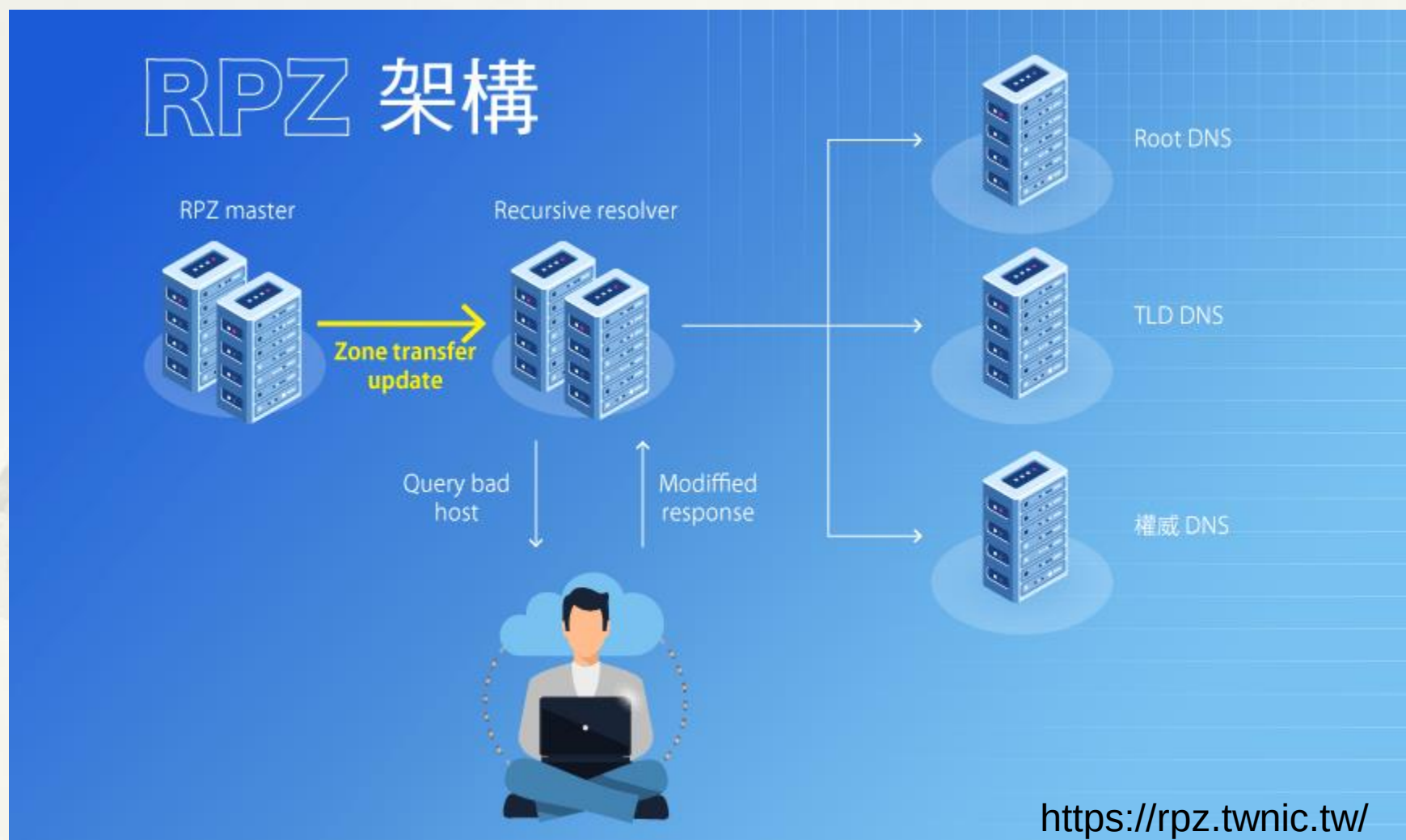


- * Ref. https://hackmd.io/@farmer87/infoblox_local_rpz_rules



回應政策區域 Response Policy Zone (RPZ)

RPZ 架構



RPZ

- * 回應政策區域 (Response Policy Zone, RPZ)
 - * DNS Resolver 提供的功能，也可稱為DNS防火牆
- * Support
 - * BIND v9.8+ support up to 64 Response Policy Zones
 - * <https://bind9.readthedocs.io/en/latest/chapter6.html#dns-firewalls-and-response-policy-zones>
 - * Unbound
 - * <https://unbound.docs.nlnetlabs.nl/en/latest/topics/filtering/rpz.html>
 - * PowerDNS Recursor v4+
- * Not Support
 - * Windows DNS Server

RPZ 之限制與使用疑慮

- * 使用類似 DNS Spoof 方式變更原查詢結果
 - * 破壞 DNSSEC Chain of Trust 信任架構
 - * 無法提供合法 HTTPS 憑證，Redirect to 警告頁面會顯示不安全
 - * 若原網站有啟用 HSTS 限制，將無法 Redirect to 警告頁面
- * 使用 Zone Transfer 方式傳輸 RPZ Zone File
 - * 雙方未認證且使用明碼傳輸，可能遭受 Man-in-the-Middle 中間人攻擊。
 - * 來源 Primary DNS Server 若遭駭客攻陷，可能派送惡意資料，將正常網站導向駭客網站。
- * 約 20% 連線單位使用 Windows DNS Server，但不支援 RPZ.



教育體系

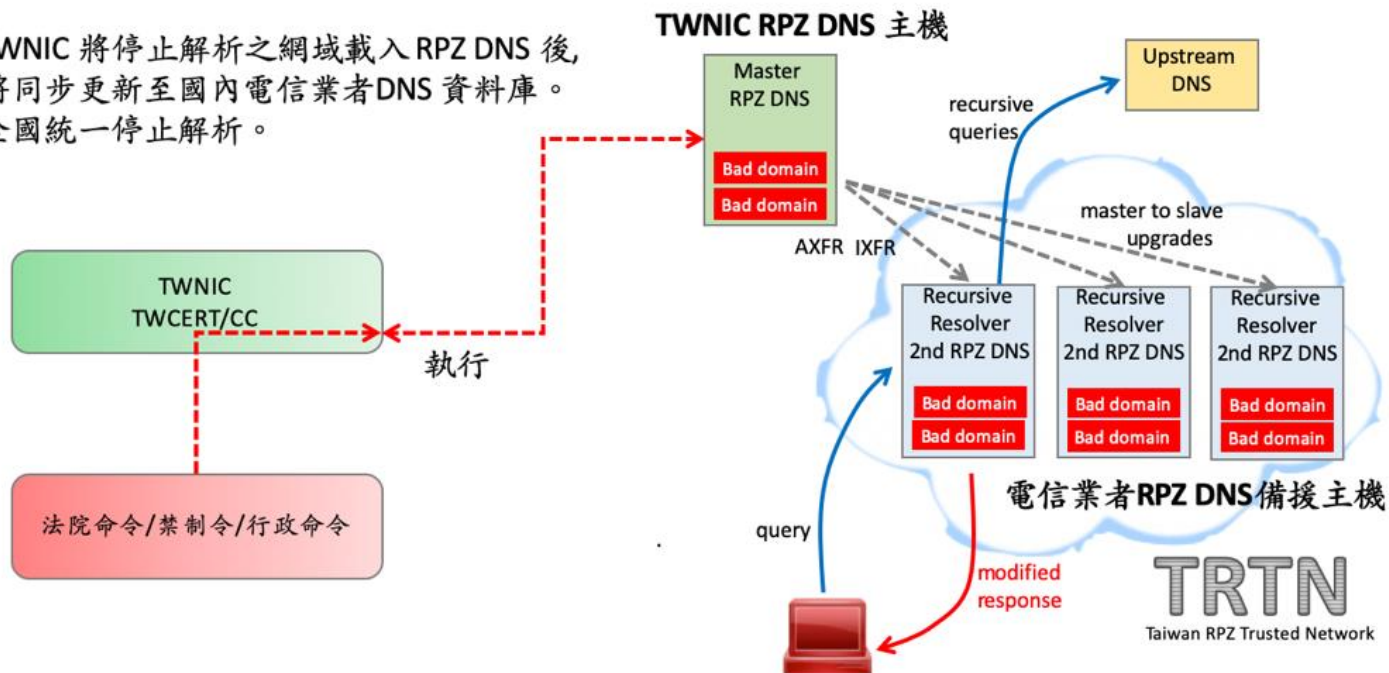
現有 RPZ 聯防案例

TWNIC RPZ

- * <https://rpz.twnic.tw/>
- * 使用方式: DNS Zone Transfer
- * 缺點: 加入單位, 會收到許多 RPZ 清單異動公文

國家型 DNS RPZ 架構

TWNIC 將停止解析之網域載入 RPZ DNS 後, 將同步更新至國內電信業者 DNS 資料庫。全國統一停止解析。



TWNIC RPZ 清單案例

rpztw. 300 IN SOA localhost. This.is.an.infringing.website.rpztw. 1740707761 60 60 86400 60

rpztw. 300 IN NS localhost.

tw21.joom.ac.rpztw. 300 IN A 34.102.218.71

*.tw21.joom.ac.rpztw. 300 IN A 34.102.218.71

tw22.joom.ac.rpztw. 300 IN A 34.102.218.71

*.tw22.joom.ac.rpztw. 300 IN A 34.102.218.71

tw23.joom.ac.rpztw. 300 IN A 34.102.218.71

*.tw23.joom.ac.rpztw. 300 IN A 34.102.218.71

....

資安院 RPZ

- * 使用方式

- * 使用 Web URL 搭配 Token ID 下載
- * https://ironcloak.nics.nat.gov.tw/api/get_linux_blacklist_dn/<Token-ID>

- * 缺點

- * 需自行設定 Cron Job 才能自動下載 RPZ Zone File

- * Zone File 案例

\$TTL 30

@ SOA rpz.nics.nat.gov.tw. hostmaster.nics.nat.gov.tw. 2024091815 300 1800 604800 30
NS localhost.

360photo.oss-cn-hongkong.aliyuncs.com CNAME .
ab27.ciscosrv.com CNAME .
administrators.ga CNAME .
adobe-flash-player.live CNAME .
amazon.panasocin.com CNAME .
ap21.ilvsmail.com CNAME .
ap97.cksogo.com CNAME .

...

教育部 RPZ BIND Config

```
options {  
  response-policy {  
    zone "rpztw";  
    zone "rpzmoe";  
  };  
};  
zone "rpztw" {  
  type slave;  
  file "rpztw";  
  masters {  
    140.111.12.87;  
  };  
  allow-query {  
    localhost;  
  };  
};
```

```
zone "rpzmoe" {  
  type slave;  
  file "rpzmoe";  
  masters {  
    140.111.12.87;  
  };  
  allow-query {  
    localhost;  
  };  
};
```

Zone File: rpztw

rpztw. 300 IN SOA localhost. This.is.an.infringing.website.rpztw. 1746667741 60 60 86400 60
rpztw. 300 IN NS localhost.

twai1.joom.ac.rpztw.	300	IN	A	34.102.218.71
*.twai1.joom.ac.rpztw.	300	IN	A	34.102.218.71
twshop15.joom.ac.rpztw.	300	IN	A	34.102.218.71
*.twshop15.joom.ac.rpztw.	300	IN	A	34.102.218.71
twshop26.joom.ac.rpztw.	300	IN	A	34.102.218.71
*.twshop26.joom.ac.rpztw.	300	IN	A	34.102.218.71
twshop28.joom.ac.rpztw.	300	IN	A	34.102.218.71
*.twshop28.joom.ac.rpztw.	300	IN	A	34.102.218.71
twshop39.joom.ac.rpztw.	300	IN	A	34.102.218.71
*.twshop39.joom.ac.rpztw.	300	IN	A	34.102.218.71
twshop45.joom.ac.rpztw.	300	IN	A	34.102.218.71
*.twshop45.joom.ac.rpztw.	300	IN	A	34.102.218.71
twshop5.joom.ac.rpztw.	300	IN	A	34.102.218.71
*.twshop5.joom.ac.rpztw.	300	IN	A	34.102.218.71
okex.ac.rpztw.	300	IN	A	182.173.0.181
*.okex.ac.rpztw.	300	IN	A	182.173.0.181

....

www.methe.shop.rpztw.	300	IN	A	34.102.218.71
-----------------------	-----	----	---	---------------

....

Zone File: rpzmoe

rpzmoe. 300 IN SOA localhost. root.localhost. 2025031001 3600 900 604800 3600

rpzmoe. 300 IN NS localhost.

testrpzblock.edu.tw.rpzmoe. 300 IN CNAME .

Convert Zone File Format

- * raw to text

~# named-compilezone -f raw -F text -o
example.com.text example.com example.com.raw

- * text to raw

~# named-compilezone -f text -F raw -o
example.com.raw example.com example.com.text

教育部 RPZ

- * Zone Transfer

- ~# dig axfr rpztw @140.111.12.87

- ~# dig axfr rpzmoe @140.111.12.87

- * 人工網頁下載(待更新)

- * <https://noc.tanet.edu.tw/index.php/download/ip/1435-4>

黑名單測試

www.methe.shop

```
C:\Users\user>nslookup
預設伺服器: dns.google
Address: 8.8.8.8

> www.methe.shop
伺服器: dns.google
Address: 8.8.8.8

未經授權的回答:
名稱: methe.shop
Address: 20.239.70.103 原始記錄
Aliases: www.methe.shop

> server 140.112.254.65
預設伺服器: ccdns1.cc.ntu.edu.tw
Address: 140.112.254.65

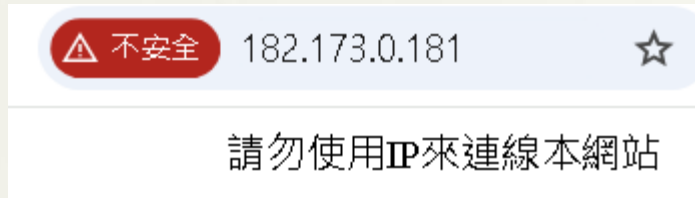
> www.methe.shop
伺服器: ccdns1.cc.ntu.edu.tw
Address: 140.112.254.65

未經授權的回答:
名稱: www.methe.shop
Address: 34.102.218.71 RPZ 記錄
```

Redirect to 警告頁面



Redirect to 警告頁面



Redirect to 警告頁面





RPZ 語法介紹

7 Types of Actions

- * Redirect to specific IP or Domain with a warning page.
 - * A 192.168.10.100
 - * CNAME www.drop.com
- * CNAME .
 - * Return NXDOMAIN
- * CNAME *.
 - * Return NODATA (empty NOERROR)
- * CNAME *.badrpz.com.
 - * Redirect to prepend subdomain
- * CNAME rpz-passthru.
 - * PASSTHRU RPZ(跳過 RPZ 檢查)
- * CNAME rpz-drop.
 - * DROP Action
- * CNAME rpz-tcp-only.
 - * Change to use TCP that require DNS client to responses with TCP.

NXDOMAIN vs. NODATA(empty NOERROR)

* NXDOMAIN

- * dig xyz.google.com @8.8.8.8

- * dig xyz.edu.com @8.8.8.8

```
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 37586
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;; udp: 512
;; QUESTION SECTION:
;xyz.edu.com.                IN      A

;; AUTHORITY SECTION:
edu.com.                     600     IN      SOA     ns37.domaincontrol.com.
```

* NODATA(empty NOERROR)

- * dig xyz.ibm.com @8.8.8.8

- * dig xyz.apple.com @8.8.8.8

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9534
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;; udp: 512
;; QUESTION SECTION:
;xyz.apple.com.             IN      A

;; AUTHORITY SECTION:
apple.com.                  300     IN      SOA     ns-ext-prod.jackfruit.apple.com.
```

CNAME rpz-tcp-only.

* dig tcp.tesla.com @127.0.0.1

```
root@ubuntu24-BIND:~# dig tcp.tesla.com @127.0.0.1
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> tcp.tesla.com @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31525
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5f8653de62fd2e400100000068216391dbf6142b5ce3a7fb (good)
;; QUESTION SECTION:
;tcp.tesla.com.                IN      A

;; AUTHORITY SECTION:
tesla.com.                    10800   IN      SOA     edns69.ultradns.com. noc.

;; Query time: 331 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (TCP)
;; WHEN: Mon May 12 10:57:21 CST 2025
;; MSG SIZE  rcvd: 144
```

CNAME *.badrpz.com.

* dig prepend.tesla.com @127.0.0.1

```
root@ubuntu24-BIND:~# dig prepend.tesla.com @127.0.0.1

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> prepend.tesla.com @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57880
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;; udp: 1232
;; COOKIE: b03185a46c53c7c901000000682164a32a0317069a100093 (good)
;; QUESTION SECTION:
;prepend.tesla.com.                IN      A

;; ANSWER SECTION:
prepend.tesla.com.                5       IN      CNAME   prepend.tesla.com.badrpz.com.
prepend.tesla.com.badrpz.com.    1800    IN      A       192.168.10.10

;; ADDITIONAL SECTION:
my.rpz.                          1800    IN      SOA     localhost. root.localhost. 100 86400 7200 604800 3600
```

CNAME rpz-passthru. CNAME rpz-drop.

* dig passthru.tesla.com @127.0.0.1

```
root@ubuntu24-BIND:~# dig passthru.tesla.com @127.0.0.1

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> passthru.tesla.com @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 13155
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 8d1629f3997e6a67010000006821656aa32b94ccf562621b (good)
;; QUESTION SECTION:
;passthru.tesla.com.                IN      A

;; AUTHORITY SECTION:
tesla.com.                10800   IN      SOA     edns69.ultradns.com. noc.teslamotors.com.
```

* dig drop.tesla.com @127.0.0.1

```
root@ubuntu24-BIND:~# dig drop.tesla.com @127.0.0.1
;; communications error to 127.0.0.1#53: timed out
;; communications error to 127.0.0.1#53: timed out
;; communications error to 127.0.0.1#53: timed out
```

5 Types of Trigger

- * Query name

www.tesla.com.my.rpz. A 1.1.1.1

web.tesla.com A 1.1.1.1 ; .my.rpz. 可省略

*.apple.com A 1.1.1.1

wildcard 作用於目前 domain, sub-domain, sub-sub-domain, ..., 但仍以 specific RR 記錄優先.

- * Authoritative DNS Server IP

32.1.11.117.140.rpz-nsip CNAME .

* IP 140.117.11.1/32

24.0.11.117.140.rpz-nsip CNAME .

* IP 140.117.11.0/24

- * FQDN of Authoritative DNS Server

nsbackup.ntut.edu.tw.rpz-nsdname CNAME .

*.ntut.edu.tw.rpz-nsdname CNAME .

- * User Client IP

8.0.0.0.10.rpz-client-ip CNAME .

* IP 10.0.0.0/8

- * DNS Answer: A record(IP addr)

32.102.8.112.140.rpz-ip CNAME .

Authoritative DNS Server IP

- * 需先查詢 NS 記錄
- * ~# dig ns nsysu.edu.tw

```
;; ANSWER SECTION:
nsysu.edu.tw.      300      IN       NS       dns.nsysu.edu.tw.
nsysu.edu.tw.      300      IN       NS       dns2.nsysu.edu.tw.

;; ADDITIONAL SECTION:
dns.nsysu.edu.tw.  300      IN       A        140.117.11.1
dns2.nsysu.edu.tw. 300      IN       A        140.117.11.11
dns.nsysu.edu.tw.  300      IN       AAAA     2001:288:8001:11::11
```

32.1.11.117.140.rpz-nsip CNAME .

32.11.11.117.140.rpz-nsip CNAME .

or

24.0.11.117.140.rpz-nsip CNAME .

FQDN of Authoritative DNS Server

- * 需先查詢 NS 記錄
- * ~# dig ns ntut.edu.tw @168.95.1.1

```
;; ANSWER SECTION:
ntut.edu.tw.        600      IN       NS       nsbackup.ntut.edu.tw.
ntut.edu.tw.        600      IN       NS       galaxy.cc.ntut.edu.tw.
```

nsbackup.ntut.edu.tw.**rpz-nsdname** CNAME .

galaxy.cc.ntut.edu.tw.**rpz-nsdname** CNAME .

or

*.ntut.edu.tw.rpz-nsdname CNAME *.badrpz.com.

DNS Answer: A record (IP addr)

- * 阻擋 www.cc.ntu.edu.tw

- * 32.102.8.112.140.rpz-ip CNAME .

```
> www.cc.ntu.edu.tw  
伺服器: [8.8.8.8]  
Address: 8.8.8.8
```

```
未經授權的回答:  
名稱: www.cc.ntu.edu.tw  
Address: 140.112.8.102
```

- * 阻擋 www.aaa.com (有 cname)

- * 32.121.66.60.45.rpz-ip CNAME .

```
> www.aaa.com  
伺服器: [8.8.8.8]  
Address: 8.8.8.8
```

```
未經授權的回答:  
名稱: ayv797h.impervadns.net  
Address: 45.60.66.121  
Aliases: www.aaa.com
```

```
root@ubuntu24-BIND:~# dig www.aaa.com @127.0.0.1
```

```
;; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.aaa.com @127.0.0.1  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 26895  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
```

```
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; udp: 1232  
;; COOKIE: 1d808e3ca441666f01000000680b597fac0672610e389be3 (good)  
;; QUESTION SECTION:  
;www.aaa.com. IN A
```

```
;; ANSWER SECTION:  
www.aaa.com. 180 IN CNAME ayv797h.impervadns.net.
```

```
;; ADDITIONAL SECTION:  
my.rpz. 1800 IN SOA localhost. root.localhost. 100 86400 7200 604800 3600
```

RPZ 是否與 DNSSEC 衝突？

RPZ 是否與 DNSSEC 衝突？

~# dig log.twnic.net.tw @127.0.0.1

```
;; ANSWER SECTION:
log.twnic.net.tw.      5      IN      A       2.2.2.2

;; ADDITIONAL SECTION:
my.rpz.                1800   IN      SOA     localhost.
```

~# dig +dnssec log.twnic.net.tw @127.0.0.1

```
;; ANSWER SECTION:
log.twnic.net.tw.      3009   IN      A       211.72.210.212
log.twnic.net.tw.      3009   IN      RRSIG   A 8 4 3600 20250604071126 20250505071126
IaiYBl6 rEJGg+WK4cZruoXSxOISy9Bq9YcTB1IOglTum23wN+lhdcfxCfiBQMUL 8LsKp4sniWCM2pj0km3uuwQ
```

* 結果不同

RPZ 是否與 DNSSEC 衝突？

* 解決方法

~# nano /etc/bind/named.conf.options

response-policy { zone my.rpz; } **break-dnssec yes;**

~# systemctl restart bind9

~# dig +dnssec log.tw nic.net.tw @127.0.0.1

```
;; ANSWER SECTION:
log.tw nic.net.tw.      5      IN      A       2.2.2.2

;; ADDITIONAL SECTION:
my.rpz.                 1800   IN      SOA     localhost. root.localhost.
```

RPZ Redirect to 警告頁面 受 HSTS 限制

HSTS

HTTP Strict Transport Security

- * www.tp1rc.edu.tw
- * Chrome F12

Name	X	Headers	Preview	Response	Initiator	Timing
www.tp1rc.edu.tw		▼ Response Headers		☐ Raw		
		Connection		keep-alive		
		Content-Encoding		gzip		
		Content-Type		text/html		
		Date		Mon, 12 May 2025 03:41:47 GMT		
		Referrer-Policy		strict-origin		
		Server		nginx/1.24.0 (Ubuntu)		
		Strict-Transport-Security		max-age=31536000; includeSubdomains; preload		

- * 在 31536000 秒（365 天）中，需使用 HTTPS 連線，且若網頁憑證無效，不能忽略警告繼續存取網站。
- * includeSubdomains; preload -- 子域名網站也適用

HSTS

HTTP Strict Transport Security

- * 因 HSTS 限制，<https://www.tp1rc.edu.tw> 無法 Redirect to 警告頁面

⚠ 不安全 <https://www.tp1rc.edu.tw>

www.tp1rc.edu.tw 通常會使用加密方式保護你的資訊。但 Chrome 這次嘗試連線到 www.tp1rc.edu.tw 時，該網站傳回了異常且錯誤的憑證。這可能是因為有攻擊者企圖偽裝成 www.tp1rc.edu.tw，或是受到 Wi-Fi 登入畫面影響而造成連線中斷。不過請放心，Chrome 已及時停止連線，並未傳輸任何資料，因此你的資訊仍然安全無虞。

目前無法造訪 www.tp1rc.edu.tw，因為這個網站使用 HSTS。網路錯誤和攻擊行為通常是暫時性的，因此這個網頁可能稍後就會恢復正常狀態。

隱藏詳細資料

重新載入

Convert to RPZ Format

- * a command-line tool written in Go for converting a list of domain names and IP into a RPZ file format.
 - * <https://github.com/pure-dns/easyrpz>
- * 語法

```
easyrpz \  
-i inputFile1.hosts \  
-i http://example.com/inputFile2.hosts \  
-e excludeFile1.txt \  
-e http://example.com/excludeFile2.txt \  
-o outputFile.rpz
```

Ref.

- * <https://dnssrpz.info/>
- * <https://www.isc.org/rpz/>
- * <https://www.ietf.org/archive/id/draft-vixie-dnsop-dns-rpz-00.txt>
- * <https://rpz-block-list.readthedocs.io/en/latest/indexTOC.html>
- * <https://www.zytrax.com/books/dns/ch7/rpz.html>

簡報完畢
謝謝