From DNS to Inbox: Exploiting dangling DNS for malicious email

DNS-OARC 43

October 26-27, 2024

SPAMHAUS

Meet the speaker

Carel Bitter
Head of Data, Spamhaus

What we'll cover

1. What is dangling DNS?
2. Introduction to SubDoMailing?
3. A Case Study: SubDoMailing
4. What are they mailing?
5. Recommendations

1 | WHAT IS DANGLING DNS?

SPAMHAUS

What is dangling DNS?

"Misconfigured DNS records that point to non-existent or expired services."

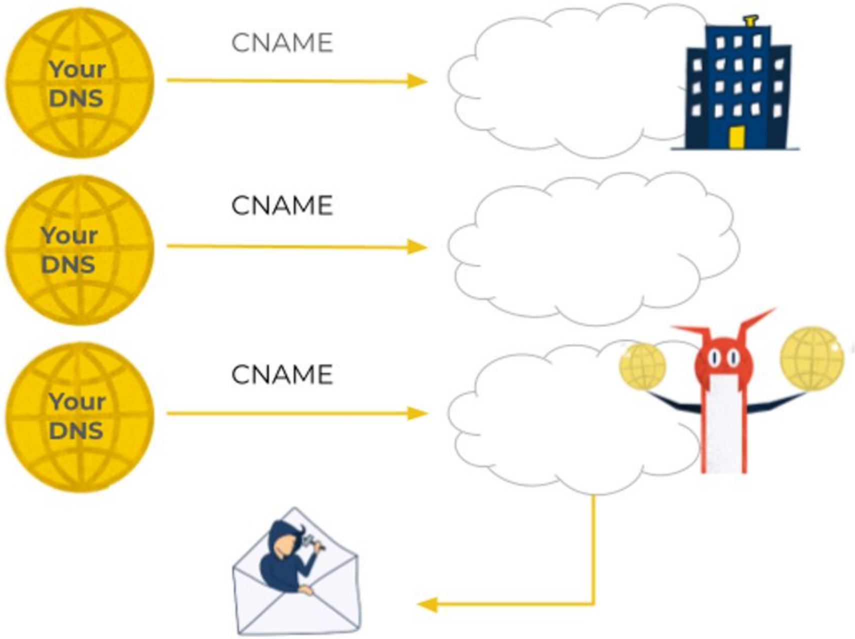
Exploiting dangling DNS records

- Leaving DNS records in a zone that is no longer used leaves domain name owners vulnerable to various forms of abuse
- Common with CNAME records
- Due to decommissioned external services (and typos)
- Zone files often seem to be a one way street ;)

CNAMES and TEXT records

- CNAMEs are used to point one domain to another e.g. prague.dns-oarc.net -> oarc43.dns-oarc.org
- By adding a TXT record to the target instead of an A record, you can publish a SPF record….
- …..and use the origin to authenticate emails!

Dangling DNS for email



You create a CNAME entry to point to a service you are using.

The service ceases to exist, but your CNAME entry continues to point to the service's domain.

A bad actor identifies the domain your CNAME is pointing to and purchases the domain.

The bad actor adds an SPF record to the text record of the domain, enabling them to send email using your subdomain. They could even add MX records and receive traffic.

2 | INTRO TO SUBDOMAILING

SPAMHAUS

SubDoMailing | Classes of domains

1. Victims (dangling CNAME)
2. CNAME target domains
3. SPF include domains
4. Infrastructure domains
5. Body/payload domains

1 | Victim domain (dangling CNAME)

- Owned by ‘innocent bystanders’
- Zone contains CNAME pointing to another domain that no longer exists
- Dangling DNS names enable abuse by third parties
- If fixed by the domain owner….the scheme falls apart
- High profile domain owners at greater risk

2 | CNAME target domain

- Domain that the dangling CNAME (victim domain) points to.
- Actual name & TLD of target domains determined by the dangling entries, so limited options!
- Two main variants:
  - External services expired domains (e.g. discontinued products)
  - Typos of legitimate targets

Example | CNAME target domain

- **victim-domain.example.com 3600 IN   CNAME a3erp-nominacloud.com**

- a3erp-nominacloud.com. 172800 IN   NS   054.a3erp-nominacloud.com
  a3erp-nominacloud.com. 172800 IN   NS   372.a3erp-nominacloud.com

- 054.a3erp-nominacloud.com. 3600   IN   A   216.22.11.204

- 372.a3erp-nominacloud.com. 3600   IN   A   66.63.160.161

3 | SPF include domain

- Included in CNAME target domains to:
  - expand the available space in SPF records
  - to make management easier
- Observed containing the live infrastructure (sending IPs) of attackers
- Great for active reconnaissance

Example | SPF include domain

- Example: a3erp-nominacloud.com

- "v=spf1 include:nicefood.us.com include:jobfinder.us.com include:healthy.de.com include:basket.de.com include:business2.me include:2ad.me -all"

- Same for:
  1paket.net
  galasport.net
  ipv4-brasil.com
  m2imb.com
  martizcx.com
  ntgmail.net

4 | Infrastructure domain

- Any other domains used by attacker to conduct campaigns
- rDNS for sending IPs
- DKIM signing (d=)

Example | Infrastructure domains

- Example rDNS domains used/owned by actor:

74.48.156.67	cytivalifesciences.me
74.48.156.68	grow4.me
74.48.156.69	larrysherwood.me
74.48.156.70	karabakh.me
74.48.161.103	canyoututor.me
74.48.161.104	profitability.me
74.48.161.105	tossing.me

- But also:

74.48.151.242	only-slocate.iodesign.me
74.48.151.243	cordial-cdpd.iodesign.me
74.48.151.244	demerit-dod.iodesign.me
74.48.151.245	iodesign.me

5 | Payload domain

- Included in the body/payload of emails
- Can be third party owned
- Can be an abused resource

3 | SUBDOMAILING CASE STUDY

SPAMHAUS

SubDoMailing Campaign

Victim domain

```
autorigoldi.it.
```

CNAME

```
skoda.autorigoldi.it.      3600    IN    CNAME   hub.dealerskoda.com.
hub.dealerskoda.com.       3600    IN    CNAME   dealerskoda.com.
```

CNAME target

```
dealerskoda.com.           3600    IN    TXT   "v=spf1 include:nicefood.us.com
include:jobfinder.us.com include:healthy.de.com include:basket.de.com -all"
```

SubDoMailing campaign

SPF payload domain

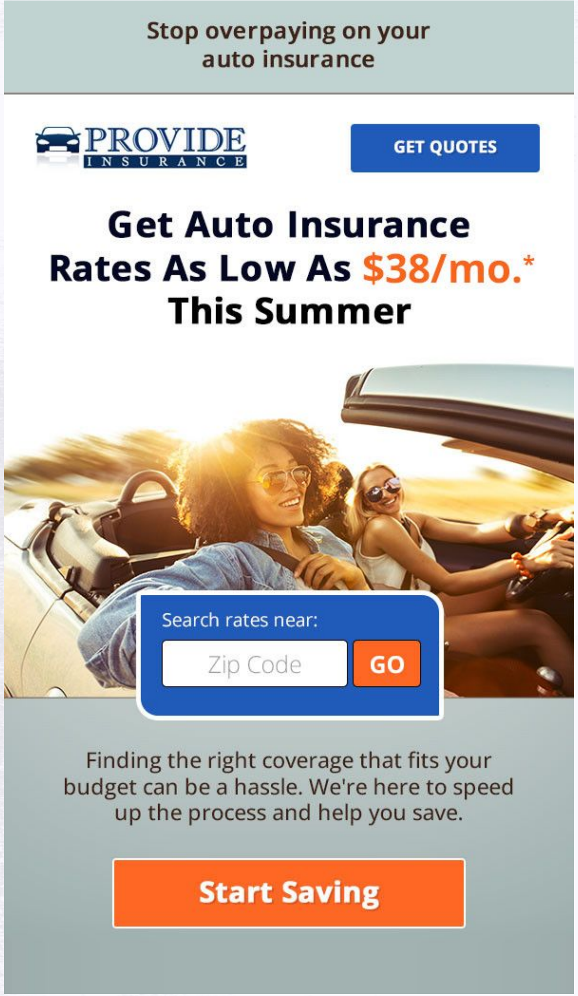
```
nicefood.us.com.            3600  IN      TXT     "v=spf1 ip4:194.54.184.139 ip4:194.54.184.140 ip4:194.54.184.141
ip4:194.54.184.142 ip4:194.54.184.143 ip4:194.54.184.152 ip4:194.54.184.153 ip4:198.27.110.66 ip4:198.27.110.75
ip4:149.56.204.126 ip4:198.27.110.69 ip4:198.27.110.72 ip4:198.27.110.74 ip4:83" ".136.49.57 ip4:83.136.49.59 ip4:83.136.49.61
ip4:83.136.49.62 ip4:83.136.49.36 ip4:83.136.49.38 ip4:148.135.102.5 ip4:148.135.102.7 ip4:148.135.102.8 ip4:148.135.102.9
ip4:148.135.102.10 ip4:148.135.50.135 ip4:148.135.50.153 ip4:148.135.50.154 ip4:148.135" ".50.156 ip4:148.135.50.157
ip4:148.135.50.158 ip4:148.135.50.160 ip4:61.97.250.130 ip4:61.97.250.141 ip4:61.97.250.142 ip4:61.97.250.144
ip4:61.97.250.153 ip4:61.97.250.154 ip4:61.97.250.155 ip4:74.208.165.47 ip4:74.208.211.170 ip4:74.208.235.197 ip4:194."
"54.184.90 ip4:194.54.184.92 ip4:194.54.184.93 ip4:194.54.184.94 ip4:194.54.184.95 ip4:185.112.82.80 ip4:185.112.82.81
ip4:185.112.82.82 ip4:185.112.82.83 ip4:185.112.82.84 ip4:69.61.104.64 ip4:69.61.104.65 ip4:69.61.104.66 ip4:69.61.104.67
ip4:69.61.104.6" "8 ip4:81.7.3.72 ip4:81.7.3.222 ip4:81.7.3.223 ip4:81.7.3.224 ip4:81.7.3.226 ip4:148.135.33.58 ip4:148.135.33.59
ip4:148.135.33.60 ip4:148.135.33.61 ip4:148.135.33.62 -all"
```

4 | WHAT ARE THEY MAILING?

SPAMHAUS

What are they mailing?

Car insurance spam!



Stop overpaying on your auto insurance

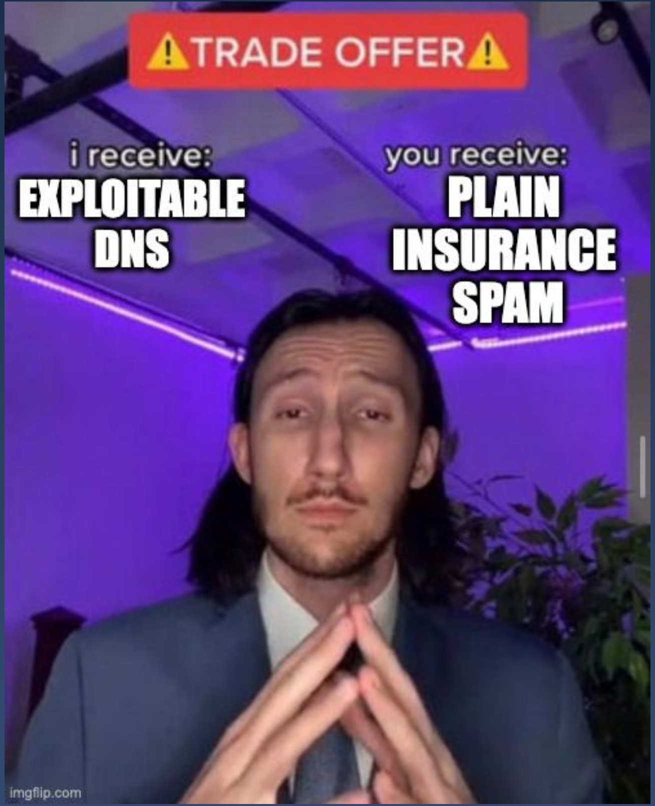
Get Auto Insurance Rates As Low As $38/mo.* This Summer

Search rates near:

Finding the right coverage that fits your budget can be a hassle. We're here to speed up the process and help you save.

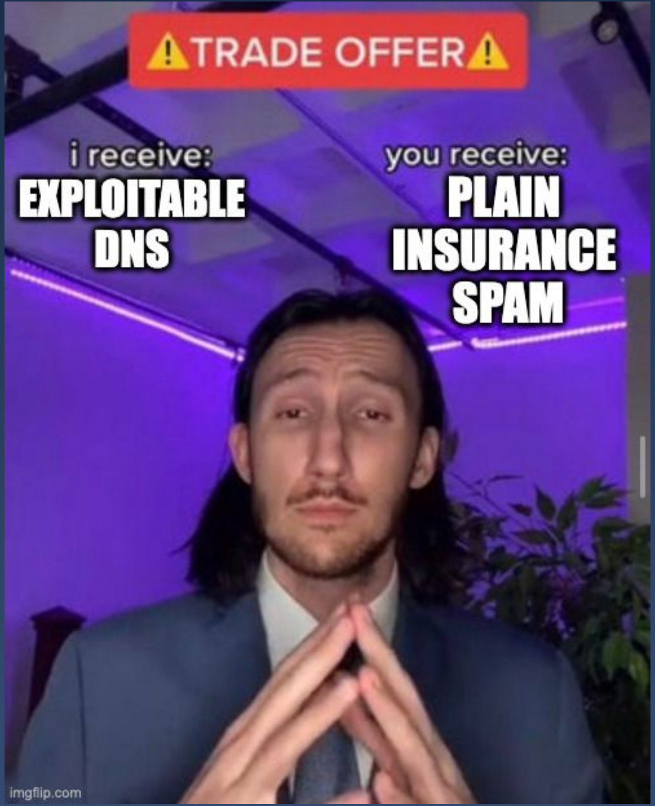
What are they mailing?

I feel cheated…



I feel cheated...

- ✗ **Not** a cool malspam campaign...
- ✗ **Or** a super targeted phishing...
- ✗ **Or** an attack targeting the business that owns the exploited domain, but...



.....this *may* still have happened!

5 | RECOMMENDATIONS

SPAMHAUS

What can we do?

- Delete deprecated entries from DNS zone files.
- DKIM alignment is a good idea.
- Watch this closely - it’s a TTP, so not limited to a single actor.

Learn more - get in contact

Carel Bitter
Head of Data, Spamhaus

✉ carel@spamhaus.com

in https://www.linkedin.com/in/carelb/

🌐 https://www.spamhaus.org

SPAMHAUS