

# Considerations for Protective DNS Server Operators

**draft-liu-dnsop-protective-dns-01**

**For DNSOP at IETF 125 on March 2026**

Haixin Duan, **Mingxuan Liu\***, Baojun Liu, Chaoyi Lu

Zhongguancun Laboratory

<https://www.liumx.net>

March 2026

# Motivation: Why do we need Protective DNS ?

- Your journey on the Internet often starts by sending DNS requests



- Attackers also widely abuse DNS (use malicious domains) for cyber attacks
  - Over 91% of malware uses DNS to carry out attacks\*



Malware



Trojan



Botnet



Phishing



Data Theft



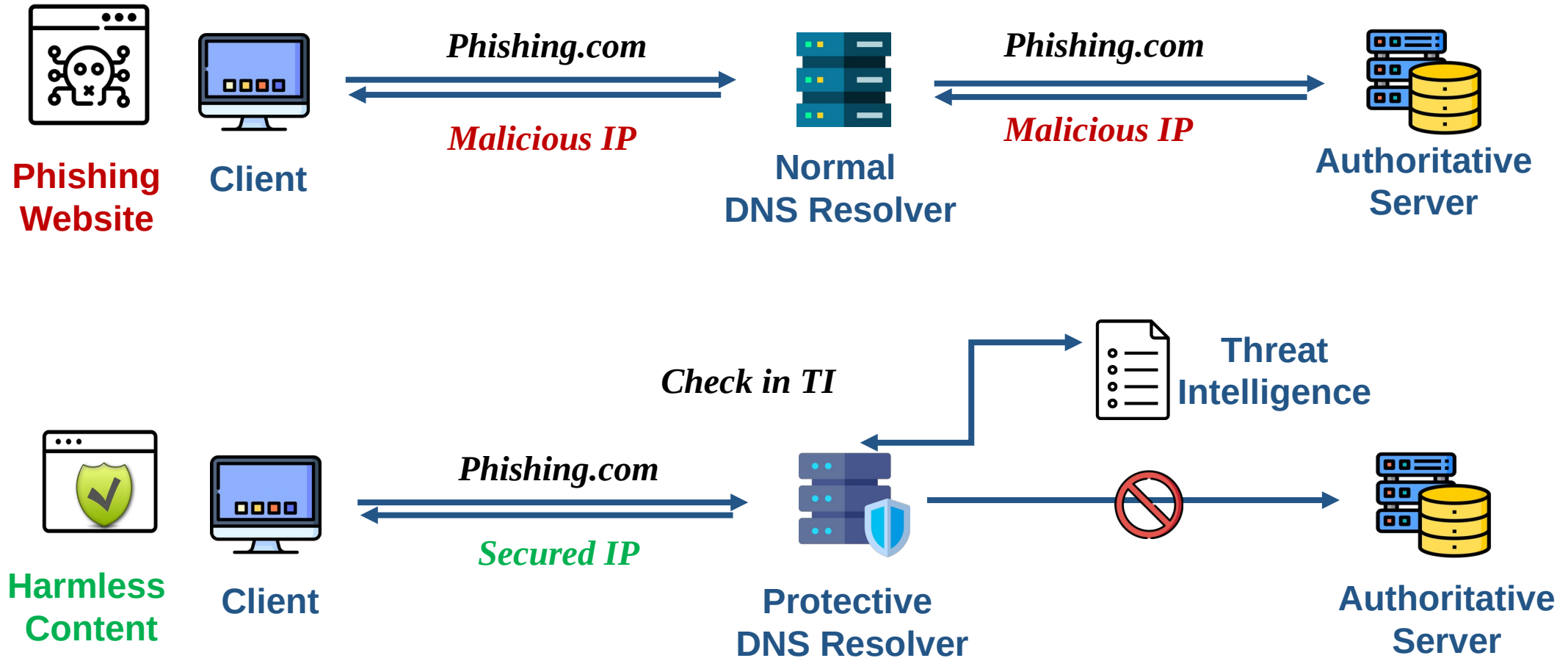
DNS Tunnel

**DNS-based blocking mechanisms are effective in curbing cyber attacks!**

\* <https://umbrella.cisco.com/blog/dns-security-your-new-secret-weapon-in-your-fight-against-cybercrime>

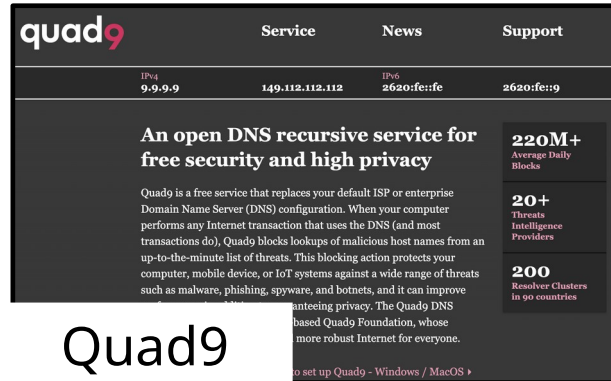
# What is Protective DNS (PDNS) ?

- **Protective DNS (PDNS)** can proactively intercept and block malicious activities during the domain resolution process

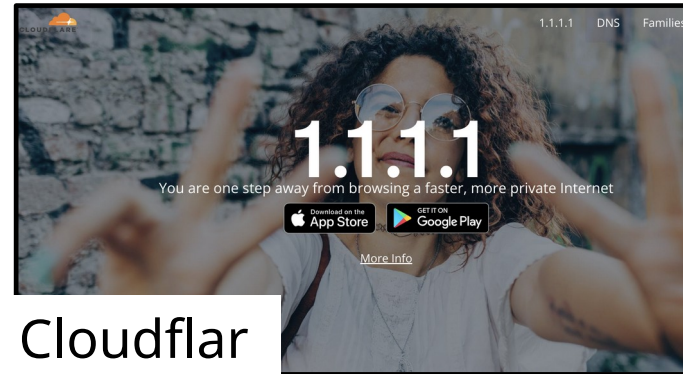


# PDNS is a Thriving Security Service

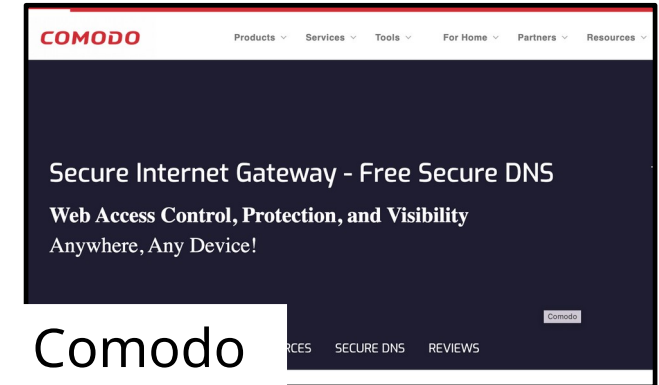
- Gained support from dozens of large DNS services



Quad9



Cloudflare



Comodo

- Promoted to establish National PDNS infrastructure



USA



Canada



European Union

# What does this document target for Protective DNS ?

## Considerations for Protective DNS Server Operators

[draft-liu-dnsop-protective-dns-01](#)

- Goal:**
- Provide specific **operational and security considerations** for Protective DNS providers to make the service **more usable and secure**.
- Why:**
- The demand for the use of Protective DNS is **constantly increasing**.
  - Due to the lack of guidance, **significant discrepancies** exist in PDNS regarding rewrite policies, blocklist selection, and performance.
  - Even **potential security risks** may emerge due to implementation flaws.

# Operational Consideration for Protective DNS

- **Blocklist Selection**

- Define the **types of domains** to be blocked based on the intended use case.
- Verify the **correctness** of these domains to avoid false positives.
- Select an appropriate **blocklist source and deployment approach** based on operational context, including device resource constraints and network access patterns, like local RPZ\*.

- **Rewriting Policy Construction**

- Select appropriate **rewriting approaches** based on their application requirements, since each rewriting strategy caters to specific security scenarios.
  - Secure IP Address
  - Specialized IP Address
  - Secure CNAME
  - Empty Answer Section
  - Special Response Codes (Rcodes)
- Consider the impact of **TTL configurations** and appropriately configure the TTL values for rewritten records.

\* <https://www.ietf.org/archive/id/draft-vixie-dnsop-dns-rpz-00.txt>

# Operational Consideration for Protective DNS

- **Performance Impact**

- Consider Factors that can **affect performance (like query latency)**, such as blacklist deployment method (remote vs. local), scale, and domain matching techniques (e.g., hash matching).

- **Offering Explanation**

- Provide **explanation of PDNS**, since its blocking is a black-box for end users, like configuring a webpage or using EDE \*.

```
+-----+
|           EDE Option           |
| +-----+ |
| | Option Code: 15 (EDE) | |
| +-----+ |
| | Option Length: xxx   | |
| +-----+ |
| | Info Code: 18       | |
| +-----+ |
| | Extra Text: "PROHIBITED" | |
| +-----+ |
+-----+
```

\* <https://datatracker.ietf.org/doc/html/rfc8914>

# Security Consideration for Protective DNS

- **Rewriting Policy Flaws**

- **Redundant Rdata:** Provide both rewriting response and original malicious response.

```
malicious_domain.com  A  controled_IP;  
malicious_domain.com  A  original_malicious_IP;
```

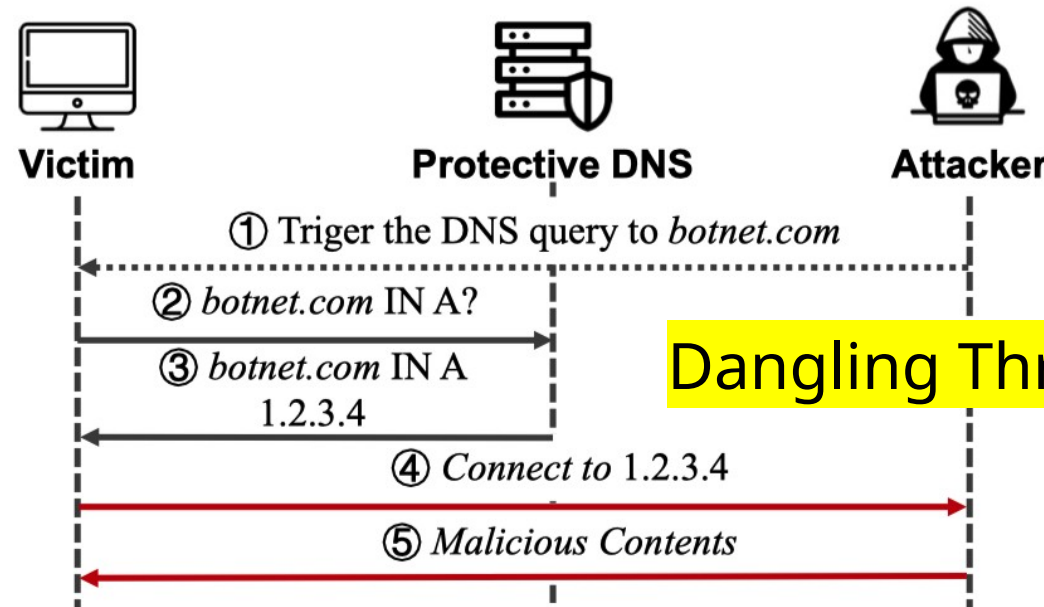
- **Missing Record type:** Ensure defense even on less common query Rtype.

```
malicious_domain.com  A  controled_IP;  
malicious_domain.com  TXT  
original_malicious_response;
```

- **Rewriting Policy Coverage:** Ensure that the defensive functions are effective in all functional scenario, like encrypted DNS and IPv6 scenarios.

# Security Consideration for Protective DNS

- **Dangling Resources:** Exercise due diligence when using **third-party network resources** to avoid takeover risks from Dangling Resources \*.
  - If the rewritten **IP is a cloud service IP**, obsolete cloud IP addresses pose a takeover risk.
  - If the rewritten **CNAME domain expires**, there is an expired domain takeover risk.
  - If the rewritten **third-party service** subdomain takeover



Dangling Threat in PDNS Infrastructure

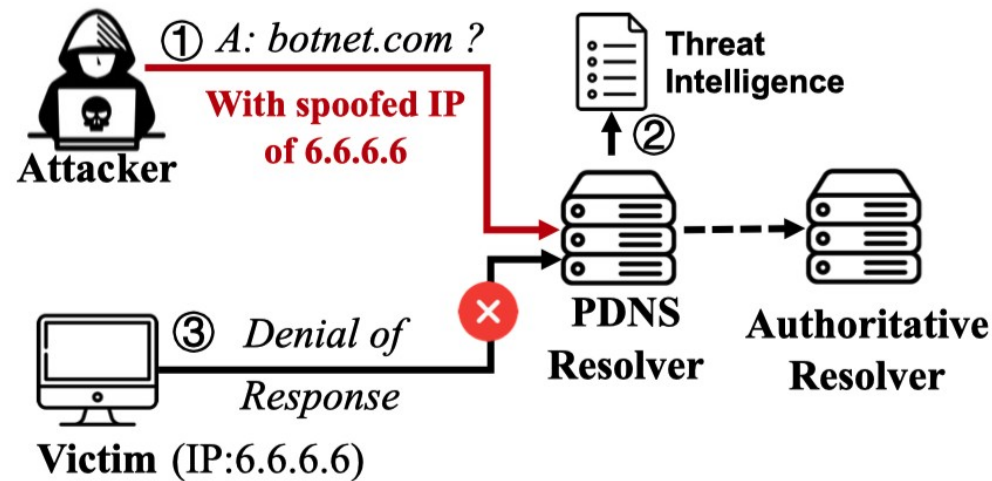
# Security Consideration for Protective DNS

- **Over-Blocking:** Minimize the impact of **over-blocking**, as this introduces significant collateral damage in two primary aspects.
  - **Blocklist Construction**
    - **Error in blocklist** directly causes collateral damage to benign domain names.
    - **Over-generalizing target domains** for blocking may also lead to collateral damage, like using keywords.

malicious_domain.com	A	controled_IP; (FQDN)	✓
"phishing" in domain	A	controled_IP; (Keyword)	✗
*.malicious_domain.com	A	controled_IP; (Wildcard	✗
Domain)			✗
*.com	A	controled_IP; (SLD/TLD Level	
Domain)			

# Security Consideration for Protective DNS

- **Over-Blocking:** Minimize the impact of **over-blocking**, as this introduces significant collateral damage in two primary aspects.
  - **Blocking Policy**
    - Empirical analysis has shown that some Protective DNS implementations **exhibit over-blocking collateral damage from aggressive blocking**, introducing **Denial-of-Response (DoR)** risk.
    - To effectively mitigate denial-of-response attacks, providers can send oversized DNS responses to **enforce TCP fallback** thereby thwarting DoR attacks constructed via IP spoofing.



**DoR Risk**

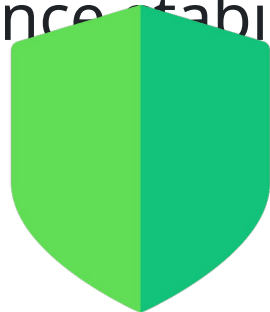
# Security Consideration for Protective DNS

- **Interaction with data integrity protection**

- Consider **DNSSEC\*-compatible** if DO bit or CD bit set in DNS queries.

- **Fallback**

- Consider **fault diagnosis** for denial-of-service (DoS) failures in individual components and corresponding fallback mechanisms to ensure performance stability.



Protective



Attack

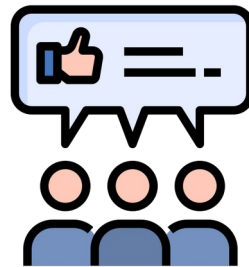
\* <https://datatracker.ietf.org/doc/html/rfc4035>

# Discussion

- **Growth in Protective DNS usage requires operational and security advice!**
- **More Feedback from operators of Protective DNS !!!!**
  - Already feedback of **Protective DNS Operator – Latin America**
  - Update of blocking types to include more than just malicious domains
  - Update the wording, such as replacing blacklist with blocklist
  - ...
- **Which of these considerations are most contentious?**

• **Next Step...**

• **Let us know your feedback!**



# Thanks!!!!

**draft-liu-dnsop-protective-dns-01**

**For DNSOP at IETF 124 on November 2025**

**Haixin Duan, Mingxuan Liu\*, Baojun Liu, Chaoyi Lu**

Zhongguancun Laboratory

<https://www.liumx.net>

November 2025