

DNS in Real-World Attacks

SOC Insights on DNSSEC Gaps, Misconfigurations, and Abuse

Olabimpe Adoloro

Cybersecurity & Data Protection Specialist

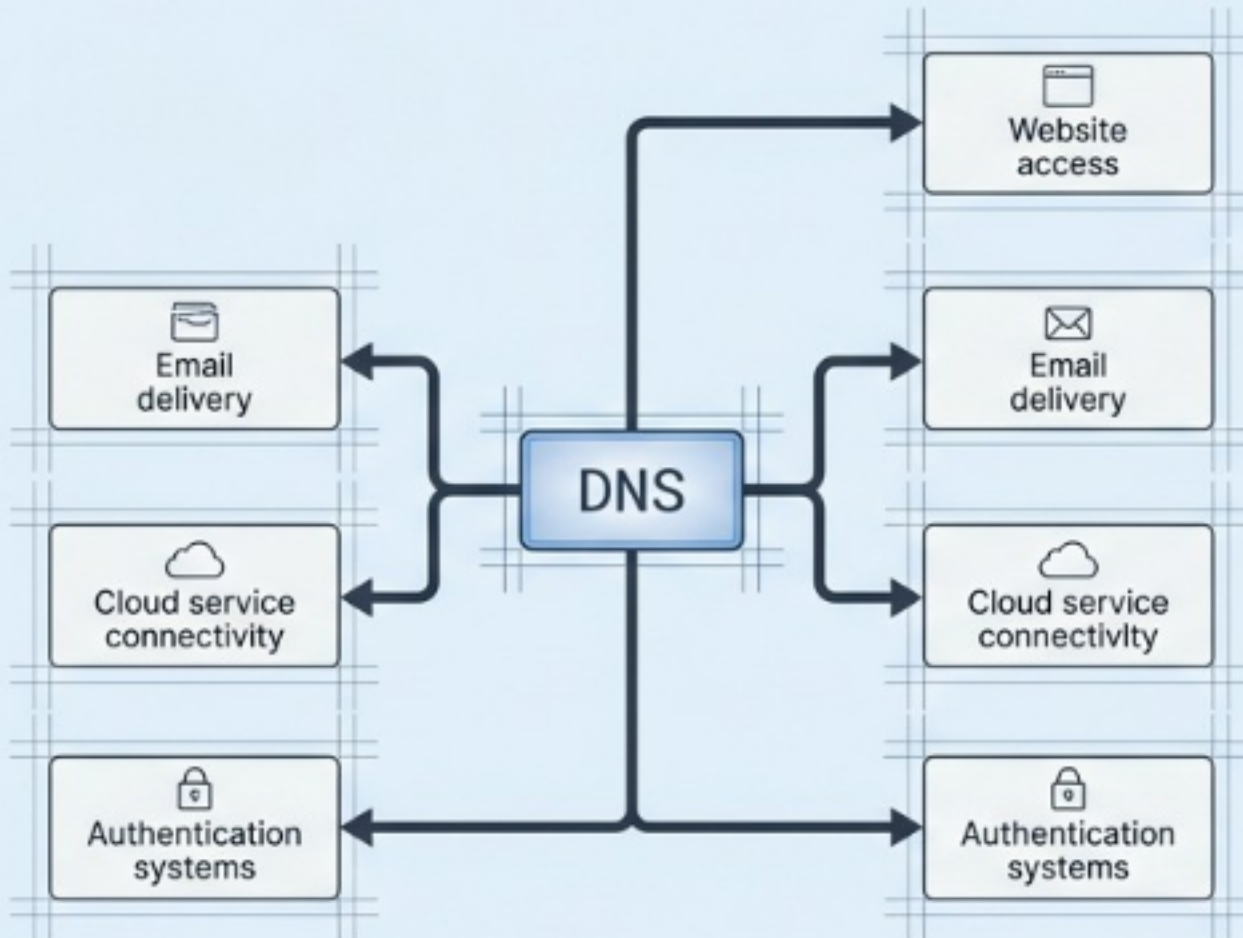
Founder, MOBA CyberSafety Nexus

**ICANN85 DNSSEC and
Security Workshop**

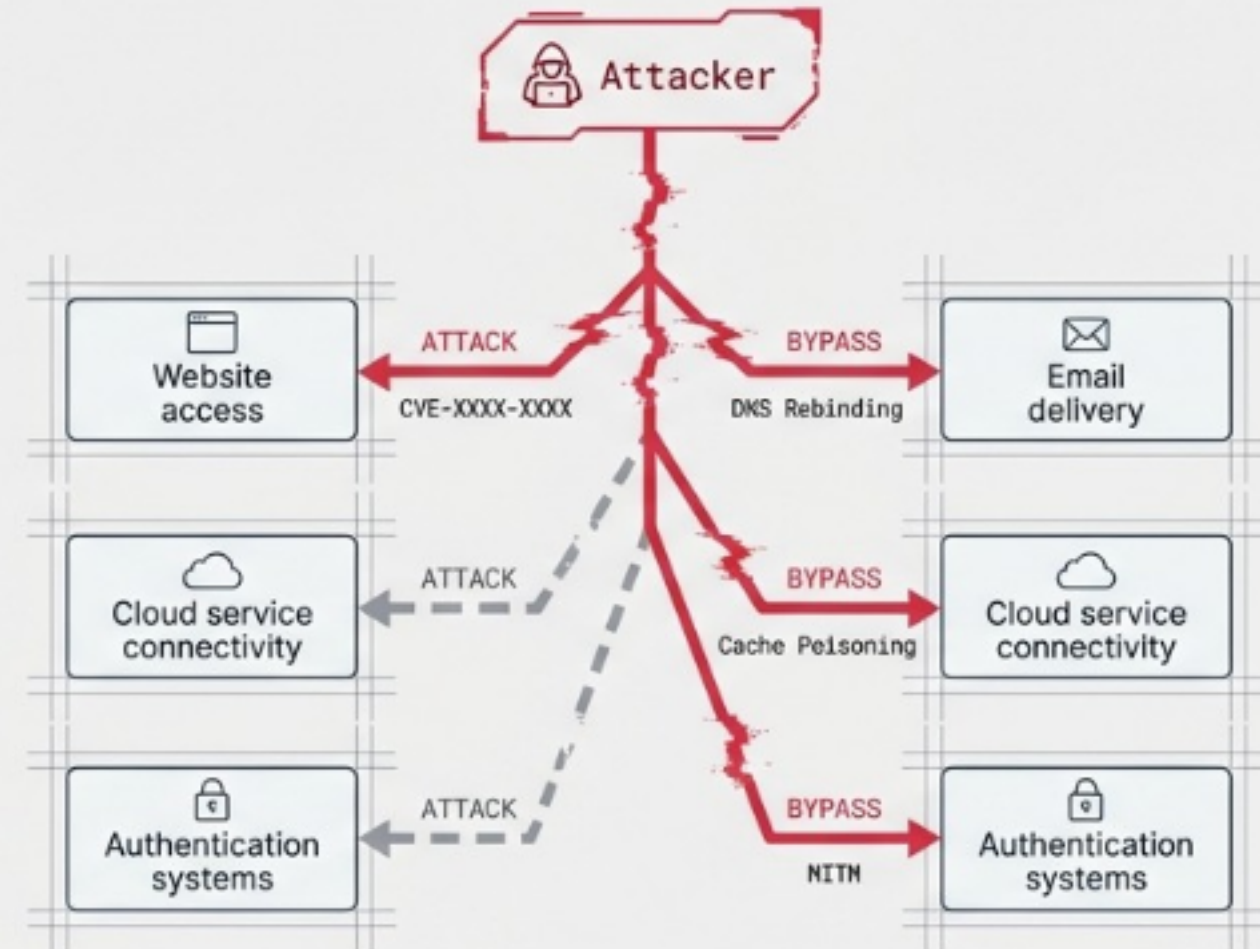
March 11, 2026

DNS powers the internet, making it a critical attack surface

TRUST DIAGRAM



ABUSE VISUAL

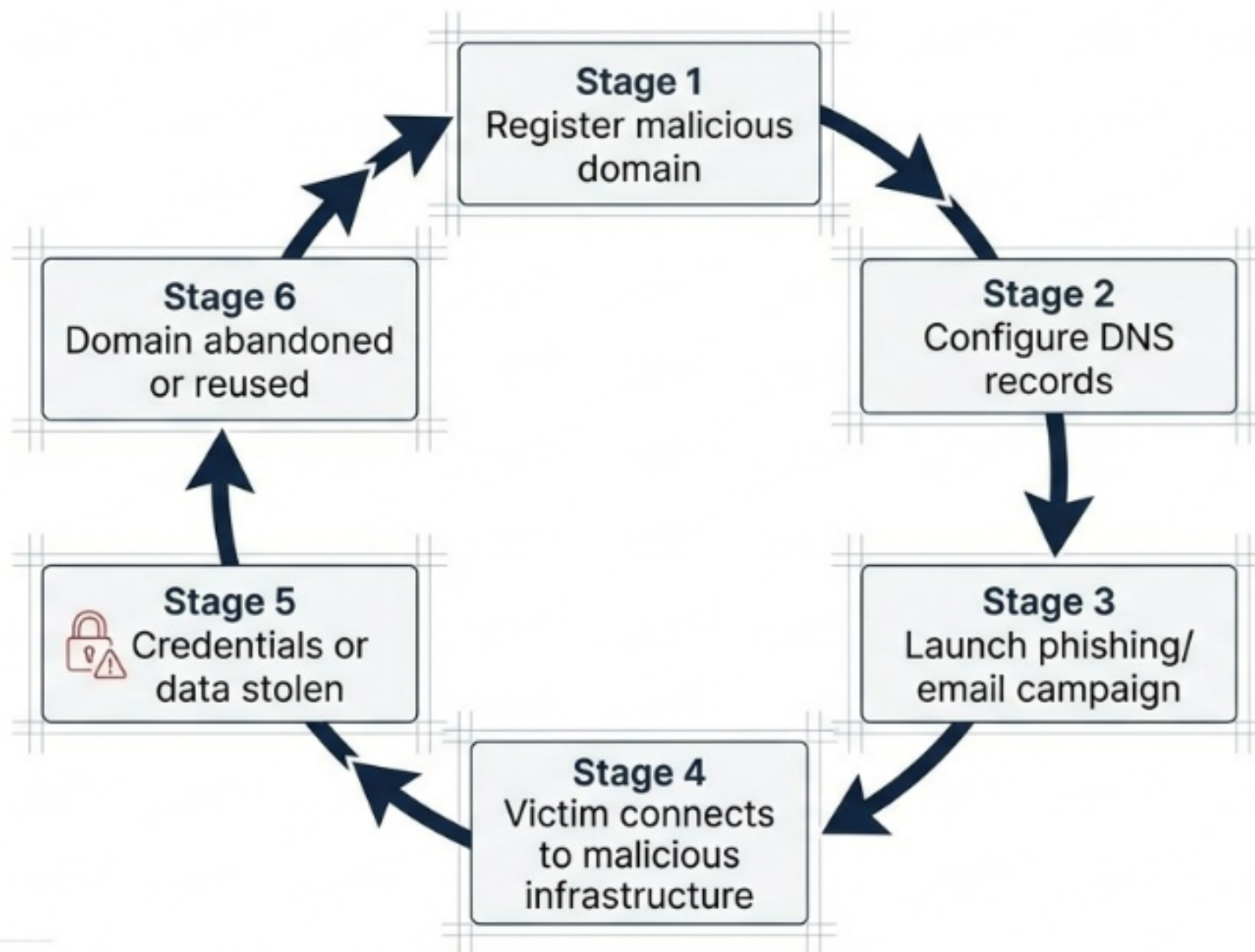


DNS is one of the most trusted systems on the Internet.
Attackers exploit that trust.

Attackers target DNS because it offers high reward with minimal operational friction



The lifecycle of a DNS-enabled attack



Case Pattern 1: Exploiting visual trust through lookalike domains

Attacker Technique

Newly registered domains are used immediately for campaigns without DNSSEC protection.

paypa**I**.com
rnicrosoft.com

Visual Deception: Uppercase 'I' mimics lowercase 'l'

Visual Deception: 'rn' combination mimics letter 'm'

SOC Impact

Exponentially increased phishing success rates due to users relying purely on visual trust.

Case Pattern 2: Bypassing email security via DNS misconfigurations

Attacker Technique

Exploiting common operational oversights:

- Missing or weak SPF records
- Missing DKIM signatures
- Weak DMARC policy (specifically set to p=none)
- Overall lack of DNS monitoring

```
_dmarc.example.com. IN TXT "v=DMARC1; p=none; sp=none;"
```



Vulnerability: DMARC set to p=none, enabling spoofing without quarantine or rejection.

SOC Impact

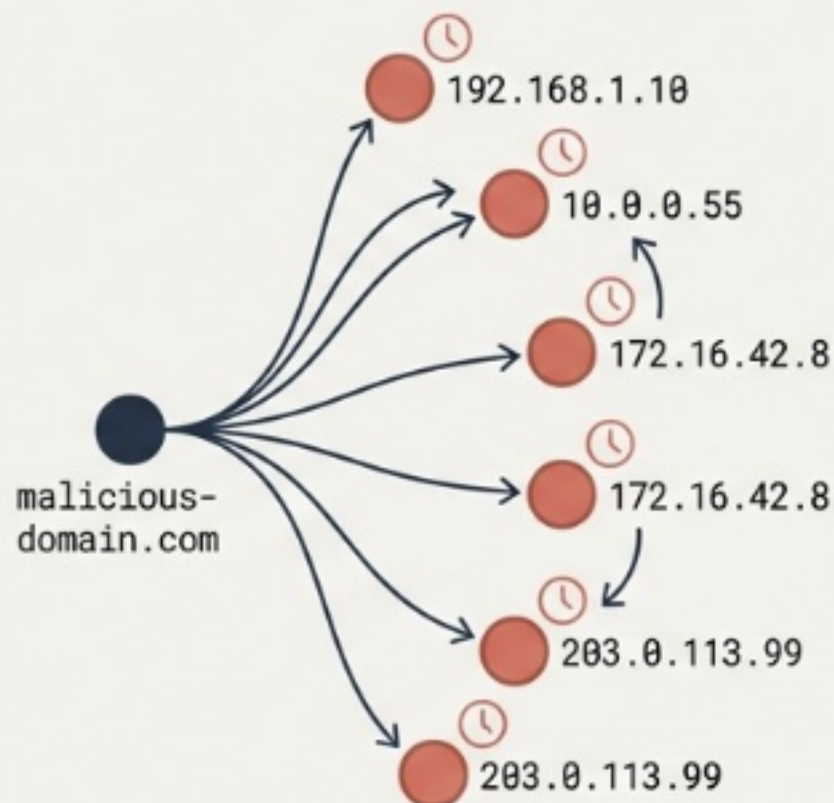
Email spoofing succeeds seamlessly, and malicious phishing emails are inherently trusted by secure gateways.

Case Pattern 3: Leveraging DNS for infrastructure evasion

Attacker Technique

Active evasion strategies observed in the wild:

- Fast-flux DNS infrastructure
- Short TTL values
- Rapid IP address switching
- Widespread abuse of subdomains



SOC Impact

Extremely difficult detection/response workflows, resulting in increased persistence of malicious infrastructure.

The defense mechanism: **How DNSSEC establishes data trust**

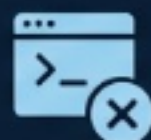


THE REALITY GAP: OPERATIONAL CHALLENGES LIMIT THE PROTECTIVE POWER OF DNSSEC.

Despite the clear benefits, SOCs and ecosystem observers note persistent operational hurdles:



- Severely limited global DNSSEC adoption.



- A systemic lack of validation implementation at the resolver level.



- High risks of operational misconfigurations causing self-inflicted outages.



- Limited overall DNS visibility within enterprise organizations.

Result: The internet ecosystem faces continued, unnecessary exposure to DNS-based attacks.

View from the trenches: DNS visibility is the ultimate operational fallback

Key Operational Insights:

- DNS visibility is **strictly critical** for proactive detection
- DNS logs provide the most valuable **forensic evidence** during an active investigation
- Early DNS **monitoring** is the **only way** to reduce eventual damage
- Acknowledgment that DNS security **maturity varies** significantly across organizations



Actionable steps to strengthen global DNS security

Organizations

- ✓ Enable DNSSEC signing and validation
- 👁️ Actively monitor DNS activity and logs
- 🛡️ Implement SPF, DKIM, and DMARC correctly

SOC Teams

- 📶 Monitor DNS telemetry continuously
- 🔍 Investigate **suspicious newly registered domains** early

Ecosystem (ICANN/Registries)

- 📢 Drastically increase DNSSEC **awareness**
- ➡️ Drive initiatives for wider adoption

“Attackers do not break DNS—they exploit gaps in our implementation”

DNS is not just infrastructure; it is a primary attack vector. Strengthening DNS security through visibility, proper configuration, and DNSSEC adoption is essential to protecting the global Internet ecosystem.