Missing DMARC Records Leading to Email Spoofing

Pending Fix • LOW • Reported by fluhar on May 18, 2025 • #PT30497_4

Vulnerability Type

Server Security Misconfiguration > Mail Server Misconfiguration > Email Spoofing to Inbox due to Missing or Misconfigured DMARC on Email Domain

Description

During the assessment, it was observed that the applications domains lack a DMARC record in their DNS configuration. This makes it easier for attackers to send spoofed emails using the organization's domain, which can deceive recipients and bypass basic spam filters.

DMARC is an email authentication protocol that builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to give domain owners control over how their email is handled if it fails authentication. A properly configured DMARC policy allows domain owners to instruct email providers to reject or quarantine unauthenticated messages and receive reports on email activity.

Affected Targets

```
https://slkohlercampaign.com/
```

```
https://npkohlercampaign.com/
```

```
https://bdkohlercampaign.com/
```

```
https://bhkohlercampaign.com/
```

OWASP Severity

LOW

CVSS v3.1 Score

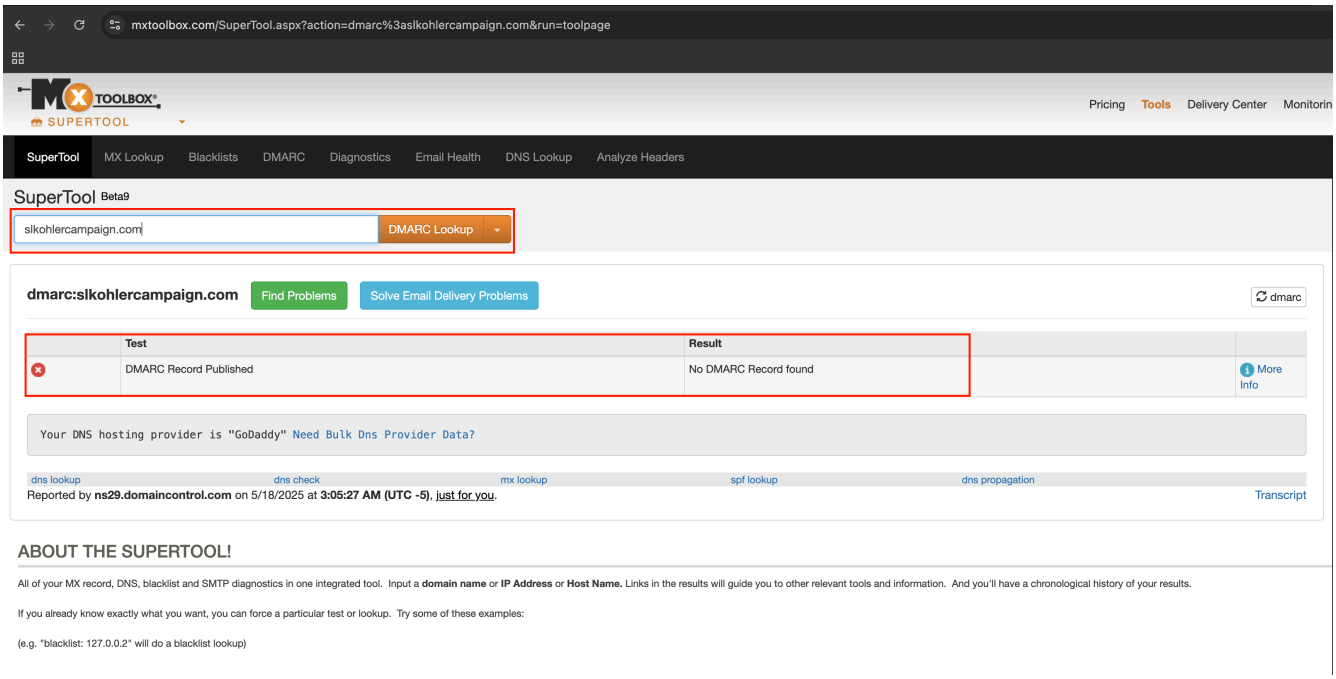
LOW (3.1)

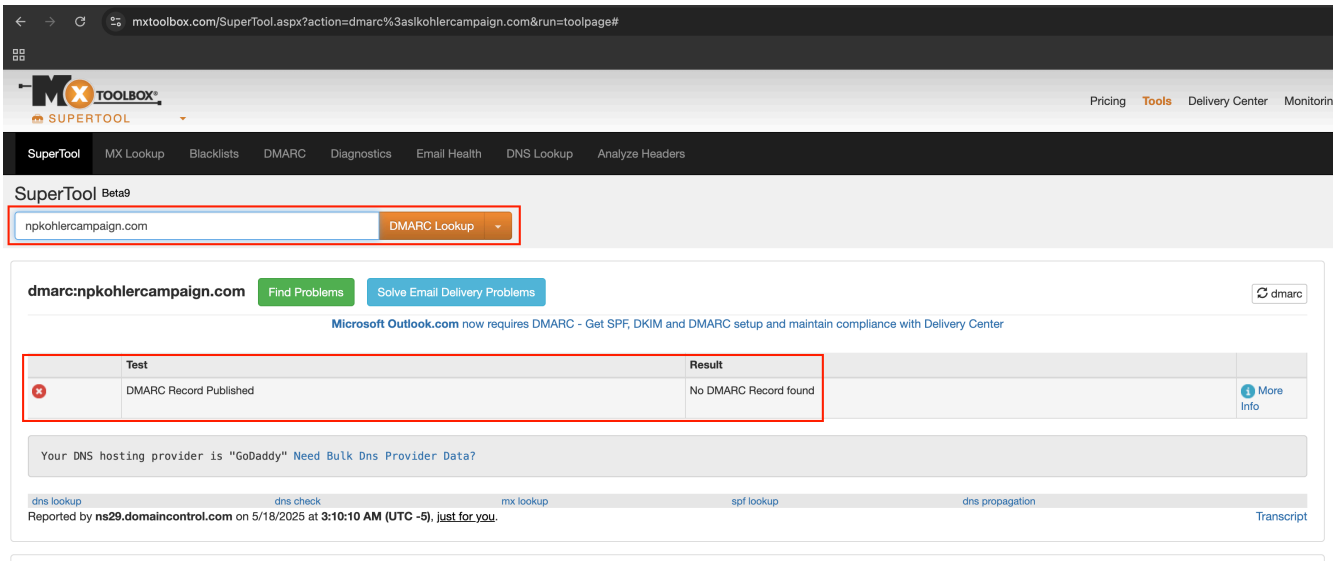
Proof of Concept

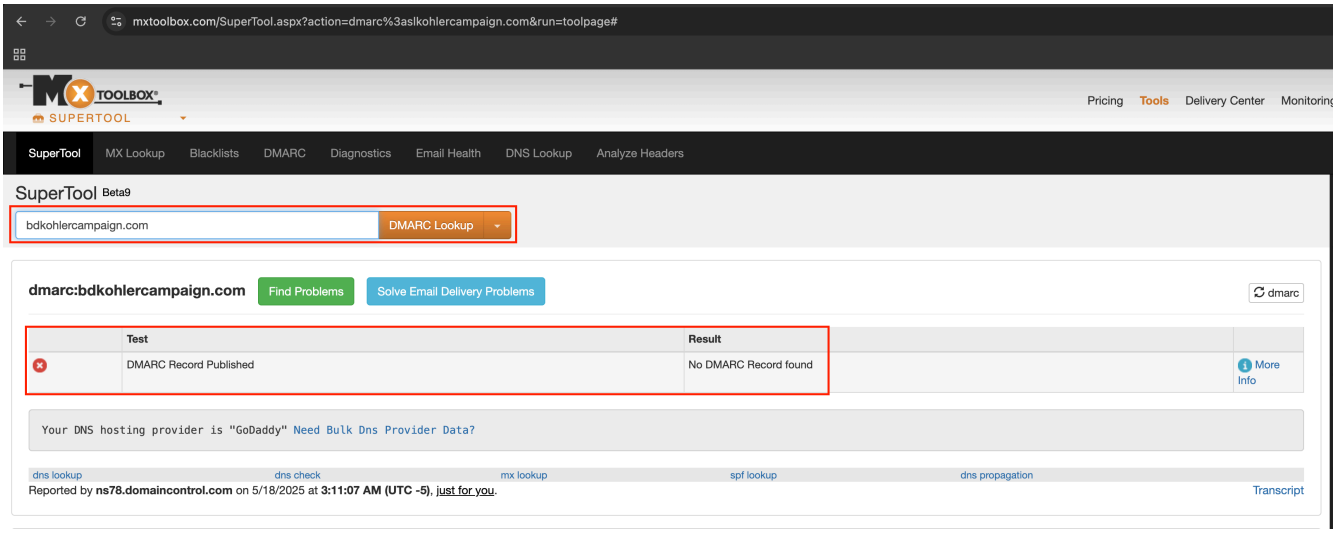
Step 1: Navigate to https://mxtoolbox.com/dmarc.aspx and enter the following domains.

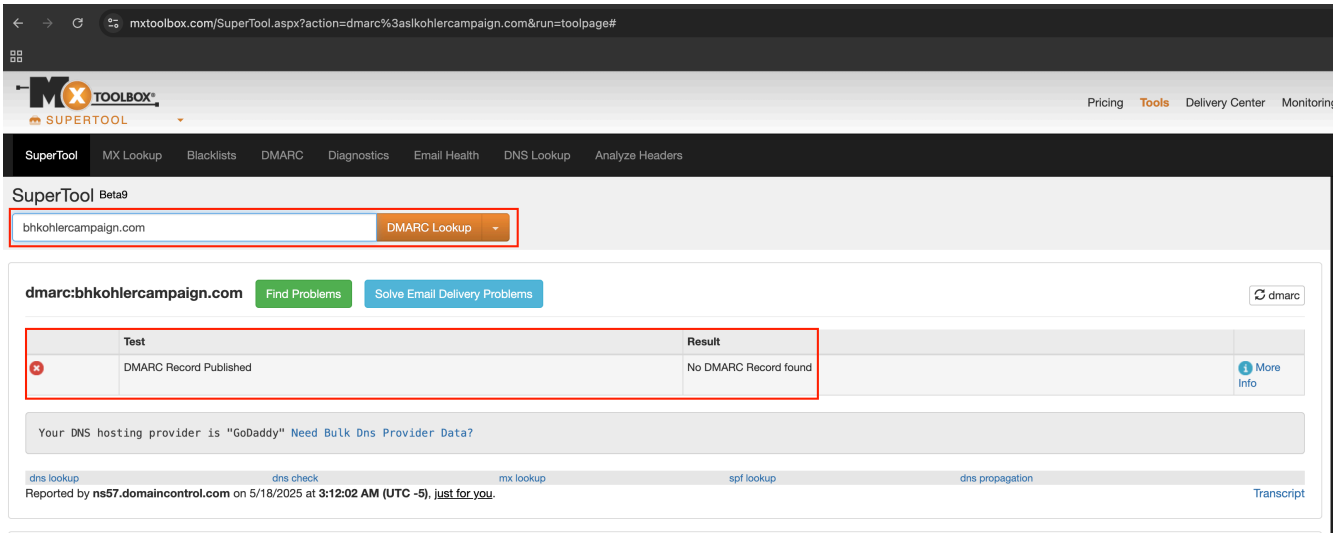
- slkohlercampaign.com
- npkohlercampaign.com
- bdkohlercampaign.com
- bhkohlercampaign.com

Step 2: Observe that the DMARC record is not configured for the domains.









Impact

The absence of a DMARC record exposes the domain to email spoofing, which can be leveraged in phishing or social engineering attacks. While this does not directly compromise internal systems, it can significantly damage the organization’s reputation, erode user trust, and increase the success rate of email-based threats. The risk becomes more critical if the domain is used for customer communication, invoicing, or internal operations.

Suggested Fix

SPF is not a sufficient email spoofing protection in case of some of the largest email providers. Emails spoofed for domains having properly configured hard fail SPF records may still be delivered to the recipient's inbox. In order to fully prevent email spoofing create a DMARC record with Ňp=rejectÓ policy. Please note that if your DMARC policy is not set up properly it may result in email delivery issues.

,
ACTIVITY

fluhar changed state to **Pending Fix** May 18