Blake Mark Productions
124 City Road
London
EC1V 2NX

Tel: +44 (0) 20 3137 0455
blakemarkproductions.com

Reason For Outage (RFO): DNS resolutions issues

Wednesday 26th October 2025

Impact

Intermittent DNS resolution failures occurred across services using our secondary nameserver. This resulted in occasional site load failures, slow DNS responses and reduced reliability for domains using our standard nameserver set. Primary DNS services remained available throughout, which limited the overall impact, but customers relying heavily on NS2 saw noticeable degradation during the incident.

Background

Our DNS platform is designed with redundancy across two independent nameserver systems (NS1 and NS2)
NS1 is hosted within our primary UK network.
NS2 is operated on a separate network to ensure service continuity even in the event of a core network failure.

This separation provides resilience against local outages and distributes DNS query load across multiple independent environments.

Details

At 07:54, automated monitoring detected intermittent DNS resolution failures affecting a number od domains. Engineers began investigation immediately.
At 08:34, we confirmed the issue was isolated to DNS resolution on NS2. All other network services continued to operate normally.
Between 08:35 and 09:45, engineers identified a large DDoS attack targeting a specific domain hosted on our DNS platform. The high-volume request load degraded NS2's ability to respond reliably.
At 09:45, NS2 was taken offline to expand compute resources and was restored at 09:55, which reduced but did not fully eliminate the impact.
At 10:10, a software based mitigation layer was introduced to filter malicious traffic patterns.

At 10:46, this mitigation was refined into an automated process that continuously identified and suppressed attack traffic. DNS stability improved from this point.
Full resolution was achieved at 12:30, when the attack traffic patterns subsided and normal DNS performance was confirmed.

Investigation

The incident was caused by a high volume DDoS attack directed at a domain hosted on our DNS infrastructure.
NS1 absorbed the attack successfully due to its network level protection. However, NS2 received a request profile that was technically valid but malicious in intent, which made automated filtering more difficult. This led to intermittent slowdowns and query failures.

Temporary expansion of compute resources initially reduced the impact, but sustainable stability required a targeted, software driven mitigation capable of analysing and supressing abnormal traffic patterns in real time. Once deployed and automated, this restored service reliability.

No data loss or security breach occurred.

Improvements

We are implementing several changes to strengthen DNS resilience and reduce the likelihood of recurrence.

- NS2 will be migrated to a load balanced cluster so that DNS queries can be distributed across multiple systems rather than a single unit.
- Additional compute and network capacity will be introduced to increase headroom for absorbing volumetric attacks.
- Automated traffic analysis will be expanded to identify and supress malicious patterns faster.
- Longer term, we are accelerating deployment of a globally anycasted DNS architecture using multiple global notes to eliminate reliance on a two-node model and significantly increase both performance and attack tolerance.

Please accept our apologies for the disruption caused by this outage.

These enhancements will provide materially stronger protection against future DDoS events.

Issued by:
Will Naughton
Head of Creative & Digital Delivery