ORNA™

Cybersecurity Advisory

# Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about an email notification from Microsoft alerting organizations as to whether they were affected by a breach of Microsoft's corporate systems that took place at the end of 2023.

## Summary

Following the **Midnight Blizzard** attack, Microsoft has been sending out notifications to affected organizations without following their own customer data breach notification process and instead opting to send an email easily flaggable as spam/phishing to the tenant administration account.

## Overview

As reported by Microsoft in two blog posts [1][2] from January and March of this year, the *Midnight Blizzard* attack, attributed to the Russian state-sponsored group *Nobelium*, involved a password spray attack on Microsoft's non-production test account, leading to limited access to corporate emails. An update revealed that the attackers exfiltrated information, including some company source code repositories and internal systems, although customer-facing systems remained uncompromised. Microsoft responded by increasing security measures, cross-enterprise coordination, and notifying affected customers.

More recently, threat intelligence analysts [3] have been sounding the alarm about Microsoft breaking with their own M365 customer data breach notification process and instead notifying affected organizations by emailing the tenant admin. Since this account is meant to be treated as a break glass account without an email address, many organizations might not be receiving it.

Furthermore, it appears that the notification email does not pass either SPF or DKIM which in most cases will cause it to be tagged as spam by Defender's email filter.

## Recommendations

### Recommendation #1: Review email logs for incoming emails sent by Microsoft

Orna recommends any organization which uses M365 services to query their email logs for emails sent by Microsoft via the email address mbsupport@microsoft.com to the admin account.

### Recommendation #2: Contact your Microsoft Account Manager

Orna recommends contacting your Microsoft account manager in order to ascertain if your organization has been affected by the Midnight Blizzard attack and to validate if any email received is legitimate.

## References

1. https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
2. https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
3. https://www.linkedin.com/posts/kevin-beaumont-security_check-your-email-logs-including-exchange-activity-7215355395878305793-K8n_/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.
Sincerely,
ORNA Team