UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K/A

CURRENT REPORT
PURSUANT TO SECTION 13 OR 15(D)
OF THE SECURITIES EXCHANGE ACT OF 1934

Date of Report (Date of earliest event reported) January 17, 2024

Microsoft Corporation

Washington	**001-37845**	**91-1144442**
(State or Other Jurisdiction of Incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

One Microsoft Way, Redmond, Washington	**98052-6399**

(425) 882-8080
www.microsoft.com/investor

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	**Trading Symbol**	**Name of exchange on which registered**
Common stock, $0.00000625 par value per share	MSFT	NASDAQ
3.125% Notes due 2028	MSFT	NASDAQ
2.625% Notes due 2033	MSFT	NASDAQ

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter). Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

EXPLANATORY NOTE

Microsoft Corporation (the "Company," "we," or "our") is filing this Form 8-K/A as an amendment to the Current Report on Form 8-K filed by the Company with the U.S. Securities and Exchange Commission (the "SEC") on January 19, 2024 (the "Original Filing").

Item 1.05. Material Cybersecurity Incidents

As disclosed in the Original Filing, the Company detected that beginning in late November 2023, a nation-state threat actor had gained access to and exfiltrated information from a very small percentage of employee email accounts including members of our senior leadership team and employees in our cybersecurity, legal, and other functions. Since the date of the Original Filing, the Company has determined that the threat actor used and continues to use information it obtained to gain, or attempt to gain, unauthorized access to some of the Company's source code repositories and internal systems. The threat actor's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. Our active investigations of the threat actor's activities are ongoing, findings of our investigations will continue to evolve, and further unauthorized access may occur.

We have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat. We continue to coordinate with federal law enforcement with respect to its ongoing investigation of the threat actor and the incident.

As of the date of this filing, the incident has not had a material impact on the Company's operations. The Company has not yet determined that the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

This Form 8-K contains forward-looking statements, which are any predictions, projections or other statements about future events based on current expectations and assumptions that are subject to risks and uncertainties, which are described in our filings with the SEC. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and the Company undertakes no duty to update any forward-looking statement to conform the statement to actual results or changes in the Company's expectations.

Item 7.01. Regulation FD Disclosure

On March 8, 2024, the Company posted a blog regarding the incident. A copy of the blog is furnished as Exhibit 99.1 to this report. In addition, as part of our ongoing commitment to responsible transparency to our customers and other stakeholders, we may provide additional updates regarding the incident and relevant developments directly to customers or at Microsoft blogs located here: https://msrc.microsoft.com/blog/ and https://www.microsoft.com/en-us/security/blog/.

In accordance with General Instruction B.2 of Form 8-K, the information in this Item 7.01 and Exhibit 99.1, shall not be deemed to be "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), or otherwise subject to the liability of that section, and shall not be incorporated by reference into any registration statement or other document filed under the Securities Act of 1933, as amended, or the Exchange Act, except as shall be expressly set forth by specific reference in such filing.

Item 9.01. Financial Statements and Exhibits

(d) Exhibits:

99.1	Microsoft Blog dated March 8, 2024 titled "Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard"
104	Cover Page Interactive Data File (embedded within the Inline XBRL document)

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

MICROSOFT CORPORATION
(Registrant)

Date: March 8, 2024

/S/ Keith R. Dolliver
Keith R. Dolliver
Corporate Secretary

Exhibit 99.1

Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

/ By MSRC / March 8, 2024 / 2 min read

This blog provides an update on the nation-state attack that was detected by the Microsoft Security Team on January 12, 2024. As we shared, on January 19, the security team detected this attack on our corporate email systems and immediately activated our response process. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM.

As we said at that time, our investigation was ongoing, and we would provide additional details as appropriate.

In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access. This has included access to some of the company's source code repositories and internal systems. To date we have found no evidence that Microsoft-hosted customer-facing systems have been compromised.

It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. Some of these secrets were shared between customers and Microsoft in email, and as we discover them in our exfiltrated email, we have been and are reaching out to these customers to assist them in taking mitigating measures. Midnight Blizzard has increased the volume of some aspects of the attack, such as password sprays, by as much as 10-fold in February, compared to the already large volume we saw in January 2024.

Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. It may be using the information it has obtained to accumulate a picture of areas to attack and enhance its ability to do so. This reflects what has become more broadly an unprecedented global threat landscape, especially in terms of sophisticated nation-state attacks.

Across Microsoft, we have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat. We have and will continue to put in place additional enhanced security controls, detections, and monitoring.

Our active investigations of Midnight Blizzard activities are ongoing, and findings of our investigations will continue to evolve. We remain committed to sharing what we learn.