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

MSRC
/ By MSRC / March 08, 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.