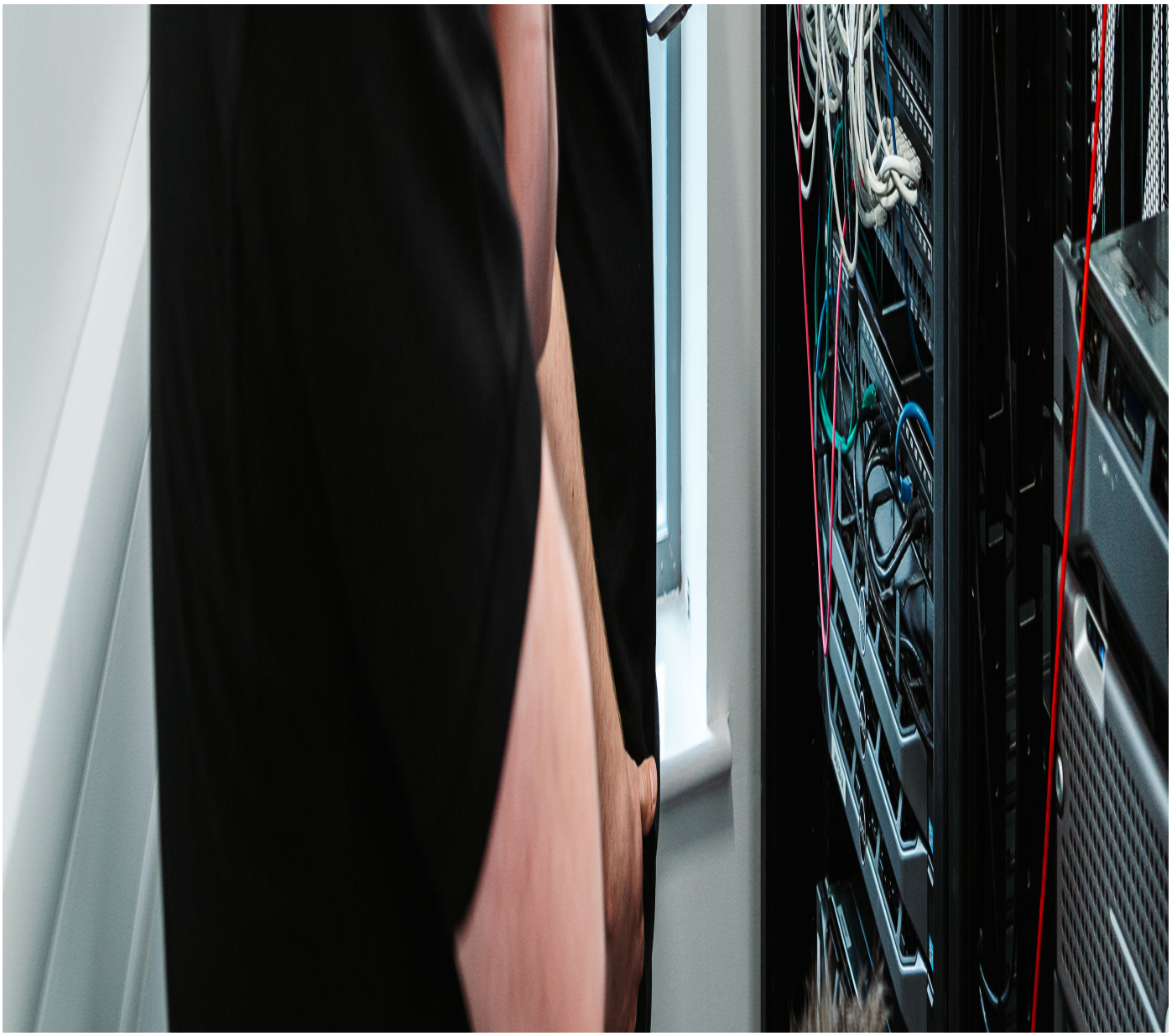
+44 345 094 0945
www.waterstons.com

Article

Mar 2024

Microsoft: Cyber Incident Review

Microsoft emails breached by nation state threat actors. Microsoft has revealed that it was targeted by nation state threat actors, Midnight Blizzard, which resulted in the compromise of several employee accounts, including those of senior leadership.



Microsoft has revealed that it was targeted by nation state threat actors, Midnight Blizzard, which resulted in the compromise of several employee accounts, including those of senior leadership.

What Happened?

In late January 2024, Microsoft released a report into a cyber-attack that took place in late November 2023.

The tech corporation revealed that the threat actor was able to initially gain access to its environment through a legacy, non-production test account, using a password spray attack - using the same password on multiple accounts via a brute force attack, before repeating with another password. These attacks were launched from legitimate, residential IP addresses within the United States, making them difficult for Microsoft to identify and block. The password spray attack was also limited in scope, targeting only a small number of accounts, and therefore generating few logs and not triggering any alerts.

The password spray attack was successful in compromising an account that did not have MFA enabled, allowing threat actors to login. While a test account and not supposed to have access within the production environment, it did have access to an OAuth application with elevated access within Microsoft's corporate environment.

This access allowed the threat actor to create new malicious OAuth applications and user accounts to maintain persistence.

The threat actors were quick to obtain full access to all mailboxes in Exchange with admin permissions, in turn giving access to emails of senior staff as well as Microsoft's internal threat intelligence teams. It appears that the attacker was primarily interested in finding out what information Microsoft had on them, rather than exfiltrating sensitive data or carrying out destructive or malicious actions.

Wider Implications

This incident highlights a wider trend of exploitation of inactive or rarely-used accounts. As organisations have increasingly shifted to hybrid models, as well as adopted various Software as a Service (SaaS) solutions, the number of accounts that organisations must manage has grown significantly. Threat actors have been able to exploit this by using accounts that have been overlooked to quickly escalate privileges following a breach and move laterally within the network.

In this incident, the account involved was an old test account that should have been identified and disabled when no longer required. Robust processes should be in place to identify leavers of the organisation, as well as ensure that service accounts or other non-interactive accounts are identified, so that all accounts can either be closed, or privileges reviewed and reduced in line with business requirements.

Organisations Should

- Ensure they are conducting regular reviews of both regular and privileged accounts to ensure the principle of least privilege is being followed and any accounts no longer required are disabled.
- Ensure they have implemented MFA on all accounts. Number matching MFA should be enabled wherever possible. MFA should now be considered a minimum account security requirement, due to its effectiveness in reducing the risk of account compromise.
- Review legacy systems such as on-premise AD that do not support MFA natively. Organisations should consider how they can add MFA support through third party tools, consider migrating to modern systems, or implement alternative conditional access controls.
- Not use weak or easily-guessable passwords. This will reduce the risk of a brute force attack (such as password spray) successfully breaching an account. Wherever available, failed login limits should be applied to accounts to further reduce the risk of brute force attacks.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430