+44 345 094 0945
www.waterstons.com

News article

Mar 2024

US Government Compromised: Cyber Incident Review

US government agency compromised by ex-employee's admin account.

A US government agency has been compromised via an admin account belonging to an ex-employee, whose account credentials had been compromised and made available on the dark web by a previous data breach.

What Happened

The US Cybersecurity and Infrastructure Security Agency (CISA) has released a report into a recent incident targeting an unnamed US state government agency. The attack used the admin account of an ex-employee, that had not been disabled, as the initial infiltration vector. The threat actors obtained the credentials from a previous data breach which had been uploaded to the dark web as part of a large repository of breached accounts. The organisation had not identified the leaked credentials on the dark web and therefore the password had not been changed prior to the recent incident. It is not clear how long before latest attack that the data breach took place. Furthermore, since MFA was not enabled on the account, threat actors were easily able to access it.

Once compromised, threat actors were able to use the account's privileged access to access a virtual SharePoint server and instance of the ex-employee's workstation. They obtained access to a second administrator account stored on the SharePoint server, which also did not have MFA enabled. The second administrator account had privileged access within both the on-premise AD and Azure AD instances allowing the threat actors to spread laterally within the network.

Once the organisation was informed of the breached account credentials online, the account was disabled, and password for the second admin account changed immediately. It is not clear from the report if any data was exfiltrated, or if any other malicious actions were taken by the threat actor.

Wider Implications

This incident is the second this month involving breached privileged accounts that had been left active when no longer required. These incidents, in addition to other high-profile attacks that used breached administrative account credentials, such as the LastPass attack in December 2022, have highlighted the risk posed by poor privileged access Management (PAM). Privileged accounts offer threat actors significant internal access, and the ability to easily spread laterally throughout the network. As threat actors continue to find both traditional and novel methods of breaching accounts, both regular and privileged, organisations are increasingly looking to adopt stricter controls on the use of privileged access, adopting Just In Time (JIT) access control mechanisms, session management tools, and increased auditing capabilities.

Organisations Should

- Ensure all accounts have MFA enabled. Administrative accounts should also have more restrictive conditional access controls applied.

- Implement dark web monitoring to monitor for any breached credentials or data linked to the organisation, so that breached accounts can be identified, and the password changed.

- Ensure they have a robust leavers process in place to ensure all employee accounts are closed on their final day. This should include both regular and administrative accounts assigned to them, as well as the identification and rotation of the credentials of any shared accounts, such as service accounts.

- Ensure they conduct regular reviews of administrative accounts and service accounts to identify any that are no longer required, and that those which are required have the minimum number of privileges, in line with the principle of least privilege.

- Ensure that passwords are not stored in unencrypted locations. Organisations should review the deployment of an enterprise password manager to ensure that all credentials are centrally and securely stored.

- Consider adopting a zero-trust security model which requires all users to only have least privilege access to perform their role, with a special focus on privileged accounts. This will minimise the impact of an account compromise.

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