

News article

Jul 2024

Ex-Employee Wipes 180 Servers After Being Fired

An ex-employee in Singapore has been jailed for using their administrative access to wipe 180 servers, four months after leaving the company.

What Happened?

In October 2022, a Cloud Consultant at National Computer Systems (NCS) in Singapore was fired, however his administrative access was not revoked.

Upset with his termination, the employee left Singapore, but continued to access NCS's systems six times between January 6th and 17th 2023, when he appears to be familiarising himself with the system, exploring possible vulnerabilities, and testing whether his activity would be detected.

In February 2023, the ex-employee returned to Singapore to start a new job, however continued to access NCS systems. They rented a room with a former NCS colleague in Singapore and used their Wi-Fi to login to the NCS network, therefore masking their activity with an employee's legitimate logins. During this time, the ex-employee searched online for scripts that could be used to delete servers one by one.

In March 2023, he launched the cyberattack on NCS, accessing the network and executing scripts, which deleted 180 virtual servers one by one. As the attack occurred over the weekend, the damage was only discovered by NCS on Monday the following week. The estimated cost of the incident and the recovery was over £500,000.

In June 2024, the ex-employee was sentenced to two years and eight months in prison for the cyberattack.

Wider Implications

While relatively uncommon compared to other types of cyberattacks, when malicious insider threats do occur the damage can often be extremely high due to the levels of access employees can possess. Using their extensive knowledge of the company's infrastructure to identify weaknesses in both technology and processes employees are able to carry out damaging attacks. These types of attacks can be difficult to identify since they are usually by an individual working alone, who may not have shown any indication that they would carry out an attack prior to the incident.

The focus for organisations should be on minimising the potential impact of an insider threat as well as the time taken to identify any destructive attacks, by ensuring the principle of least privilege is applied to all administrative access, and that all actions are logged and can be traced back to a user account.

Organisations Should:

- Ensure that they have implemented a leavers process that disables all normal and administrative accounts immediately when an employee leaves, and that the process is regularly audited to validate that all steps have been followed and access has been removed.
- Ensure that the principle of least privilege is applied, so that users only have the minimum access required for their role.
- Ensure that administrative access is appropriately recorded and ensure that system and data owners have the responsibility for performing a regular review of administrative access to ensure access and access levels are appropriate.
- When it comes to service accounts and local administrative access, consider a mechanism to centrally manage the password (such as Microsoft LAPS) so can be easily changed should someone with privileged access leave the organisation.
- Where possible, consider linking administrative access to secondary authentication mechanisms (such as a YubiKey) or implementing controls to restrict the source of any access attempts (such as IP allow lists or conditional access).

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 30+ 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