Australian Government
Australian Signals Directorate

Mitigating the Use of Stolen Credentials

First published: December 2011
Last updated: October 2021

Introduction

An organisation's information is often vulnerable to compromise through the use of stolen credentials. This risk increase when users access sensitive information and services via remote access solutions, including Virtual Private Networks (VPN). This publication explains the risks posed by the use of stolen credentials and how they can be mitigated.

Impersonating a user without their knowledge

Stolen credentials can be used by malicious actors to circumvent security measures which an organisation has implemented to protect sensitive information and services. With these legitimate credentials, malicious actors can impersonate a user without their knowledge.

With legitimate credentials, malicious actors can use remote access solutions to mask their activities and avoid detection. Failure to regularly audit logs from remote access solutions increases the risk and extent of a compromise.

While multi-factor authentication provides an additional layer of security, some implementations are more effective than others. Multi-factor authentication that has not been implemented or configured properly can result in a false sense of security and leave an organisation vulnerable.

Mitigation strategies

The Essential Eight from the *Strategies to Mitigate Cyber Security Incidents* should be implemented as a minimum on networks. However, organisations that allow personnel to access their network via remote access solutions should implement the following additional mitigation strategies:

- Disable LanMan password support and cached credentials on workstations and servers to make it harder for malicious actors to crack password hashes.
- Implement network segmentation and segregation into security zones to protect sensitive information and critical services such as key business systems, user authentication and user directory information. Organisations should assign remote users with a lower level of trustworthiness and limit what they can remotely access on the organisation's network. This includes not allowing direct remote access for privileged accounts.
- Centralise and time-synchronise logging of successful and failed computer events, and conduct regular log analysis. Logs should be stored and retained for at least 18 months. Analysis should focus on network administrators, senior executives and their personal support staff, and network access via remote access solutions.
- Monitor for:
    - remote access credentials being used from two different IP addresses simultaneously

- remote access credentials being used from an IP address that geo-locates to a country that a user is not physically located in
- remote access credentials being used from IP addresses that geo-locate to different countries, where the elapsed time between the VPN accesses is insufficient for the user to have travelled between the countries
- a single IP address attempting to authenticate as multiple different users
- changes to the properties of user accounts, for example, activating the options 'password never expires', 'enable reversible password encryption' or 'no lockout after X incorrect password attempts'
- the re-enablement of previously disabled user accounts or addition of new user accounts.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Further information on the use of remote desktop clients for remote access, including associated risks, is available in the *Using Remote Desktop Clients* publication.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).