(UPDATED) AUGUST 2012

Mitigating the use of stolen credentials to access agency information

1. Australian Government information is vulnerable to compromise through the use of stolen legitimate credentials on agency networks. These risks increase when users access sensitive information and services via remote access solutions, including Virtual Private Networks (VPN). This document is intended for Information Technology Security Advisers and explains the risks posed by the use of stolen credentials and how they can be mitigated.

Adversaries can impersonate a user without their knowledge

2. Stolen credentials can be used by an adversary to circumvent security measures, including multi-factor authentication mechanisms, which an agency has implemented to protect its most sensitive information and services. With these credentials, an adversary can impersonate an agency user without their knowledge, making it difficult to detect any malicious activity.

3. With legitimate credentials, cyber adversaries can use remote access solutions to mask their activities and avoid detection. Failure to regularly audit logs of network access via remote access solutions increases the risk and extent of compromise.

4. 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 your network vulnerable to malicious activity.

Mitigation strategies

5. DSD reiterates the importance of implementing the top four *Strategies to Mitigate Targeted Cyber Intrusions* as a minimum on your agency's network. However, agencies that allow users to access their network via remote access solutions should implement the following **additional** mitigation strategies:

   a. **Disable LanMan password support and cached credentials on workstations and servers,** to make it harder for adversaries to crack password hashes.

b. **Implement multi-factor authentication** for remote access solutions and users such as network administrators, senior executives and their personal support staff, who are most likely to be targeted by cyber adversaries. Ensure that your multi-factor authentication solution is properly implemented and configured for optimum security. When implemented correctly, physically separate tokens and smartcards are the most effective forms of multi-factor authentication, as the adversary requires physical access to the token or smartcard and a user will notice if they are missing. Software based certificates are less effective as an adversary can steal a copy of the certificate without physical access, and without the user noticing.

c. **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. Agencies should assign remote users with a lower level of trustworthiness and limit what they can remotely access on the agency's network. This includes not allowing direct remote access for privileged accounts.

d. **Centralised and time-synchronised logging** of successful and failed **computer events**, with 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; network access via remote access solutions; and, authentication and user credentials, especially from computers other than the user's usual computer. Security staff should also monitor:

(1) remote access credentials being used from two different IP addresses simultaneously;

(2) remote access credentials being used from an IP address that geolocates to a country that the user is not physically located in;

(3) remote access credentials being used from IP addresses that geolocate to different countries, where the elapsed time between the VPN accesses is insufficient for the user to have travelled between the countries;

(4) a single IP address attempting to authenticate as multiple different users; and,

(5) 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'. Other changes to monitor may include enabling previously disabled user accounts or adding new user accounts. Adversaries use these techniques to extend the amount of time that the agency employee's credentials are valid for.

6. Agencies should also ensure that their **password policy** mandates that users select strong, complex passwords, as per the requirements of the *Australian Government Information Security Manual*.

Further information

7. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.dsd.gov.au/infosec/ism/index.htm

8. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies can be found at:

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.