MS-ISAC®

MS-ISAC Security Primer

Exposed Credentials

April 2018, SP2018-0316

The impact of publicly exposed user credentials has far reaching affects, because credential reuse can result in data breaches, system compromises, loss of brand reputation, as well as financial losses. Cyber threat actors (CTAs) take advantage of employee password reuse and employee use of organizational email addresses beyond business purposes to gain access to SLTT government domain account credentials. Some CTAs target login credentials instead of vulnerabilities because it is easier to exploit credentials and gain access to resources through elevated credentials. Credentials with elevated permissions expose organizations to greater risk, allowing for the installation of software or reconfiguration of security controls. If a CTA is able to use elevated credentials, they can access additional hosts, install malware, steal data, and/or disable or modify security controls.

Organizational Recommendations:

If credential exposure is confirmed, triage the incident to ensure the threat is isolated and a data breach has not occurred. Responding quickly and efficiently to determine a data breach or other further compromise has occurred increases network resiliency. The incident response process for stolen credentials should include, but is not limited to the following:

- Enforce a password reset on the compromised account.
- Identify if unauthorized logins, potentially indicated by unusual IP addresses or times, occurred on the network, and if any occurred, reset all passwords on the compromised device.
- Identify and remediate if email rules have been setup on the affected user's email account:
    - Actors maintain persistence access to compromised accounts using deletion rules that conceal variances in sent or received mail for those accounts.
    - Forwarding rules allow for an actor to monitor mailboxes without needing to log into the compromised accounts. However, forwarding rules may inadvertently result in data breaches as additional, potentially sensitive, data can be forwarded.
- Identify high-value accounts and computers that were compromised or affected in the attack, where the compromise may have greater repercussions, such as users with access to sensitive data, including human resource and finance department employees; administrators with access to servers; members of Active Directory Admin Groups; and other accounts with elevated permissions.
- Verify that affected systems are rebuilt using clean builds.
- Where possible, enable two-factor authentication.
- Remind the user to not use their work email address for personal activities.
- Be sure your information security policy prohibits the re-use of network passwords on any third-party accounts, business or personal.

User Recommendations:

- If the exposed account included personal information, such as a Social Security Number, bank account information, or credit card information; further assistance is available through the Federal Trade Commission's Identity Theft website.
- Do not use a work email address for personal use.
- Remember to avoid reusing the exact passwords, or passwords that are similar, as cyber threat actors use techniques to guess similar passwords.
- If a website or account offers it, enable two-factor authentication.
- Consider using an offline password manager to curb password re-use.

TLP: **WHITE** The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/.