ADVISORY FOR ICM SECTORS

Social Media Account Takeover

Original report published on: July 01, 2024[1]

Executive Summary

Social media account takeover attacks are rapidly increasing over the years, compared to other forms of identity theft. These accounts are rich in personally identifiable information (PII), such as a user's real name, email address, birth date, relationship status, physical address, private messages, photos, videos, and feed posts. This valuable data can be used by malicious actors to steal identities or be sold on the dark web for US$25 to US$60 per account, according to the Dark Web Price Index 2023. More insidiously, bad actors can use this information to spy on account owners, post offensive or embarrassing content, blackmail them, or gather intelligence about individuals or organisation.

Background

In 2022, the Identity Theft Resource Center (ITRC), reported receiving four times more inquiries about social media account takeovers compared to 2021, and forty times more than in 2020.[2]

Malicious actors obtain login credentials through phishing, data breaches and dark web. Once they gain access using legitimate credentials, they take control of the account by changing the password or security settings to lock out the legitimate owner. Posing as the account owner, they then conduct malicious activities such as employing social engineering tactics to access trusted circles within the victim's social media accounts.

Social media account takeovers have multiple impact including to businesses and can lead to significant business disruption. In addition, it takes time to remediate and recover system before fully recovery online for end customers.

Detection and Mitigation

IMDA recommends for organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Adopt advanced account security:
    - Use enterprise/paid version of account monitoring and security services.
        - Limit the number of trusted devices that can access the social media account.
        - Retain access audit logs for investigation purposes.
        - Geo-fencing: Have in place device tracking of login attempts and their login location.
- Enable 2FA/MFA:
    - Use Fast IDentity Online 2 (FIDO2) compliant hardware security key.
    - Software Authenticator (e.g. Microsoft, Google)
- Conduct regular security awareness:
    - Emphasise importance of phishing prevention to employees

    - Conduct Social Media Phishing exercise.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	T1589	Gather Victim Identity Information
Resource Development	T1586.001	Compromise Accounts: Social Media Accounts
Initial Access	T1566.001	Phishing: Spearphishing Attachment
	T1566.002	Phishing: Spearphishing Link
Execution	T1204	User Execution
Persistence	T1098	Account Manipulation
Privilege Escalation	T1078	Valid Accounts
Defense Evasion	T1027	Obfuscated Files or Information
Credential Access	T1003	OS Credential Dumping
	T1111	Multi-Factor Authentication Interception
Discovery	T1087	Account Discovery
Collection	T1185	Browser Session Hijacking
Impact	T1531	Account Access Removal

References

1. ^ “Hijacked: How hacked YouTube channels spread scams and malware”
2. ^ “The Weekly Breach Breakdown: Hacked and Furious - The rise in Social Media Account Takeover”
3. ^ “How hackers took over Linus Tech Tips”