Whatsapp Account Hijacking

11th February 2021

Category:
Social Engineering

CTM360 has observed a sudden rise in Whatsapp accounts being hijacked in the MENA Region. In most cases, this occurs through social engineering, in which the victim would receive a Whatsapp message or phone call; they are usually requested to provide verification codes or personal/confidential information. Such disclosure would enable the hijackers to take over their victims' Whatsapp accounts.

Following these occurrences, scammers could then use these accounts to impersonate the victim or even Whatsapp's support team, usually to send suspicious links to unsuspecting users, or further implement social engineering techniques on other potential victims.

THREAT TARGETS:
- General Public
- Public & Private Sector

POSSIBLE IMPACTS:
- Compromise of account credentials & confidential data
- Financial, Reputational and Data loss

TARGET AUDIENCE FOR CIRCULATION:
- General Public
- IT security team
- Executive management & staff

ALTERNATIVE METHODS USED TO HIJACK WHATSAPP ACCOUNTS

Although most attacks occur through social engineering, many scammers had deviated from their traditional methods. Some key examples may include but are not limited to:

Brand impersonation: Big brands may often be targeted, e.g. banks and financial institutions, to display a sense of legitimacy. Threat actors may often use a well-known brand image claiming to be from a reputable company. With a convincing display, it wouldn't take much effort to attain trust and obtain confidential information from victims.

- **High profile Impersonation:** Scammers may often choose to impersonate C-level executives of large, well-known organizations and other well-known influential personalities. Assuming the character of high profile individuals may convey a sense of importance to the victim, and perhaps invoke a sense of urgency to respond and comply with any given requests.
- **Hijacked Whatsapp Accounts:** Scammers may use hijacked Whatsapp accounts to send malicious links or requests to the previous account owner's contacts. Since the contacts are already connected with the victim, the sense of trust may be used to the scammer's advantage.
- **Fake Promotions:** Fraudsters may often send links or messages containing information regarding special promotions on fake E-commerce sites. These sites would often lure their victims into providing their WhatsApp registration codes.
- **Compromising Victims Voicemail Using Default Password:** Scammers may bypass the Whatsapp verification process with the help of the target's voicemail account. This is done when the hacker repeatedly fails the registration code and Whatsapp performs a voice verification by calling the victim directly. By initiating the attack at odd hours, scammers would be able to redirect the message to the victim's voicemail, which the hacker can easily penetrate to recover the audio message. As a result, victims may get their account stolen without even realizing what had happened.

SECURE YOUR WHATSAPP ACCOUNT

WhatsApp users are advised to take necessary precautionary measures to protect themselves from falling victim to attacks. Some of these include:

- Protecting your WhatsApp account by enabling the 'Two-Step Verification' feature; is found under the 'Settings' tab of your WhatsApp application. Users may also enable the option of a backup email address if they wish.
- Changing your default voicemail PIN. Please refer to your respective Telco service providers for information on changing/resetting your voicemail PIN.
- Do not share your WhatsApp account verification codes or any One-Time Passwords (OTP) with anyone. You may receive suspicious messages from existing contacts or strangers via WhatsApp. Do not respond, especially if the sender requests an OTP or code. Also do not click on any links or provide any personal information.
- Verify the authenticity of the messages through alternative means (e.g. calling the contact, online research etc.) If the suspicious messages are from unknown numbers, report the contact to WhatsApp directly.

CTM360's CIRT team has been continuously addressing incidents related to Account Hijacking and Reclamation. If such a case is identified, please contact info@ctm360.com for assistance.

Disclaimer

For more information:
Email: monitor@ctm360.com
Tel: (+973) 77 360 360