iZOOlogic

iZOOlogic Limited
Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com

Case Study: CEO Telegram Account Hacking - World’s Largest Airline

Introduction

This case study details the hijacking of a CEO’s Telegram account causing significant reputational damage to the world’s largest Airline .

Background

Social media messaging services, and chat Apps such as Whatsapp and Telegram, are increasingly used by Executives for business communication which poses a significant risk.

Whilst providing an unparalleled method of instant and global communication, and individuals. Platforms including Facebook, Instagram, LinkedIn, WhatsApp and Telegram, are widely manipulated for fraudulent activities that involve scam through profile impersonation. In this scenario, the chat application Telegram was utilized for account takeover that involved the CEO of the world’s largest airline.

iZOOlogic provides solutions to the world’s largest airline, deploying systems and tools to circumvent malicious attacks directed towards key personnel and executives. The airline has been targeted repeatedly through various cybercrime extending to digital devices such as smartphones through social media applications and chat apps. With the enormous value and assets surrounding the airline, key personnel are well tied to its value, and thus prompting malicious actors to perform fraudulent activities involving the identity key personnel to perform leverage attacks against the airline.

iZOOlogic provides Executive Protection solutions for high profile individuals, such as “C-Level” and Board Members, to protect against impersonation, account take over, Business Email Compromise, and other leveraged attacks.

Types of Social attacks against the Airline

1. The creation of fake social media accounts impersonating key personnel and executives. These accounts are used to look and act like the legitimate person. These fake social media profiles not only victimize unsuspecting executives but specifically target customers of the corporation for the sole purpose of attaining vital information. This leads to scam incidents extracting large amounts of money from the corporation.

2. The distribution of malicious malware links via targeted impersonated social media accounts and chat accounts utilizing the airline’s name and brand. These links directed the airline’s existing and potential customers, to download malware on their devices, in an attempt to steal login credentials.

3. The distribution of ‘fake news’ via social media platforms to propagate false information (in an attempt) to deliberately influence the share price of the airline. Such an attack would have resulted in widespread impact across several financial markets around the world and potentially penalizing the airline.

4. The distribution of false documents and materials in the executive’s name. Such documentation including “Statements of Financial Condition” could be released via social media platforms through impersonated accounts of key personnel or senior management profiles thus giving them credibility.

5. Account Hijacking and Identity Theft is an attack involving social engineering techniques aiming to reach the targeted personnel by attempting to steal the account to gain access to current contacts. Successfully hijacked accounts pose a critical risk because once the attack becomes successful this could lead to further attacks targeting the contacts for financial gain. Information gained by the attacker could be sold to various criminal networks to plan the next attack.

Issues Encountered

- The Telegram account of the Airline's CEO was hijacked through social engineering techniques involving a two-factor authentication breach.
- Contacts of the CEO were directly contacted by the hijacker posing as the CEO.
- The criminal took over the account by setting up a different recovery address and effectively changing the phone number attached to the account.

Challenges

- Telegram's support group including their abuse team are made up of volunteers who have intermediate availability.
- Response from their support team will vary depending on their availability.
- The abuse team and support team are not publicly advertised, thus difficult to search for an active support line.

Resolution

- iZOOlogic's team of analysts utilized existing relationships with Telegram's abuse team.
- iZOOlogic sought the cooperation of top-level management of Telegram.
- iZOOlogic through the cooperation of Telegram's management team was able to disable the account hijacked by the threat actor in less than 4 hours effectively halting the threat actor's fraudulent activities.
- Top-level management of Telegram prioritized the resolution of the incident by effectively reversing all actions done by the threat actor through their abuse team performed in less than 12 hours.
- Hand-in-hand offered walkthrough assistance that resolved the matter with the airline's CEO InfoSec team on account recovery.

Conclusion

The impacts resulting from a hijacked social media profile and/or chat application profile could be more critical than a network breach. Criminals are actively evolving by creatively launching different types of attacks including account takeover, impersonation and identity theft accompanied by spear-phishing techniques through different channels such as social media platforms and chat applications. In this case, a potential financial loss was prevented by a rapid proactive and reactive approach from our team.

Corporations must safeguard their key personnel across disparate platforms, not only in social media but through applications that have a social reach. Impersonation may lead to loss of financial assets and reputational damage not only to the executive impersonated but to the whole corporation itself. Reputational damage is intangible and will have a domino effect as a whole.

iZOOlogic offers an evolving suite of tools and solutions to keep key personnel, executives, brand, and corporation safe across all social media platforms and digitally visible platforms similar to social media.

iZOOlogic

iZOOlogic protects the world’s leading organisations, across Banking, Finance, and Government.

The iZOOlogic platform provides real time Threat Intelligence and a seamless Global Security Response.

iZOOlogic helps organisation's manage Digital and Reputational Risks, and to reduce fraud and revenue losses.

To learn more, visit www.izoologic.com or ***Contact Us***

HQ / EMEA OFFICE

Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com

US OFFICE

Level 1, 444 Castro Street
Mountain View, California,
USA
+1 650 396 3352
sales@izoologic.com
www.izoologic.com

APAC OFFICE

Suite 18, Level 27, Rialto Tower
Collins Street, Melbourne, 3000,
AUSTRALIA
+61 3 9088 0338
sales@izoologic.com
www.izoologic.com

iZOOlabs / GSOC

Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com