CYBER ATTACKS: ANALYSIS OF A REAL-WORLD INCIDENT

Title: Compromised Employee Credentials and Widespread Bitcoin Scam on Twitter (July 2020)

Author: Sylvanus Egbosiuba Chinedu, MSc Big Data Technology

Date: 31st May 2024

Introduction

This document provides an in-depth analysis of the security breach that transpired on Twitter on July 15, 2020. The incident involved unauthorized access and control of several prominent accounts, intrusion into direct message inboxes, and extraction of Twitter data, leading to significant security compromise and damage to the platform's reputation. The report further explores the causes behind this incident, potential measures that could have been implemented to address or lessen the vulnerabilities, and recommendations to avert similar incidents in the future.

Twitter, a social media platform, allows users to create accounts using email and personal details. It offers account verification for notable entities and individuals to ensure content authenticity. Users can share information on their timelines, follow other accounts and hashtags, and engage through likes, comments, and retweets. This report will consistently use the name 'Twitter' for clarity, despite the company's recent rebranding to 'X'.

Incident Overview

Types of attack: Phone Spear phishing attacked and social engineering

Initial Discovery: login credential of some employees with access to administrative support tool were compromised between 14-15th July, 2020 leading to multiple account hijack and wide-spread of scam bitcoin misinformation on twitter, by mid morning on the 15th July 2020 signs of attack were reported as several employee notified the internal fraud monitoring of social engineering attempt. These incident was fully identified on the same day at about 3:13pm ET when the first bitcoin scam tweet was tweeted to the public.

In general, this led to 130 accounts users being compromised, leading to attackers tweeting from 45 accounts of these accounts, accessing 36 accounts direct message inbox, and 8 unverified accounts "Your Twitter Data" being downloaded.

Immediate actions taken: At around 6:18pm ET the same day, twitter blocked all verified account from sending tweets and restricted accounts that had password reset the previous week. Internally, twitter logged off

all employee off the internal VPN, this was done in batches. Every employee was required to login to a secure environment with zero trust, starting from the company's CEO.

Incident Analysis

Who was affected: There is no clear number of how many twitter employees were targeted by the social engineering/ phone spear phishing attack and it is not clear how many employee details were compromised from the incident. It is certain that some employee details were compromised which enabled human vulnerabilities to be exploited.

However, this led to data breach of 130 twitter accounts, the following persons were among the known affected public figures who were victims of this attack; Barack Obama, former President of America and second highest follower on twitter, Joe Biden, currently President of America and president candidate at the time of the incident, Elon Musk CEO of X and CEO of Tesla, Jeff Bezos CEO of Amazon, Bill Gate Founder and former CEO of Microsoft Inc., Kim Kardashian and Kanye West both America's media and entertainment personalities. Also Tech company like Apple, Binance, Uber, etc., were also affected as all of the listed accounts and more were used to spread the bitcoin scam tweet.

Nature and type of cyber attack

The attack on the 15th July 2020, originated from a successful phone phishing/social engineering were the cybercriminal exploited human vulnerability. From investigation, the penetration started on 14th July 2020, attackers at the stage of reconnaissance gathered information about the organization staff by scraping through LinkedIn using a paid feature for the recruiter to get their personal contact details. when twitter employee contact detail were obtained, the attacker delivered social engineering attacked on twitter by calling up employee in the Consumer service unit, claiming to be calling from the organization's IT helpdesk department. Though some twitter employees reported the social engineering attempt to the internal fraud monitoring team. They were still able to convince one or more employees to access the fake VPN phish page and input authentication details on a false login which made it possible for the hacker to use the credential in real time to log into the real VPN and the first level penetration was established. However, the attacker could not Command and control the level of privilege needed to launch the desired attack because the access gain was for low-level employees who did not have access to the internal administration tool, but the attacker had access to the system to study the procedure and gain internal knowledge.

On 15th July the attacker were able to launch a more sophisticated attacked on the employee in Tech support unit who had access to the internal administrative tool which their credential were also used real time by the attacker jump the two factor security to access the system that allowed them to target 130 account, send out tweets from 46 accounts, accessing 36 DM and 8 your Twitter data.

The cybercriminal initiated their scheme by commandeering the profiles of 'Original Gangster' (OG) Users, which are distinguished by their succinct usernames, often just one or two characters in length. Following the infiltration of these OGUser accounts, the perpetrators then proceeded to market the stolen accounts and moments later, the hacker brought the attack public by taking over high to push a cryptocurrency scam, a known cryptocurrency trader's twitter accounts "@AngeloBTC" and Binance were hacked and used to push for a paid telegram group promising to post their active trader signal to the telegram group member and sending bitcoin wallet link to twitter user for payment via DM.

Severity of the cyber attack

The cyber attack, despite originating from a low-skill technique, resulted in significant consequences due to the high exposure and the number of individuals and entities affected. Consequently, it has been designated as a high severity incident. The section elaborates on the impact.

High-profile account targeted: A notable aspect of the attack was the compromise of 130 accounts belonging to prominent figures, which were then used to disseminate a Bitcoin scam. These accounts span a variety of influential sectors including politics, entertainment, business, and technology. The potential ramifications of this breach could have escalated to severe global political conflicts and market disruptions.

Financial scam: The financial aspect of the attack was aimed at promoting a Bitcoin scam, which led to Twitter users incurring losses exceeding $118,000.

Social media volatility exposure: The incident also exposed the susceptibility of social media platforms to penetration and manipulation through social engineering, underscoring the potential for more advanced future attacks given the equation **"Attackers' gain > Cost of attack."**

Reputational damage: Furthermore, the attack has inflicted reputational damage, undermining the trust users place in the protection of their data and the veracity of information shared on Twitter and other social media platforms. This loss of confidence was mirrored in the financial markets where Twitter's stock value dropped by 4% on the day of the attack.

Threat actors and their motives

The incident in question involves cybercrime staged by four individuals: Joseph James O'Connor, identified as the mastermind, alongside Graham Ivan Clark, who at 17 years old served as the co-conspirator, Mason John Sheppard, and Nima Fazeli. Three of the suspects were apprehended on July 31, 2020, while O'Connor was detained in August of the same year.

The attack was financially motivated, prompting swift action from 15 cryptocurrency firms following directives from the Department of Financial Services (DFS) to block the fraudulent wallet. This intervention prevented around 6,031 transactions totaling approximately $1,347,050. Despite these measures, the scam managed to accrue over 320 transactions, amounting to roughly 12 bitcoins valued at approximately $118,000 at the time of the incident, with about $61,000 extracted from the wallet.

Given the prominence of the victims and the significant access the hackers gained during the breach, it's evident that the incident had the potential to inflict more than just financial losses and damage to the Twitter's reputations.

Indicators of Compromise (IOCs)

By the time mid-morning arrived on July 15, 2020, evidence of the attack had emerged. A number of

employees alerted our internal fraud monitoring team about unusual activities, suggesting that there might be an attempt at social engineering underway

The initial significant signs of the system breach crystallized when multiple original gangster accounts (OG Users) had been compromised and a deceptive tweet from Binance was detected at 3:13pm ET This events unfolded after reports from some members of the Twitter Consumer and Tech support team regarding a Phone phishing attack to the internal fraud monitoring unit.

The employee report served as a valuable signal for the potential breach, prompting the immediate commencement of preventative measures. Such measures may include tracking of activities from unregistered system IP addresses within the organization's VPN. Additionally, deploying an organization-wide alert through pop-up notifications and emails detailing the correct reporting procedures in the event of a compromise is advisable.

Compromised security elements (C.I.A. Triad)

Confidentiality Breach: The incident resulted in the exposure of employee login information and allowed the attacker to obtain unauthorized access and control over various account profiles, personal demographic information, private direct messages, and "Twitter Data" (YTD). Additionally, the intruder was able to post tweets from the compromised accounts.

Integrity: The significant breach of information integrity happened when data from 130 accounts were exploited to propagate a Bitcoin scam, with the perpetrators masquerading as the account owners. The attacker manipulated the email addresses linked to these profiles, facilitating a password reset and subsequent unauthorized access. Notably, many of the individuals targeted in this incident were high-profile public figures of global renown.

Availability: During the period of the incident, every user impacted was unable to log into their account, preventing access to their profiles, the ability to post content, or engage in communication with fellow users.

Authenticity: Throughout the duration of the Twitter account breach, the ability to confirm the authenticity and origin of the information was compromised. The content disseminated from the hijacked account reflected the perspectives of the impostors, rather than the legitimate account holders. This led to a dissemination of unverified and potentially misleading information under the guise of trusted sources.

Exploited Vulnerabilities

The organization's operational structure necessitates the provision of specific administrative services to its clients, crucial for maintaining account integrity and operability. These include account modifications, verifications, and profile email updates/changes, managed through a dedicated administrative instrument known as the "agent tool."

The COVID-19 pandemic led to a significant shift in global working dynamics, including at Twitter. In response, Twitter implemented a remote work policy, enabling most staff to work from home using an internal VPN to securely access necessary support tools, including the administrative agent tool.

Commonized issue: Twitter's inadequately prepared remote working system faced frequent VPN-related network issues. Hackers exploited these issues by contacting employees under the guise of the IT department, convincing them to log in through a fraudulent phishing page.

Poor security awareness/Human vulnerability: Social engineering attacks rely on deceiving individuals into surrendering their credentials. The incident revealed that several Twitter staff members lacked sufficient security training, and the company did not regularly conduct tests for social engineering vulnerabilities or phishing drills.

Lack of swift response to security issue: The internal fraud monitoring department did not promptly address a security alert from employees. Records show no measures were taken in response to alerts issued after unsuccessful social engineering attempts. Implementing a block on staff password resets and preventing logins from unregistered system IP addresses could have reduced the chances of a successful cyber attack.

Affected systems, data, or users

VPN and Agent tool: Employee VPN access and the agent tool's login details were exposed, allowing the intruder to take over the system.

Client sensitive data: During the occurrence of this event, approximately 130 accounts were affected through various methods, putting every Twitter user in risk of having their personal information compromised and made public.

Lessons Learned

This section will explore the insights gained from the incident and recommend measures to strengthen the organizational security structure to prevent similar events in the future.

Awareness training and Penetration testing: Training in security awareness and conducting penetration tests are crucial, as this incident underscored the significance of every employee's role in maintaining security. Such initiatives highlight how inexpensive social engineering tactics can tarnish an organization's reputation. To mitigate human-related risks, it is essential for Twitter to:

- Amplify investment in employee training to recognize the hallmarks of cyber threats such as social engineering and phishing.
- Ensure employees adhere to security protocols, including distinguishing between authentic and fraudulent organizational webpages.
- Implement regular penetration testing to maintain security consciousness among employees, with additional training for those who do not meet the standards.
- Maintain a confidential and always-available incident reporting channel.

Access Privilege: To modify user accounts, a more stringent standard procedure is required to ensure they

undergo multiple levels of checks, including modification and verification controls. Once any changes have been made to accounts, a high-level employee must approve the verification of the account profile changes.

Improve Detection risk control: The breach originated from a hacker's system, differing from the addresses on record for the affected employees. Consequently, Twitter must enhance its detection mechanisms. The improved system should.

- Detect sign-in attempts from any device whose IP address is not listed in the company's records.
- Alert when the company's VPN is accessed from an IP address or location that does not match the employee's registered details.
- Block access to the company's data if there's a discrepancy between the IP address or location and the employee's registered information.

Priority Security: At the time of the security breach, Twitter had deprioritized security measures, evidenced by the absence of a Chief Information Security Officer (CISO) for almost half a year leading up to the incident. Despite reports of social engineering activities made to the internal fraud monitoring team, Twitter prioritized maintaining service availability over a temporary shutdown to address security vulnerabilities. This decision was supported by the lack of capacity for such action, as confirmed by the Chief Technology Officer, Parag Agrawal.

Conclusion

The July 2020 Twitter hack emphasizes the critical need for strong information security and the severe consequences of its failure. This attack, using simple social engineering, exploited human and system vulnerabilities to great effect. It impacted high-profile figures across various sectors, revealing the fragility of our global digital infrastructure.

This event highlights the need for ongoing cybersecurity investment, including better employee training, strict access controls, and advanced threat detection. The consequences—financial losses, damaged reputation, and potential misinformation spread—underscore the importance of a proactive, comprehensive approach to digital security.

Organizations must prioritize cybersecurity, implement robust protocols, and ensure quick, coordinated responses to threats. This breach eroded public trust, affected stock markets, caused financial losses, and demonstrated the true cost of neglecting cybersecurity. In our interconnected world, a vigilant, prepared, and responsive security stance is crucial to protect information integrity

References

Twitter Investigation Report (no date) *Department of Financial Services*. Available at: https://www.dfs.ny.gov/Twitter_Report (Accessed: 4 June 2024).

Support [@Support] (2020) 'We are aware of a security incident impacting accounts on Twitter. We are

investigating and taking steps to fix it. We will update everyone shortly.', *Twitter*. Available at: https://x.com/Support/status/1283518038445223936 (Accessed: 4 June 2024).

BBC News (2020) 'Twitter hack: What went wrong and why it matters', 16 July. Available at: https://www.bbc.com/news/technology-53428304 (Accessed: 4 June 2024).

BBC News (2020) 'Twitter hack: Staff tricked by phone spear-phishing scam', 31 July. Available at: https://www.bbc.com/news/technology-53607374 (Accessed: 4 June 2024).

Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others | CNN Business (no date). Available at: https://edition.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html (Accessed: 4 June 2024).

Goldman, J.V., David (2021) *Massive internet outage: Websites and apps around the world go dark | CNN Business*, *CNN*. Available at: https://www.cnn.com/2021/06/08/tech/internet-outage-fastly/index.html (Accessed: 4 June 2024).

Thompson, N. (no date) 'How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One', *Wired*. Available at: https://www.wired.com/story/inside-twitter-hack-election-plan/ (Accessed: 4 June 2024).

Witman, Paul D. and Mackelprang, Scott (2022) "The 2020 Twitter Hack – So Many Lessons to Be Learned," Journal of Cybersecurity Education, Research and Practice: Vol. 2021 : No. 2 , Article 2. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/2

'2020 Twitter account hijacking' (2024) *Wikipedia*. Available at: https://en.wikipedia.org/w/index.php?title=2020_Twitter_account_hijacking&oldid=1224672151 (Accessed: 4 June 2024).