ON-DEMAND INTELLIGENCE ALERT

CyberLAB Africa | NG Desk

Massive Twiter Social Media Account Take Overs

CYBERLAB

INTELLIGENCE & RESEARCH

Twitter was thrown into chaos on Wednesday, July 15th, 2020, after accounts for some of the world's most recognizable public figures, executives, and celebrities started tweeting similar bitcoin addresses where people are required to pay into for double returns. It was later discovered that the accounts were compromised, and the information shared in the tweets about the double returns was a scam that many unsuspecting individuals fell for.

The breached Twitter accounts were observed to be all verified twitter accounts with over 10million followers each, to the right is a table showing the compromised accounts and their handles.

The accounts stated were seen tweeting similar messages about giving back to the community which required individuals to make payment to specific bitcoin accounts and get double the amount back within a stipulated time frame. Screenshots below show sample tweets.

List of Hacked Accounts

Kim Kardashiam West - @KimKardashian	Warren Buffet- @WarrenBuffet
Ye- @Kanyewest	Binance - @binance
Mike Bloomberg- @MikeBloomberg	CashApp - @CashApp
Jeff Bezos - @JeffBezos	Wiz Khalifa @wizkhalifa
Bill Gates - @BillGates	Joe Biden @JoeBiden
Floyed Mayweather - @FloyedMayweather	TRON Foundation - @Tronfoundation
Elon Musk - @elonmusk	Apple - @Apple
KUCOIN - @kucoincom	Barack Obama - @BarackObama
Uber - @Uber	

Preview of some Hacked Accounts

Figure 1a: Jeff Bezos

Figure 1b: Barack Obama

Figure 3: Apple's compromised tweet

Figure 2: Mayweather's tweet

Two bitcoin wallets were identified to be used in the attack which are:

- **bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh**
- **bc1qwr30ddc04zqp878c0evdrpfx564mmf0dy2w39l**

As at the time of this report, and over the past 24 hours the account had processed 380 transactions and received almost 13 bitcoins — or approximately USD 117,079.

After conducting an investigation which is still ongoing, a statement was released by Twitter support disclosing the incident was due to a coordinated social engineering attack, which targeted some of its employees with access to internal systems and tools.

Insights gotten from other posts related to this breach inferred that the Twitter employee whose access was breached may have been bribed (although this is yet to be verified) by hackers to give access to the internal panels. Screenshots were provided by Data breach, monitoring, and prevention service, which shows the panel access to some of the hijacked social media accounts, shown in figures 6 and 7.

A hacker who went only by "Kirk" was said to be the central player in this attack. They also suggested that Kirk initially gained access to Twitter's admin panel by first getting into a Twitter employee's Slack account. More details are sure to come out in the coming days; the FBI is investigating, and Twitter has said it will share the results of its ongoing investigation when there is progress.

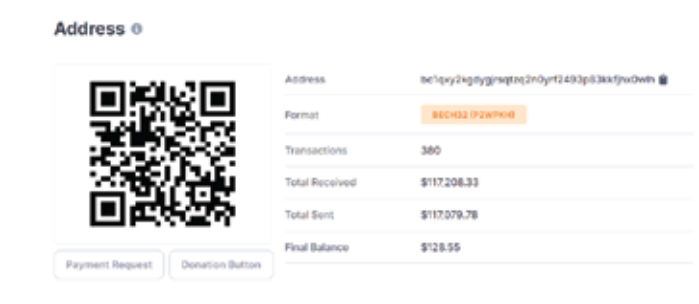

Figure 4: Total amount sent to the Bitcoin account

Figure 5: Twitter's official tweet about the incident

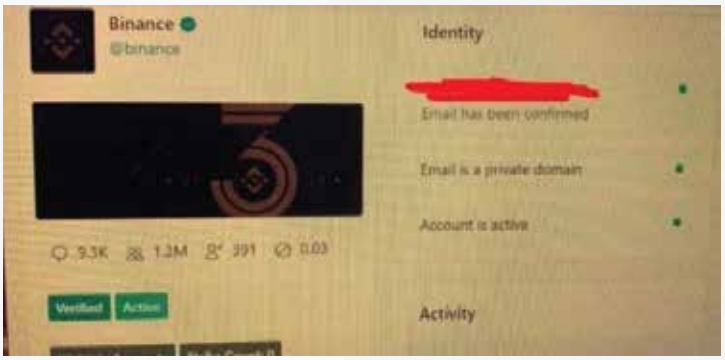

Figure 6: A screenshot showing the panel's access to Binance

Figure 7: Screenshots of another user panel

CYBERLAB
INTELLIGENCE & RESEARCH

SIMILAR ATTACKS IN NIGERIA

CyberLAB has observed an increase in cyber-attacks on organizations and its executives' social media accounts in Nigeria. In June 2020, we identified 5 take over cases of Nigerian Enterprises, this type of attack usually involves several attempts by malicious actors to guess the password of the particular social media account or the use of orchestrated social engineering activities to obtain social media passwords, we also can verify there is an increase of chatter in SIM SWAP NIGERIAN underground groups.

Once one of the methods is successful, the attacker proceeds to change details of the account in order to avoid the victims taking back the control of their accounts.

Attacks like this if successful, can cause severe reputational damage to the affected organization and financial loss to unsuspecting victims. Unauthorized access to any organization or VIP's social media account can also be used to plan and perform large scale cyber-attacks, fraudulent activities, phishing, etc as can be seen in the Twitter incident.

CYBERLAB
INTELLIGENCE & RESEARCH

RECOMMENDATIONS

Below are some recommendations which have been inferred from similar attacks in Nigeria, which should serve as a guide and be adopted for various organizations and their executives.

- The use of a strong password for accounts.

- Organizations should manage separate passwords for each social media account.

- Organizations must ensure implementation of multi-factor authentication on social media accounts.

- Use of password managers to store passwords and do not store passwords in clear-text.

- Use a dedicated SIM card that belongs to the organizations for multi-factor authentication, not use a personal SIM card.

- Password reset email in use should be company email, not personal email.

- Awareness should be done for all PR and corporate communications teams to ensure they are aware of such attacks.

- The organization should be notified as soon as possible when password reset emails are received, monitor email password reset alerts.

- Subscription to a threat intelligence service that covers brand protection which includes Impersonation, typo-squats, positive and negative mentions on social media, etc.

CYBERLAB
INTELLIGENCE & RESEARCH

CyberLAB is leading the revolution in threat intelligence in Africa. CyberLAB's mission is to monitor and alert users of immediate risk using a tactical approach; We gather massive amounts of data using various sources such as publicly available web-references, social media channels, and the deep dark web using a wide range of honey-pot techniques. CyberLAB Africa is modular and supports both large and growing companies requiring threat intelligence services.