Dahir Abib

Binance Security Breach Report

Table of content

Report summary

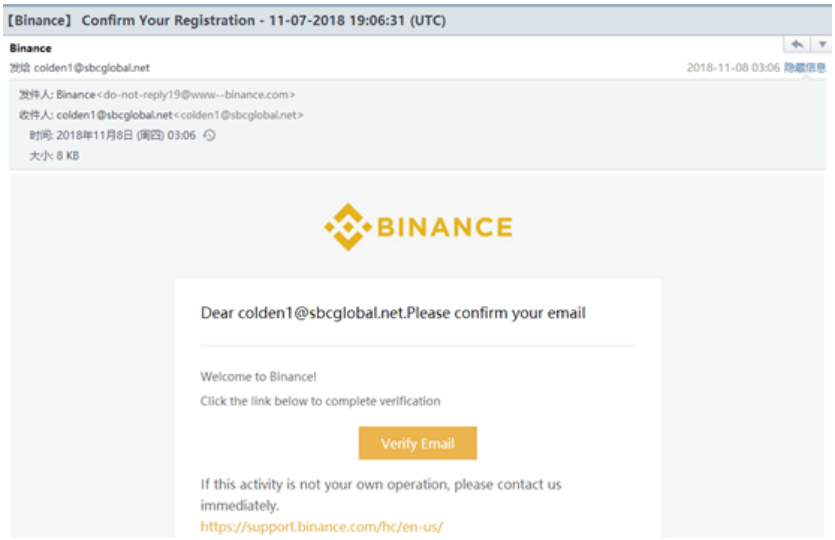
Binance, the number one crypto-currency exchange in the world amassing 28.6 million users sounds secure right? On May 7th, 2019, Binance suffered a large-scale security breach where hackers were able to steal many API keys and 2FA codes. With that and a variety of attack methods such as phishing and viruses, the hackers were able to withdraw 7,074 bitcoins totalling £30.2 million from two addresses into 44 bitcoin addresses through a single transaction. First I will show the transaction hash showing the withdrawal of bitcoins from one of Binance's 'hot wallet'. A definition of a 'hot wallet' is any cryptocurrency wallet connected to the internet. The transaction hash is **e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea**.

As some of us may know, blockchain technology is a decentralised, digital ledger of transactions that records information that is near impossible to change or hack. The transaction hash above in bold can be searched on websites such as 'blockchain.com/explorer ' which is public to everyone and has information such as historical prices, most recent transactions, mined blocks and can also purchase digital assets from. I've written a report explaining who was behind the attack, what was taken, when it happened, how they did it and why. According to Binance, it is said to have awarded a team of 'investigators' for identifying the perpetrator. The cryptocurrency exchange didn't externally put a team together but offered a £188,500 reward for any information leading to the arrest of the hackers. Binance's CEO, Changpeng Zhao (CZ), confirmed that the culprits have been identified and are currently being pursued. The US Department of Justice have been pursuing the hackers however they remain at large. CZ confirmed that 7074 bitcoins were stolen which is 2% of their total BTC holdings in one transaction and has been transferred to an unknown wallet. Verified accounts were also hijacked and unauthorised withdrawals were completed however CZ has kept his promise of covering the incident in full using their safety funds for scenarios such as this one.

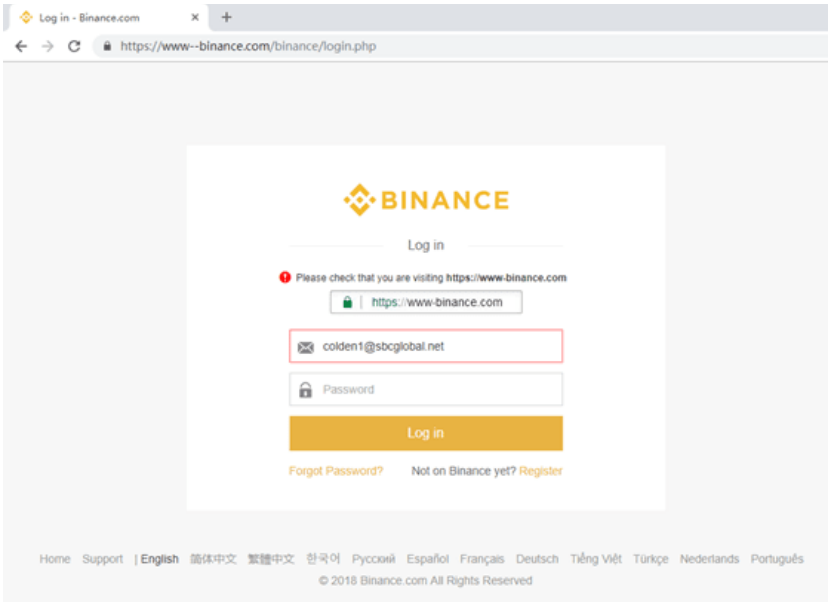
The date of the attack was on the 7th of May 2019 and was stolen from a 'hot wallet' which is a cryptocurrency wallet connected to the internet. Any wallet connected to the internet always has a security flaw and that is one of the main reasons crypto fanatics always say to take your crypto off exchanges and into cold storage; that being on paper or a hardware wallet. The cold wallet stores user's addresses and private keys which are compatible with legitimate software on the computer and works in conjunction with blockchain technology. Looking into the attack and analysing how they did it, I can confirm the initial access point was done in two ways, phishing and accessing valid accounts. The phishing stole a total of 74 bitcoins whilst the remaining were compromised via user application programming interfaces which are known as API keys and 2FA codes. This enabled the hackers to access the company's hot wallet and cipher 7,000 bitcoins to external wallets.

Initial access

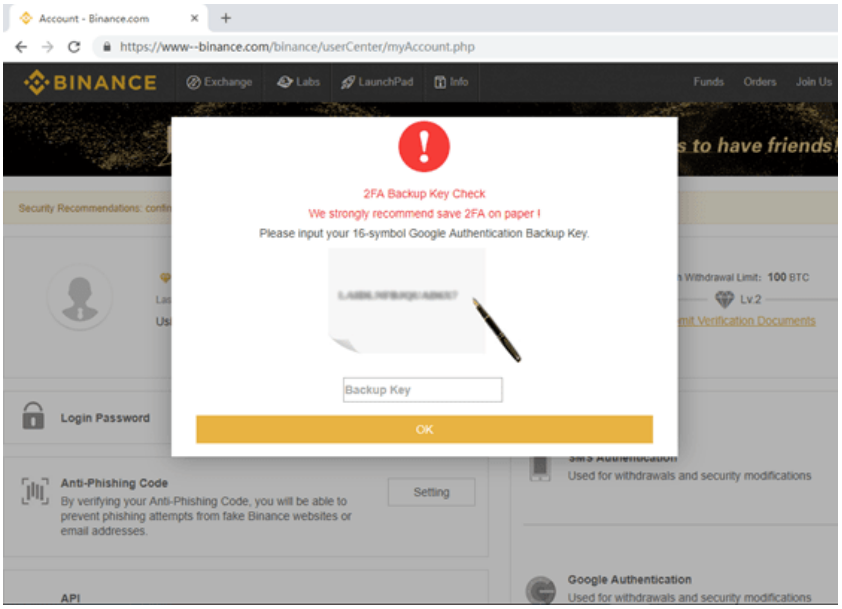
Phishing is a type of social engineering attack created by hackers to obtain sensitive information. In this case the phishing email was disguised as a Binance communication email to mimic it as one of their own. Below I've attached a real phishing email sent out to users to obtain their details. The email itself was sent from ‘do-not-reply19@www--binance.com’ which isn't the legitimate email address.



Some users may be quick to notice that it is a phishing email however some don’t and click the ‘verify button’ which leads to another page. This other page leads to a PHP page which is written in HTML and is used to create dynamic web pages such as this



The victims will fill in their details and after clicking login the hackers will have prepared a window which will look something like this.



The hackers will have prepared a sophisticated php page which will prompt the user to input their 2FA code to 'verify' it. This is not genuine, but some victims still disclose this without delay. Just like that the hackers have obtained 2FA codes, username and password to gain full access to the victim's account.

Using this sophisticated method of phishing they were able to acquire valid credentials to log in to existing accounts and drain funds to external wallets. The other way they were able to withdraw the remaining 7,000 was accessing the company's hot wallet via api keys and two-factor authentication. The way they were able to access the API keys was that some users use web-based wallets which have a lot of security flaws against them. They're trusting third parties with very opaque terms of service and privacy policies to govern their digital accounts and letting them be preyed on; removing the decentralized aspect of blockchain technology. Hackers were able to scoop up tons of details and put them together to have all the information to log in as the user. There have been multiple attempts to rid centralised web-wallets and the closest thing to an answer is Web3.0 Web 3.0 is the decentralized web which will eradicate problems like this and bring security back to digital assets. Users will be able to interact with their wallets, people and businesses without worrying about their data being infiltrated.

This attack was a well thought and calculated attack where scheduled transactions were completed to mimic typical exchange behaviour and bypass the security firewall. A very interesting finding was that the hackers placed the funds in SegWit wallets which create some sort of legal ambiguity against them so eventually when they have been caught it may be difficult to pin the theft to them. The discovery of Binance's hot wallet is still a mystery as they are not sure how it was accessed. System location discovery may have taken place when the hacker attempted to get detailed information about the operating system the company was using including versions, patches, seed phrases or even wallet addresses.

Prevention and Remediation

Prevention from cryptocurrency hacks is quite different from user and exchange. Below I will explain the key security control you will need to prevent these types of attacks. For the user being vigilant and always having an eye for detail. Phishing emails are more and more common so always read where the email is coming from as that is a sign. Don't press links via emails too as you might download a trojan not knowingly. With regards to having a safe and secure account make sure there is 3FA set up; and email code will be sent out, a one-time passcode will be sent out and you would need google authenticator to verify yourself. If a hacker has accessed your email and stolen you're the one-time passcode from your number you still have your last line of defence which is the google authenticator. The google authenticator is a mobile security application based on two-factor authentication which allows users to very themselves before granting them permission to use websites or services. If you have more then £10,000 in you exchange and you plan on keeping your crypto for a period, it is highly suggested to offload your digital assets and keep them in external wallet as this is more secure and keeps your protected if anything happened to the exchange. It is your own responsibility once your transfer out your digital assets to an external wallet as you are not covered by the exchange's insurance program.

As for exchange their best option would be keeping all their holding in cold storage as hackers won't have any access to them because they are not connected to the internet. Perhaps in web 3 when a decentralized internet is about companies and people may be able to keep their assets online.

Att&ck Analysis

Initial access	**(T1566.001/2) Phishing** Spearphishing (attachment/link)	**(T1078) Valid Accounts** Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access
Persistence	**(T1053) Scheduled Task/Job** A task can also be scheduled on a remote system, provided the proper authentication is met	
Discovery	**(T1082) system location discovery** A Hacker may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.	**(T1087.003) email account** Attempt to get a listing of accounts and email addresses to access funds. **(T1049) system network connections discovery** may attempt to get a listing of network connections to or from the compromised system they are currently accessing
Exfiltration	**(T1029) scheduled transfer** Hackers may schedule data exfiltration to be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.	**(T1567) over web service** Hackers may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise.
Command & Control	**(T1071.003) mail protocols)** communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic.	**(T1001.003) protocol impersonation** may impersonate legitimate protocols or web service traffic to disguise command and control activity and thwart analysis efforts. By impersonating legitimate protocols or web services, adversaries can make their command and control traffic blend in with legitimate network traffic.

Referencing

1. **Cybercrooks steal $40m in Bitcoin from crypto-exchange Binance, 2021**
   The Daily Swig | Cybersecurity news and views. 2021. *Cybercrooks steal $40m in Bitcoin from crypto-exchange Binance*. [online] Available at: <https://portswigger.net/daily-swig/cybercrooks-steal-40m-in-bitcoin-from-crypto-exchange-binance> [Accessed 5 December 2021].

2. **Hackers stole $40 million from cryptocurrency exchange Binance, 2021**
   CISO MAG | Cyber Security Magazine. 2021. *Hackers stole $40 million from cryptocurrency exchange Binance*. [online] Available at: <https://cisomag.eccouncil.org/hackers-stole-40-million-from-cryptocurrency-exchange-binance/> [Accessed 6 December 2021].

3. **Binance awards $200,000 bounty after cyber-attackers indicted in US, 2021)**
   The Daily Swig | Cybersecurity news and views. 2021. *Binance awards $200,000 bounty after cyber-attackers indicted in US*. [online] Available at: <https://portswigger.net/daily-swig/binance-awards-200-000-bounty-after-cyber-attackers-indicted-in-us> [Accessed 6 December 2021].

4. **NAST, C.**
   Hackers Stole $40 Million From Binance Crypto Exchange
   (Nast, 2021)
   Nast, C., 2021. *Hackers Stole $40 Million From Binance Crypto Exchange*. [online] Wired. Available at: <https://www.wired.com/story/hack-binance-cryptocurrency-exchange/> [Accessed 6 December 2021].

5. **ZHANG, C.**
   Binance Security Breach Update
   I (Zhang, 2021)
   Zhang, C., 2021. *Binance Security Breach Update*. [online] https://binance.zendesk.com/. Available at: <https://binance.zendesk.com/hc/en-us/articles/360028031711-Binance-Security-Breach-Update> [Accessed 6 December 2021].

6. **RUSTGI, N.**
   Why Did Binance Hackers Transfer Bitcoins into SegWit Addresses Only?
   In-text: (Rustgi, 2021)
   Your Bibliography: Rustgi, N., 2021. *Why Did Binance Hackers Transfer Bitcoins into SegWit Addresses Only?*. [online] CoinGape. Available at: <https://coingape.com/why-binance-hackers-steal-bitcoin-segwit-address/> [Accessed 5 December 2021].