OTP bots and crypto: A tactic to disrupt

Received (in revised form): 4th November, 2022

Kristen Spaeth
Senior Investigator, Coinbase, USA

Kristen Spaeth is a Senior Investigator on the Global Intelligence team at Coinbase, where she works on investigations in coordination with law enforcement to keep criminal activity off the Coinbase platform. Prior to joining Coinbase, she was a Senior Cybercrime Analyst in the Cybercrime and Identity Theft Bureau at the Manhattan District Attorney’s Office. She has been the investigative lead on numerous complex long-term investigations involving identity theft, money laundering, terrorism financing, bank fraud, network intrusions and enterprise corruption. She holds a MSc in criminal justice from Long Island University, Post Campus.

E-mail: kristen.spaeth@coinbase.com

Abstract  One-time password (OTP) bots are a form of crimeware-as-a-service that is being used to bypass two-factor authentication (2FA) on victim accounts. The bots are operated through Telegram and are sold at various price points in exchange for cryptocurrency. The bot operators facilitate a false phone call to victims, impersonating their financial institution, to obtain their OTP to commit an account takeover. Account takeovers facilitated by this type of social engineering are an enormous threat to financial institutions due to the inability to identify the attack without secondary corroboration. This paper illustrates the typical workflow of an OTP bot, avenues of institutional platform investigation and detection, as well as potential mitigation options to combat OTP bot attacks.

KEYWORDS:  otp bots, 2FA, fraud, account takeovers, cryptocurrency

INTRODUCTION

‘For security, and so we can block this request, we’ll need to confirm your identity. Please key the six-digit code we sent you. When you are finished, please press pound.’ Receiving an automated call from one’s personal financial institution asking to verify a potential fraudulent transaction would likely cause an immediate reaction in entering the six-digit code that was sent via short message service (SMS). Unbeknownst to the victim, by entering the code that was sent to them, they have just handed over access to their account(s) to a bad actor through a one-time password (OTP) bot.

With the growing integration of automated technologies for everyday processes, such as self-checkout retail kiosks and mobile delivery robots, it is no surprise that cyber criminals are also removing direct communication with victims, opting for a completely automated form of interaction. OTP bots are a form of social engineering that allows bad actors to obtain the one-time passwords from victims to bypass the two-factor authentication (2FA) on an account. The OTP bot sends a false phone call, disguised as a robocall from a victim’s financial institution, and ultimately tricks the victim into divulging their 2FA code. The attacker then uses the code to gain access to the victim’s account, subsequently committing an account takeover.
OTP bots were first developed as a crimeware-as-a-service in late 2019, with a significant rise in popularity in the summer of 2021, likely due to the COVID-19 pandemic causing fraudsters to implement a work-from-home model. The bots are sold and operated through Telegram, an encrypted messaging platform, wherein there are dedicated channels for specific bot operators. These channels promote their bots as products, posting photos of successful takeovers to gain business from new customers. To allow the account takeover to materialise, the purchaser of the bot must provide the victim's personal identifying information (PII), including their phone number and name of their financial institution, to the OTP bot operator. From there, the operator customises the robocall script for the victim and executes the fraudulent call through the OTP bot. Contingent on compliance, the entire phone call interaction could be less than one minute.

OTP bots can attempt to steal OTPs for anything that requires 2FA: traditional financial institutions, cryptocurrency exchanges, social media platforms, e-mail service providers and more. Any customer account that has saved credit card, debit card, bank account information or direct access to funds would be of interest to bad actors and could be a fruitful target of account takeover.

As corporation security operations are evolving, so are OTP bots, their operators and scammers. New bot channels are being created on Telegram on a consistent basis, promoting competitive pricing, high efficacy rate and, most importantly, ease of use. One OTP bot operator, uniquely named ‘OTP BOT’ (see Figure 1), states on their website that 'SIM swaps are no longer necessary due to our technology'.

The proliferation of new OTP bots and unique attack methodologies has made the detection of account takeovers increasingly difficult. Moreso, OTP bots are incredibly easy to use and have shown an efficacy of 80 per cent, given the victim answers the call and is provided with accurate information from the bad actor. As such, OTP bots are here to stay for the foreseeable future.

**OTP BOT ARCHITECTURE AND PROCESS**

The first step to committing a successful OTP bot attack is having the fraudster obtain victim account credentials. These are typically purchased from carding vendors such as Brian’s Club, Yale Lodge or Trump’s Dumps, as operational examples at the time this paper was written. Users purchase ‘dumps’ or ‘fullz’ of information that include everything from social security numbers to specific debit card PINs for a victim. These dumps can be customised to include people and cards that have registered billing addresses located in a specific area of the world to circumvent geographic barriers, depending on the fraud that is intended to be committed.

Once the fraudster chooses their victim, usually based on their financial institution, they then pick their OTP bot of choice. OTP bots can offer an array of subscription options to their customers, ranging from one-time use, weekly use, monthly use, to lifetime usage of the specific bot. Subscription prices fluctuate between hundreds to thousands of dollars, which at first thought could seem incredibly high; however, paying US$4,000 for the use of a bot to commit an account takeover that will potentially net over ten times that amount appears to be a tremendous bargain. Many OTP bot providers take payment in cryptocurrency, which is where crypto exchanges can be seen as high value, both as targets of attack and as an investigative resource.

After payment for the bot service is sent, the fraudster sends PII for their victim, including the victim’s phone number and financial institution, to the OTP bot operator, which typically provides a variety of services. Some OTP bot operators provide ‘full service’, wherein they not
only make the phone call to the victim, but they commit the account takeover for the fraudster as well. Other OTP bot operators only provide the phone call, and the fraudster is on the other end committing the takeover themselves. Regardless of the account service that is provided, the robocall is generally consistent across the bots (see Figure 2).

Once all the pertinent information has been provided, the bot then makes a spoofed call using interactive voice response (IVR) technology, impersonating the targeted institution to the victim under the ruse of verifying unauthorised account activity. Spoofed IVR calls are all made through the Telegram application programming interface (API), which eliminates the potential to do a call traceback to identify the true identity of the caller, and therefore may be a hindrance to law enforcement investigations. The following is an example of a potential OTP bot transcript:

‘Welcome to PayPal’s fraud prevention system. We have recently received a payment request of $58.82. If this was not you, please press 1.
[Victim presses 1] In order to secure your account, please enter the code we have sent to your mobile device now.
[Victim then enters the OTP that was provided, either via SMS or an authenticator application]
Thank you. Your account has been secured and this request has been blocked. Please make sure to only enter your password at PayPal.com. Don’t worry, if any payment has been charged to your account, we will refund it within 24–48 hours. Your reference ID is 1549926. You may now hang up.¹⁴

The script of an OTP bot can be completely customisable, from the language that is spoken, specific wording of the ‘unauthorised transaction’ on the account, to the hold music playing in the background. The OTP that was sent to the victim during the call is initiated by a login attempt made by either the fraudster or the bot operator. Once the victim enters the OTP during the call, it is then passed back through Telegram to the attacker, who then uses the OTP to bypass the 2FA on the victim’s account and gain access.

**SMSRANGER AND PAYMENT INFRASTRUCTURE**

While the bots are operated out of Telegram, the purchasing transaction is not always made through Telegram. Some established bot vendors have websites that can be accessed through a Clearnet search, such as SMSRanger. SMSRanger, which began operating in 2021, is one of the most popular OTP bots in current operation and advertises itself as ‘the most advanced SMS capture bot on the market’⁵ (see Figures 3 and 4).

SMSRanger has a website that comes up as the first hit on a simple Google search. The website provides link access to the Telegram channel, a section for customer reviews and purchasing options. The purchasing links lead to a payment processing page hosted by Sellix, where bot packages are displayed along with their prices. The operator of SMSRanger solely accepts cryptocurrency as form of payment for bot access, specifically Bitcoin, Ethereum, Litecoin or Nano, which are subject to change at the operator’s discretion. The purchaser selects their package of choice, which prompts them to input an e-mail address for the transaction. They are then provided a cryptocurrency address, depending on the crypto that they selected, to send the funds to complete the transaction.
The fact that OTP bots are being purchased with cryptocurrency creates an enormous intelligence-gathering opportunity for fighting financial crime, because the payment infrastructure is transparent. Cryptocurrency payments for OTP bots and the subsequent usage of funds by the receiving address are visible on a blockchain, which is a public ledger. For example, the cryptocurrency address that was provided during the purchase of SMSRanger can be entered into a blockchain explorer, where the entire transaction history of the address, including every single sending and receiving transaction, can be viewed and is unable to be altered.

Throughout platform investigations, we have determined that most OTP bots accept payment in Bitcoin or Ethereum. The use of privacy coins for payments or conversions has been extremely limited, which is indicative to us as an investigative team that the operators are generally not particularly sophisticated in laundering the funds.
The purchasing of OTP bots using crypto puts crypto investigators in a unique position, as we are not only able to trace the funds of sellers of the bots, but we are also able to see who is purchasing the bot in furtherance of their own criminal activity. This provides two different avenues for potential investigation:

1. Trace the funds sent to the operating OTP bot crypto address through blockchain analytics tools, with the intention of finding an identified entity where the threat actor withdraws their money, otherwise known as a cash-out. Funds can be sent and laundered to an unlimited number of wallets, which could lead to a very long and arduous money trail. If funds are eventually traced to a known entity, such as a centralised cryptocurrency exchange, legal process can then be sent to the entity in hopes
of identifying the account holder of that
address or wallet; or
2. Identify the purchasers of the bot if
they used a hosted wallet or exchange
to process the transaction and open
individual investigations into those
account holders.

Purchasers of OTP bots can likely be
attributed to their own individual fraud and
identity theft ring. For example, if Coinbase
can identify 100 unique purchasers of an
OTP bot, there are potentially 100 unique
individuals facilitating their own fraud rings,
who can then be referred to and investigated
by law enforcement. Each unique purchaser
likely has numerous victim accounts that they
are attempting to access, which ultimately
leads to thousands of identified accounts and
their own spinoff investigations.

If a threat actor purchases an OTP
bot through a centralised cryptocurrency
exchange, it is unlikely that customers of
the same exchange will be victimised from
that attack. Typically, threat actors will target
victim accounts held at traditional financial
institutions. This is due to a few reasons:

- Fiat banks generally have a larger number
  of established high-value accounts as
  compared to cryptocurrency exchanges,
  which leads to more opportunity for the
  threat actor. An established account is one
  that has been open with an institution for
  a number of years with either a minor or
  non-existent history of issues between the
  company and the customer;
- An established account at a fiat institution
  commonly will have a high withdrawal
  limit due to the longevity of the account
  being opened, lowering the risk of not
  being able to withdraw or transfer funds
  when accessed; and
- Information about infiltrating traditional
  financial institutions and guidance
  surrounding navigation of implemented
  fraud rules is more readily available on
  dark web forums.

In June 2022, Timmy Ijie was sentenced
to four and a half years at a UK court for
operating an OTP bot. The investigation was
led by the City of London and Metropolitan
Police, whereby it was stated in the case press
release that:

‘Ijie used an online messaging app,
Telegram, to offer specialist software for
sale which enabled fraudsters to bypass
banking security systems. Ijie offered the
software through a monthly subscription,
charging a fee of around £600 per month,
payable in cryptocurrency … Ijie boasted
on social media how successful this
software was, in enabling the commission
of fraud. He bragged that, in one day
alone, it had been used by criminals to
defraud over 150 victims and posted
positive reviews from criminals who had
successfully used the software.’

Ijie is the first individual who has been
criminally sentenced for operating an OTP
bot.

PLATFORM BOT DETECTION

With the prevalence of bots and forms of
social engineering progressing at a rapid
pace, the bigger issue at hand is how
institutions can detect and protect their
systems and customers from OTP bot
attacks. Unfortunately, there is no simple
answer. It is incredibly difficult to proactively
prevent attacks, and it is equally difficult to
retroactively identify takeovers stemming
from bot attacks.

One of the most difficult aspects as
an issue to FinTech is victim association.
Retroactively, it is hard to determine users
and accounts that are victims of these specific
attacks. Without outside knowledge or
corroboration from the account holder,
there essentially is no way to know from an
institutional standpoint that an account was
fraudulently accessed because the account
holder unknowingly provided their OTP
to a bad actor. To identify accounts that were victims of bot attacks, the victim typically must corroborate the activity by self-reporting the takeover to their financial institution.

One method of potential identification of specific bot operations on platform would be through the observation of an attack through a controlled purchase. In this instance, law enforcement would employ an undercover (UC) identity to purchase the bot for intelligence gathering. UC purchases of services by threat actors can be exceedingly fruitful, in that these operations can provide device information that belongs to the bot operator. Because a UC purchase of the bot would require ‘victim’ credentials, institutional security operations and intelligence teams can view the attack in real time, since the accounts that are going to be ‘taken over’ are known.

Once a bot completes the UC attack, there is a multitude of information that can be obtained and therefore analysed. The first piece of data that would/should be of interest would be the Internet protocol (IP) address(es) that accessed the accounts at the time of attack. Accounts associated by IP connectivity likely would lead to other victims as well as hopefully a potential target of investigation. Device identifiers, such as international mobile equipment identity (IMEI) numbers and media access control (MAC) addresses, can be of immense investigative and identifiable value if retained by the targeted institution. If hard device identifiers are not retained, it is probable that some form of internal identification is assigned to a user’s device that could then be searched on the platform in the same manner as an IMEI or MAC address. Other datapoints of interest include user agent strings, device screen resolution and source of account access. These indicators could give tremendous insight into the true location of the attacker, how the attacker accessed the platform, and if multiple devices were used within a single account takeover.

Additional observable information includes patterns of transaction and login activity. For example, a threat actor disabling SMS 2FA on an account and immediately enabling Google authenticator within a few seconds may indicate operation of other victim accounts. The process of switching 2FA methods within a uniquely short timeframe could help group other accounts that have the same event log.

It is important to note that the threat actor operating the bot is likely aware of potential internal account triggers, specific to each institution they are attacking. This makes identification of these attacks even more difficult to recognise because the account typically does not have any signs of suspicious or unusual activity as compared to a regular user. For example, threat actors may learn that many financial institutions flag suspicious transfers above certain monetary thresholds and will deliberately structure theft transactions to fall below those amounts. Many threat actors are generally aware of these mechanisms across all financial institutions, both fiat and crypto, and therefore tend to send funds in small batches. The smaller transactions typically pass through without triggering any internal fraud indicators as they do not aggregate the amounts that are sent, contingent on the transaction monitoring rules put in place by the institution to detect customers who may be attempting to structure transactions and evade thresholds.

THREAT MITIGATION

A recent report published by Proofpoint states that ‘attackers attempt to initiate more than 100,000 telephone-oriented attacks every day’. With the rise in popularity of OTP bot use by threat actors and the institutional difficulty of detecting real-time attacks, threat mitigation ideas and plans are limited.

The first and arguably the most effective line of defence against OTP
bot attacks begins at the customer level. Educating consumers on the dangers of social engineering attacks as well as general etiquette in safeguarding personal information is vital in attempting to reduce successful account takeovers. Favorable targets of OTP bot attacks are people who possess below-average computer literacy and technical prowess, thus being more vulnerable to fraud, scams and exploitation. Some potential examples of valuable and practical measures of consumer education at an institutional level are email campaigns and in-app notifications. These e-mails and notifications should be specific in providing information about the current threat landscapes that are respective to the institution, therefore providing users the tools to allow them to protect themselves in addition to the safeguards already put in place by the business.

At the same time, it is prudent to recognise that OTP bot attacks materialise because the bad actor already has the victims account information. It is reasonable to believe that compromised credentials could be obtained from a multitude of sources: company information breaches, potential malware infections on personal devices, an account takeover that occurred at another institution, etc. With the tremendous amount of personal data and account information that is already circulating on darknet markets, businesses must also take a proactive approach to ensure safety for their customers and systems.

Another advantageous suggestion to further combat OTP bot attacks is to leverage dark web intelligence for compromised account credentials. Regardless of how the user’s information was originally obtained, implementation of credential stuffing and account takeover software can offer protection. Software companies that provide these services operate by running current user account credentials against dark web data dumps, which then gives the operating institution the opportunity to not only alert the customer that their information has been stolen but can also require the user to change their account password. If a threat actor provides an incorrect password to an OTP bot, the following attempted attack will be unsuccessful because they cannot even log into the account to initiate the OTP request.

Furthermore, implementation of alternative methods of 2FA, such as time-based one time password (TOTP) codes from authenticator applications and security keys, would ultimately destroy the OTP bot market. Hardware security keys, such as Thetis or YubiKey, leverage FIDO Universal 2nd Factor (U2F) protocol which enables users to securely access their accounts by use of a physical device. For an attacker to obtain access to a victim account that uses a security key as their method of 2FA, the attacker would physically need to have the key in their possession. As a result of materially needing the security key to access an account, it essentially renders hardware security keys as hack-proof and phish-proof. Platform application of more secure methods of 2FA would likely also require a business to include additional resources regarding customer education efforts.

**CONCLUSION**

OTP bot attacks are only going to become more elaborate as technology and the modern-day criminal advances. Law enforcement and crypto investigators can trace and attempt to identify bad actors on a mostly reactive basis, but it is imperative that proactive measures are taken by businesses and corporations to safeguard their platforms and customers. It is necessary for institutions to implement a combination of customer education, utilisation of alternate and more secure 2FA methods, as well as platform credential monitoring to their existing security efforts to successfully disrupt the current state and future evolution of OTP bot attacks.
References