

RSAConference2022

San Francisco & Digital | June 6 – 9

SESSION ID: **AFD-M02**

One-Time Password “OTP” Bot Attacks

Kelsey Dean

Manager, Global Intelligence
Coinbase

Kristen Spaeth

Senior Investigator, Global Intelligence
Coinbase

TRANSFORM



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

RSA[®]Conference2022

OTP Bot Attacks

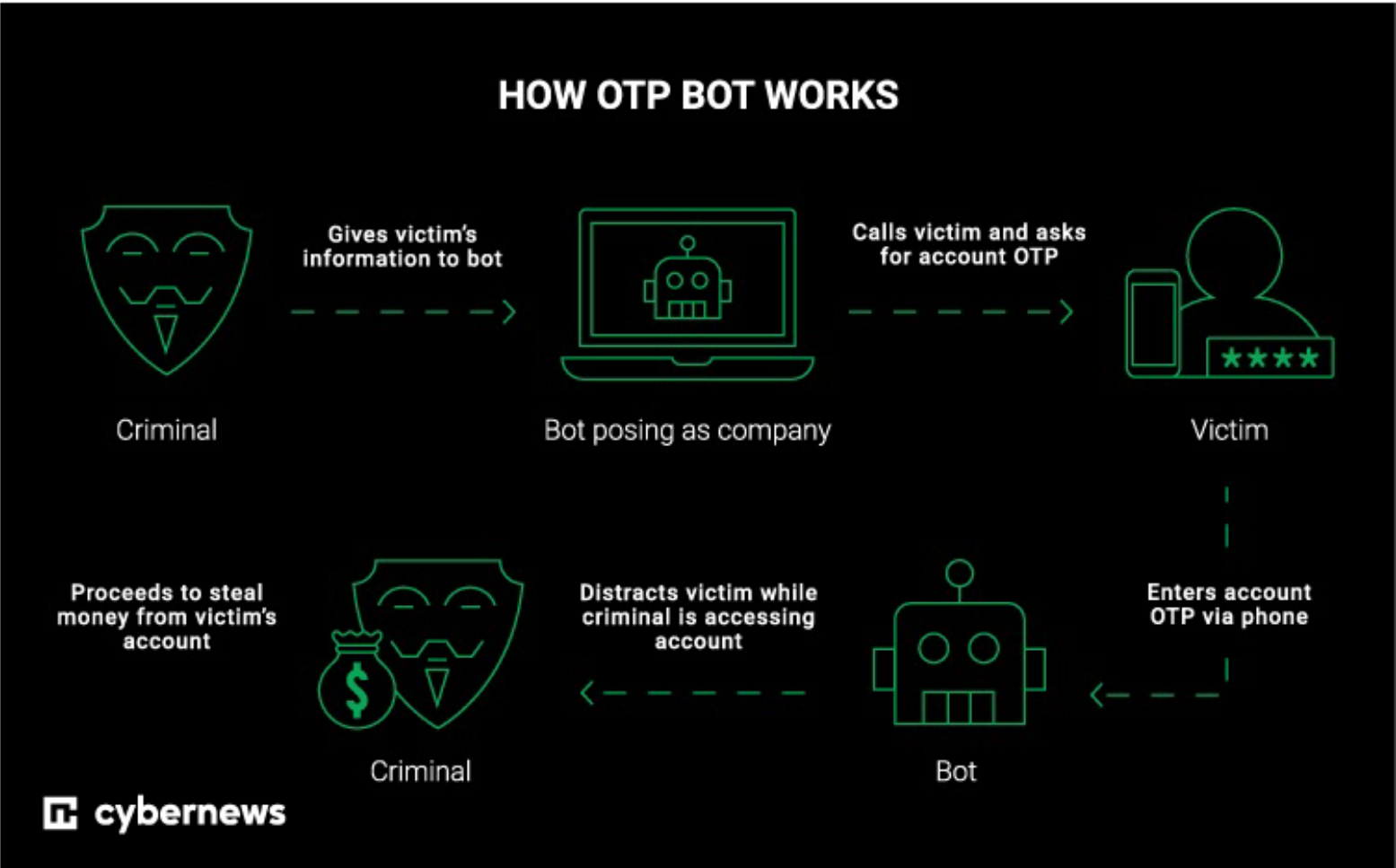


Telegram OTP Bots

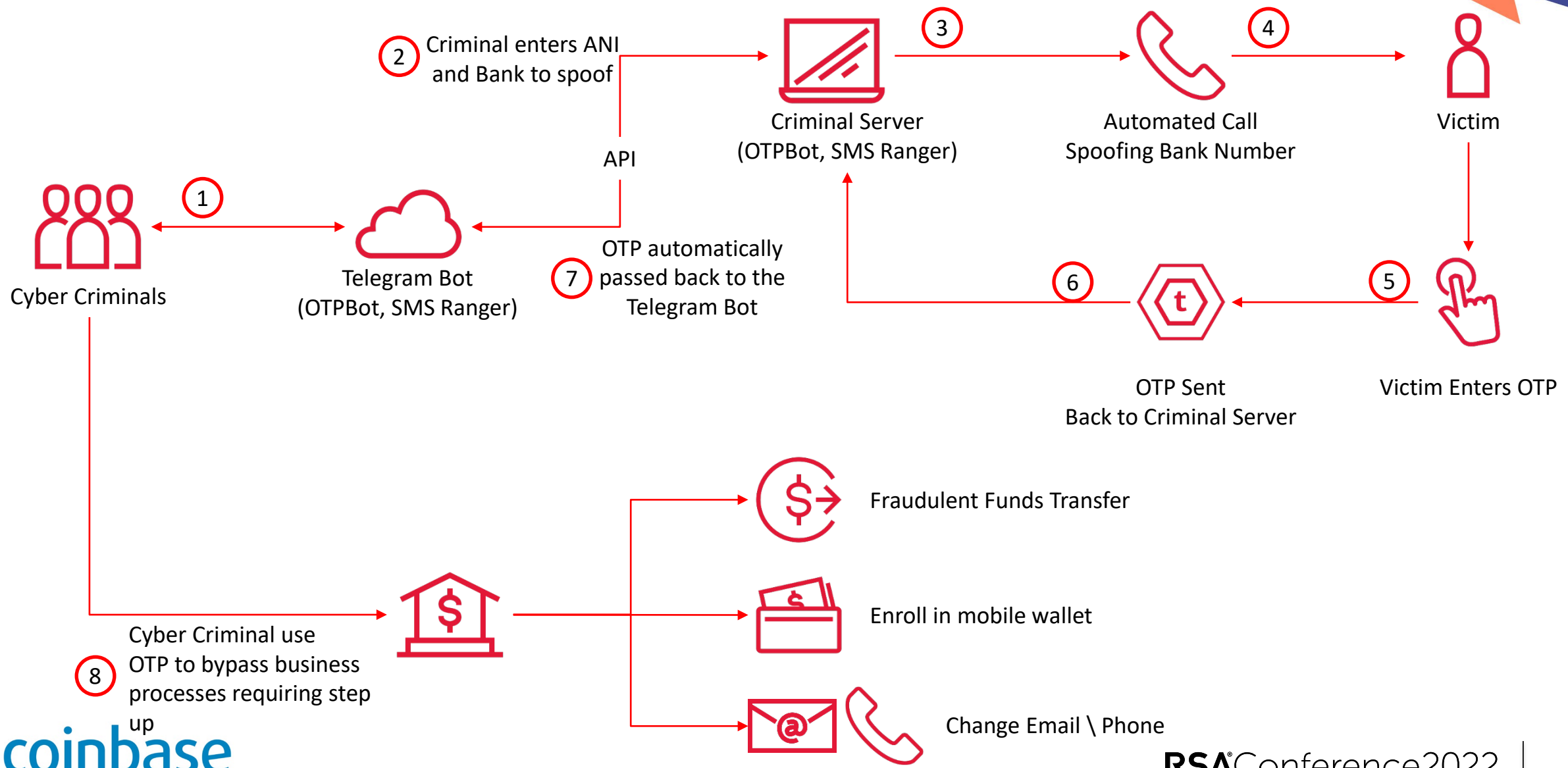
- Began services in early 2021, popularized in July 2021
- Sells on average for \$500-700 USD
- Targets financial services
- Bot makes a robocall to the victim, tricking them into providing their OTP
- OTP is sent back to the bot user
- Threat actor then commits ATO



Telegram OTP Bots



Telegram OTP Bot Architecture



Telegram OTP Bot Example



Source: <https://www.youtube.com/watch?v=GNXhHAh67DQ>

Notable Threat Actors – SMSRanger



Sms Ranger

@thesmsranger

BEWARE OF SCAMMERS PUTTING @ in bio.
ONLY USE SMSRANGER.io

SEND MESSAGE

Notable Threat Actors – SMSRanger



SMSRanger Updates
5.98K subscribers

November 5



SMSRanger Updates

DAILY REALTIME SERVICE STATUS

US 🇺🇸 UP ✓
CA 🇨🇦 UP ✓
FR 🇫🇷 UP ✓
UK 🇬🇧 UP ✓
ITA 🇮🇹 UP ✓
GE 🇩🇪 UP ✓
CO 🇨🇴 UP ✓

ALL SERVICES UP AND RUNNING!!

MESSAGE @THESMSRANGER FOR PAYMENTS. PLEASE DO NOT FALL FOR THE FAKE ACCOUNTS MESSAGING YOU TO PURCHASE. WE WILL NEVER MESSAGE YOU FIRST.

3.3K 👁 14:38



SMSRanger Updates



🌐 NEW ULTIMATE PACKAGE 🌐

THIS INCLUDES:


COUNTRIES:
🇺🇸 US / 🇨🇦 CA / 🇬🇧 UK / 🇫🇷 FR / 🇪🇸 SPAIN / 🇩🇪 GERMANY / 🇮🇹 ITALY / 🇨🇴 COLOMBIA

LANGUAGES:
ENG / FR / SPANISH / GERM / IT

MESSAGE @THESMSRANGER FOR PAYMENTS.

PRICE PER MONTH: 1500USD
PRICE FOR LIFETIME: 7500USD

3.6K 👁 edited 14:38



SMSRanger Updates
@smsranger

5.98K

292

54

2

95

Subscribers

Photos

Videos

Files


Links

SMSRanger is the most advanced SMS capture bot on the market.

Capture OTP, personal credentials, and much more

Updates and News Channel

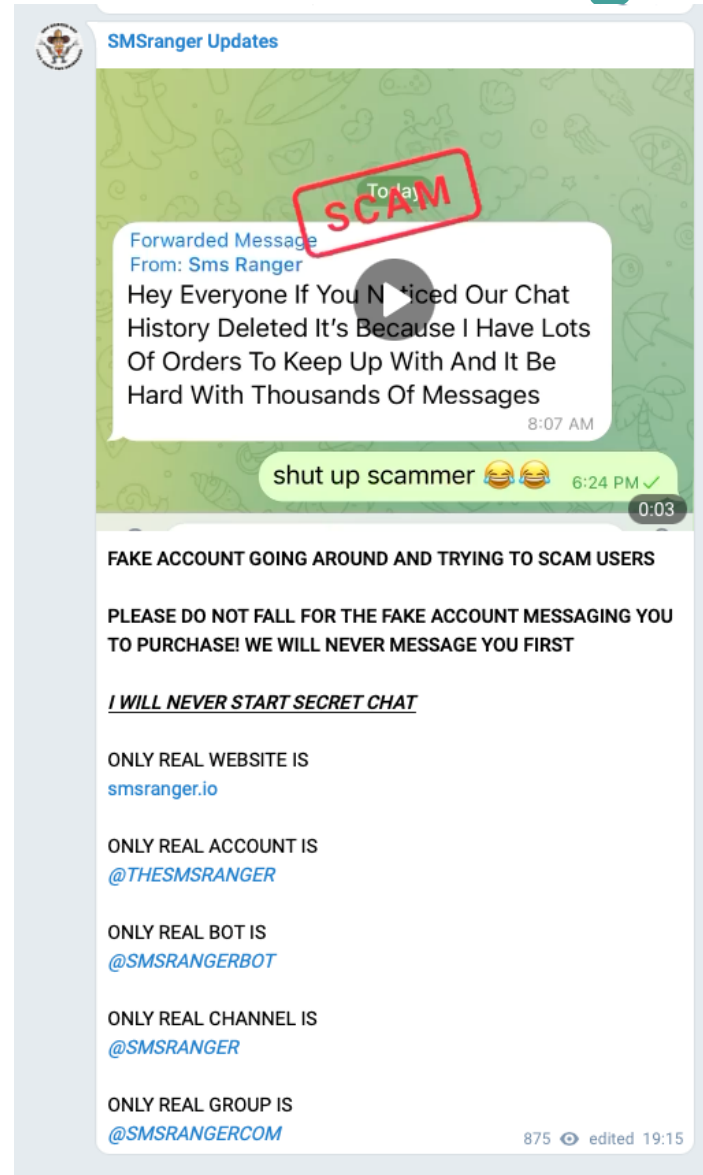
For Sales Contact: @thesmsranger

 **DOWNLOAD TELEGRAM**

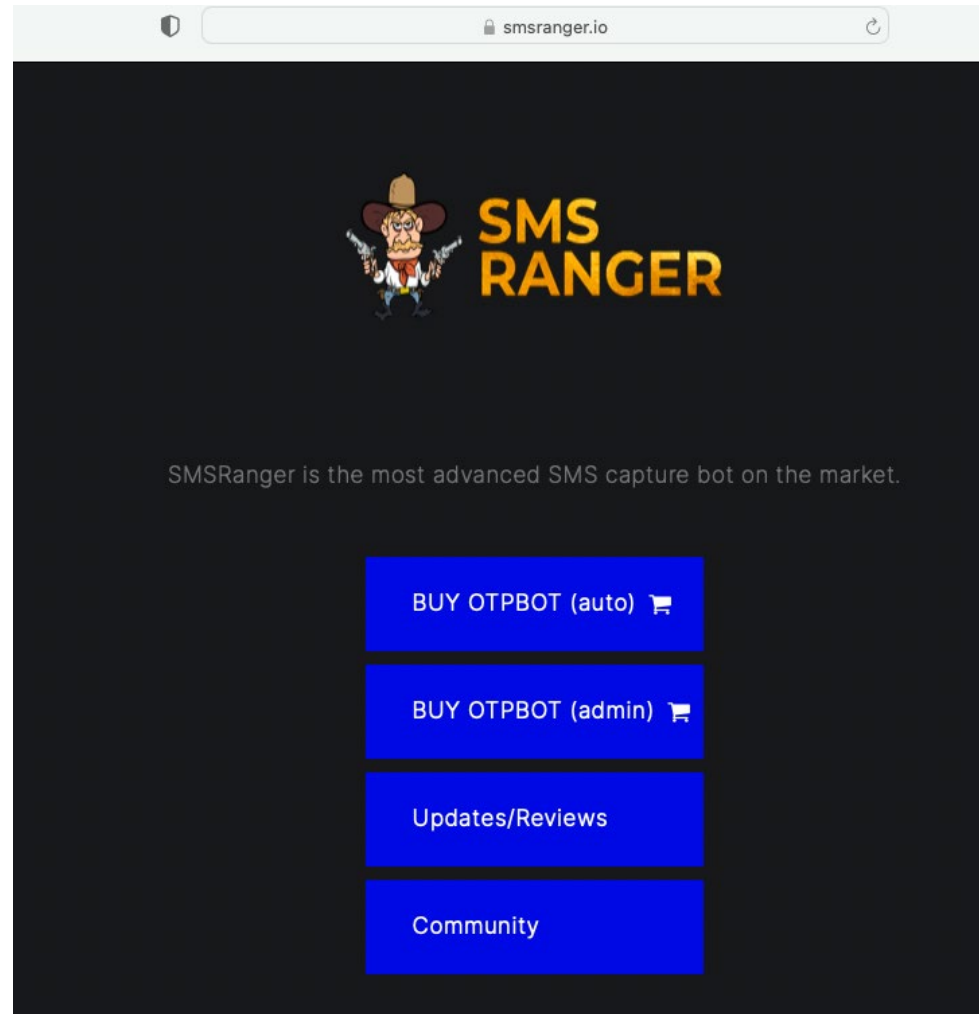
to view and join the conversation

[About](#) [Blog](#) [Apps](#) [Platform](#)



Notable Threat Actors – SMSRanger




Notable Threat Actors – SMS Ranger



Notable Threat Actors – SMS Ranger





SMSranger

Providing customer services since July 2021

Product Quality


5 ★★★★★ (4 reviews)

Products

Contact

Feedback

Terms



Search for a product...

Q

Sort By: Default

▼

MSRANGER

OTP / 2FA &

ORE CAPTURE B

heSMSranger | smsranger.i

(promo) 14 days TRIAL

\$380.00

Stock 7

MSRANGER

OTP / 2FA &

ORE CAPTURE B

heSMSranger | smsranger.i

30 Day Subscription

\$600.00

Stock 4

MSRANGER

OTP / 2FA &

ORE CAPTURE B

heSMSranger | smsranger.i

Lifetime Subscription

\$4000.00

Stock 3

Notable Threat Actors – SMSRanger

- Easy to use
- Those who pay for access can use the bot by entering commands similar to how bots are used on popular workforce tools, like Slack
- Entering commands enables various modes, scripts aimed at services and specific institutions
- Once a target phone number has been entered, the bot does the rest of the work
- 80% efficacy rate if the victim answers the call (Intel 471)

Telegram OTP Bot Detection

- Hard to proactively prevent attacks
- Hard to retroactively identify takeovers
- Bot is sold as a service to threat actors by threat actors; can lead to thousands of suspects and victims
- Not every attempt is successful
 - The tool is widely promoted in Telegram channels, but scammers occasionally use false advertisement of successful takeovers

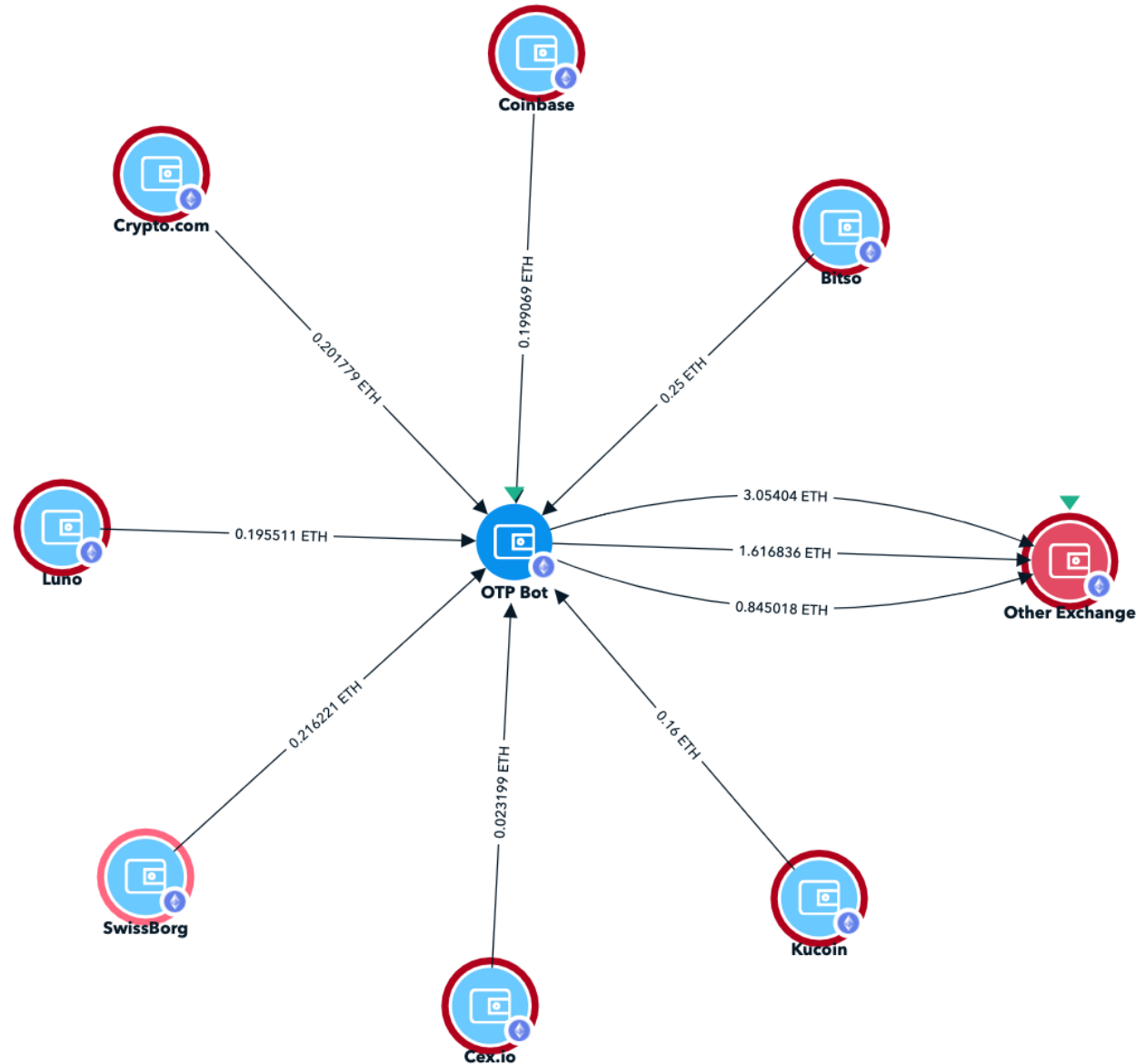
OTP Bots and Coinbase

- Coinbase has been the target of many OTP Bots, especially in Telegram and WhatsApp advertisements
- Most activity seen on the platform has been in relation to the **purchasers** of the bot for attacks on other institutions
- Identified bot attacks on Coinbase accounts have not been successful financially
- Purchasers have typically been using their Coinbase account to buy access to the bot, then committing ATO's at other traditional financial institutions

Payment Infrastructure

- The public ledger creates a big intel gathering opportunity to trace and identify attackers buying the OTP bot and the OTP architects selling their bot
- Typical purchase amount is \$500-\$700 USD, accepted in BTC, ETH and LTC
- Can be multiple transfers of crypto to numerous exchanges before cashout
- Proceeds of takeover are sent in crypto and then usually withdrawn to fiat currency

Payment Infrastructure



Issues to FinTech

- Victim association
 - Hard to determine users that are victims of these specific attacks
 - Credentials usually obtained in darknet market dumps, not always leading to active and valuable accounts
- Attack anticipation
- Identification of attack patterns
 - Pattern of sending activity
 - Pattern of login activity
 - Timing of password cracking

Industry Best Practices

- Enabling and familiarizing users with security keys
- Use a different method of 2FA, such as biometrics
- Consistent monitoring of attack patterns by confirmed data
- Pro-active threat landscape monitoring
- Communication between financial institutions
- Educating users about current threat landscapes
 - Coinbase Earn campaign regarding account safety

Gathering Intel on OTP Bots Targeting Your Company



- Keywords: “OTP bot” “SMS bulk” “SMS%” “authenticator”
 - “Bot” may be too broad
 - These keywords are typical of PURCHASERS of the bot
 - Further analysis can be made from those accounts, using IP and device data
- Telecoms can search for spammed landlines or spammed non-working numbers
- Analysis on user accounts that have customer service outreach