For more information contact:
Jean Creech Avent
J.CreechAvent@ArkoseLabs.com

Week of July 4, 2022

A weekly analysis of trending fraudster activity on the Dark Web

FRAUD THREAT ALERT

Bot-as-a-Service OTP Scam

The chatter: Fraudsters on Telegram have been holding robust discussions about a new malicious bot for sale that enables less technically-savvy fraudsters (Luddite Fraudster category) to gain one-time-passwords (OTPs).

Who's buying: Fraudsters who are committing account takeover (ATO) attacks and need OTPs to get into accounts to complete the scam.

Three benefits of OTP Bots:

1. OTP Bots save fraudsters time, which increases their chances of success and ups their ROI.

2. OTP Bots open the door for less technical fraudsters to attack at scale because the Bot does all the work so less technical fraudsters no longer have to social engineer their way into an online account.

3. It's cheap. This is a trending topic among fraudsters because of the ROI. The fraudster who developed the OTP Bot shown here is charging the following for unlimited calls:
    a. $30 a day
    b. $150 a week
    c. $700 a month

That means the price is the same if a fraudster is trying to take over one account and needs one call done by the Bot to get the OTP or if the fraudster needs 5,000 calls done.

For more information contact:

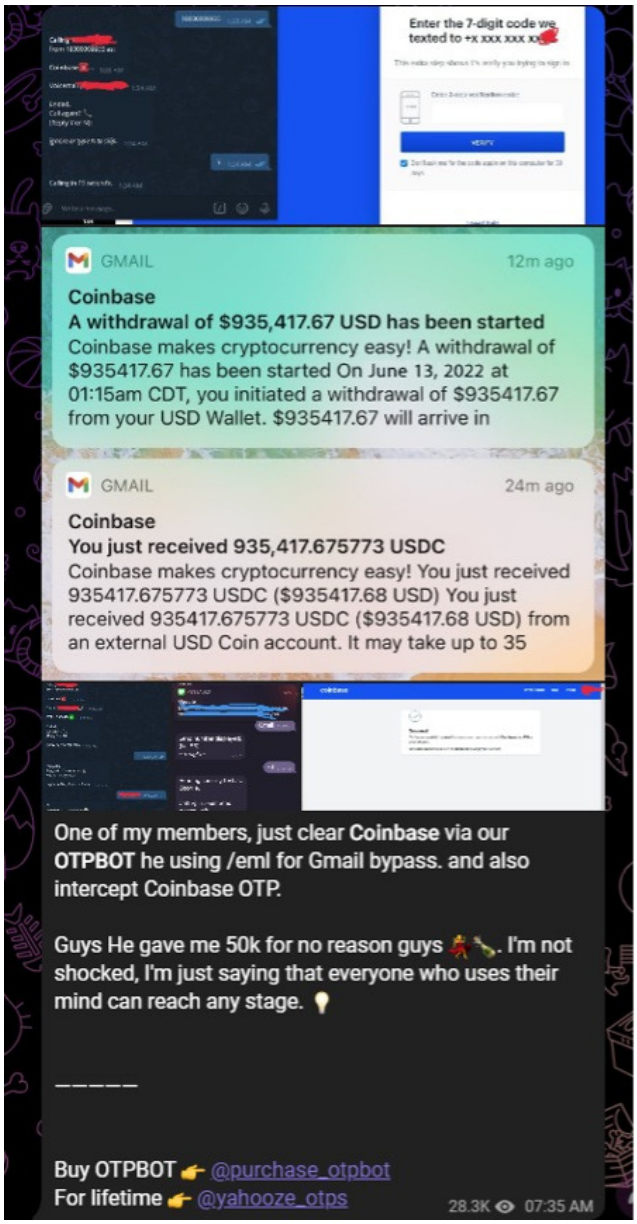
Jean Creech Avent
J.CreechAvent@ArkoseLabs.com

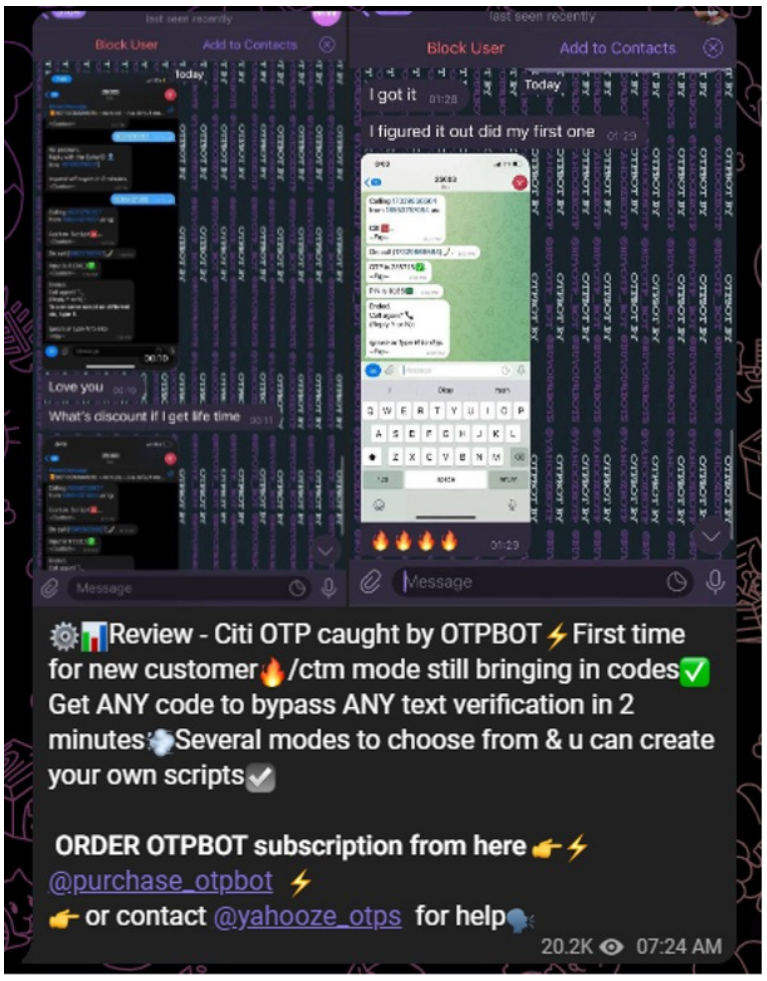
Week of July 4, 2022

A weekly analysis of trending fraudster activity on the Dark Web

FRAUD THREAT ALERT

Bot-as-a-Service OTP Scam





For more information contact:

Jean Creech Avent
J.CreechAvent@ArkoseLabs.com

Week of July 4, 2022

A weekly analysis of trending fraudster activity on the Dark Web

FRAUD THREAT ALERT

Bot-as-a-Service OTP Scam

Verification: This is a verified seller and a verified product. The fraudster has been advertising OTP Bot for at least two months.

How the scam works: When the fraudster initiates the ATO, the attack triggers the actual bank to check the activity and notify the consumer of unusual activity, sending the consumer an OTP. The Bot spoofs the bank, calls the consumer and requests the OTP code.

Twist: In this attack, it is the bank's friendly bot that ultimately sends the OTP back to the malicious bot – Bot v Bot. The victim provides the Bot with the OTP. At that point, the fraudster now has the OTP and can use it to easily access the consumer's bank account. In the screenshots, you see that this fraudster is charging $700 a month and has 600 regular members, resulting in thousands of dollars being stolen through OTP Bots.

To reach scale fraudsters take three actions:

1. Spray and pray: They mass spam
2. Old Data: Fraudsters tap into data from past breaches or pastebin dumps
3. Buy: Fraudsters leverage information they purchased from a Dark Net vendor, as well as background check sites, credit report sites, etc.

For more information contact:

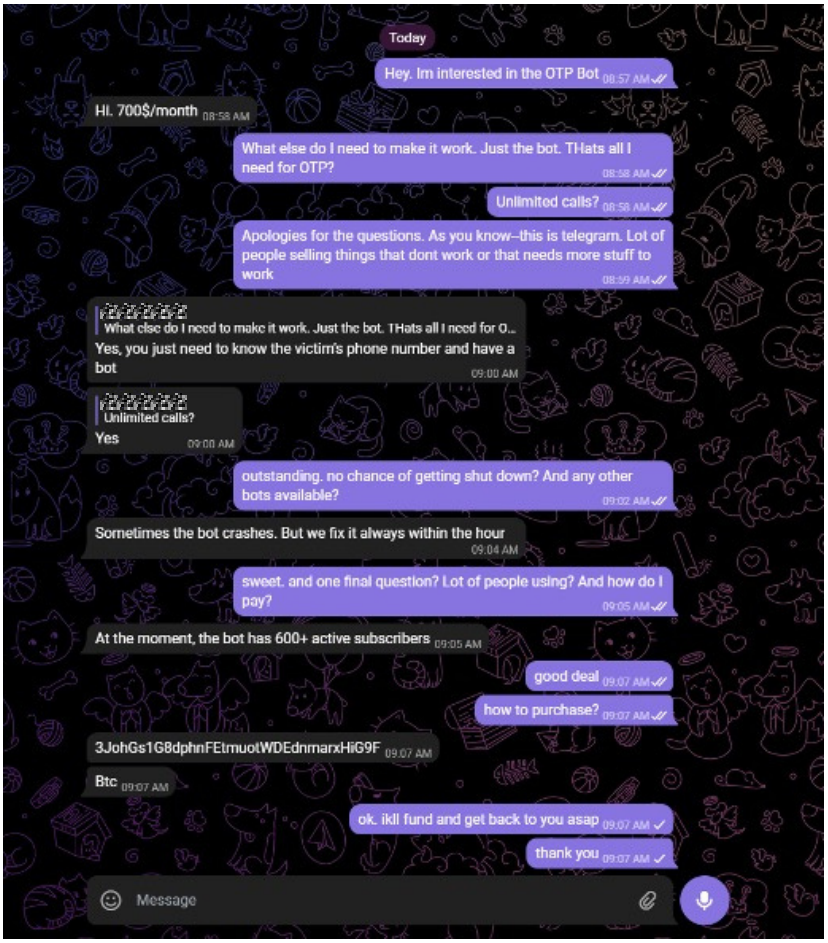
Jean Creech Avent
J.CreechAvent@ArkoseLabs.com

Week of July 4, 2022

A weekly analysis of trending fraudster activity on the Dark Web

FRAUD THREAT ALERT

Bot-as-a-Service OTP Scam



For more information contact:

Jean Creech Avent
J.CreechAvent@ArkoseLabs.com

Week of July 4, 2022

A weekly analysis of trending fraudster activity on the Dark Web

FRAUD THREAT ALERT

Bot-as-a-Service OTP Scam

Stat: From May 27 through June 27, 2022, conversations discussing OTP and related bots were popular on Telegram channels such as AIO, Dark Web Forum and others with at least 10 vendors advertising bots capturing OTPs and those vendors also operating their own stand-alone Telegram channels advertising the bots, and offering screenshots of the success criminals are having.

Trend: OFF-THE-SHELF: Historically only 5% of attacks have been Bots. Today, though, Bots are becoming ubiquitous because technically-savvy fraudsters are creating and licensing Bots for other fraudsters to use (Bots-as-a-Service). Bots-as-a-Service is making it easy for Rookie Fraudsters, Luddite Fraudsters, and Master Fraudsters to use Bots in their attacks on consumers' online accounts at scale.

Quote: Arkose Labs Chief Criminal Officer Brett Johnson: “Fraudsters nowadays don't have to understand how to build a Bot. They don't have to know how to run Bots. It is all done for the fraudsters by other fraudsters who do have the technical skills. The only thing the fraudster needs to do is pay the other fraudster $30 a day for unlimited attacks.”

.