

4. I investigated a wide range of cyber cases at the FBI, including computer intrusions by cybercriminals and nation-states, counterintelligence and insider threats, intellectual property rights violations, online child exploitation, extortion, and internet fraud. The cases for which I was responsible included matters involving millions of dollars of illicit funds transferred to Russia via a digital currency exchange; a cross-jurisdictional, coordinated takedown of over seventy cybercriminals associated with the “Zeus Trojan” email malware¹; the apprehension and conviction of the creator of “Gozi” malware; a multinational investigation into the use of stolen account information from a hacked ATM network, resulting in nine convictions and millions of dollars seized in cash and property; dismantling of the LulzSec hacking group; and the FBI’s response to nation-state-sponsored distributed denial-of-service (“DDoS”) attacks on U.S. banks’ websites—the most significant and sustained DDoS attacks against U.S. critical infrastructure originating from a nation-state actor in history.

5. I held leadership roles at the FBI’s New York and Newark field offices as well as at the FBI headquarters in Washington, DC. I served as Assistant Special Agent-in-Charge at the FBI Newark field office, leading the Joint Terrorism Task Force, Cyber Task Force, and various Counterintelligence squads. I also was Chief of Operations for the National Cyber Investigative Joint Task Force, enhancing interagency information exchange and intelligence integration in the cyber field.

6. I hold a Bachelor of Science degree from Peru State College, Nebraska, Master of Business Administration degree from Monmouth University, New Jersey, and a Master of Science in Information Technology from Carnegie Mellon University, Pennsylvania. I am a Certified

¹ Malware is software that is designed specifically to disrupt, damage, or gain unauthorized access to a computer system.

Information Systems Security Professional (CISSP). A true and correct copy of my curriculum vitae is attached to this declaration as Exhibit 1.

7. I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during this investigation, including from my direct interaction with the online criminal enterprise operated by Defendants—referred to in this action as the “Fraudulent Enterprise”—that is in the business of obtaining Microsoft accounts through fraud and selling them to cybercriminals for a wide variety of internet-based crimes.

I. BACKGROUND ON CYBERCRIME-AS-A-SERVICE

8. Crime-as-a-service (CaaS) is a business model for the trafficking of criminal services on various forums and websites making them relatively easy for anyone who intends to engage in unlawful conduct, including cybercriminal activities. CaaS is a challenge for law enforcement and the cybersecurity community as it generally allows for less sophisticated cybercriminals to engage in cybercrime without needing to possess advanced skills or develop the tools and techniques themselves.

9. CaaS providers include:

- a. Malware developers and individuals who specialize in building malware delivery tools who sell their products on an underground marketplace, which is managed and administered by another services provider.
- b. Infrastructure providers who allow criminals to rent or purchase infrastructure to host malware, deliver DDoS attacks, spam, and as a proxy to obfuscate their identity and location.

- c. Phishing providers who offer phishing kits, which can be used to create and distribute phishing emails, websites, or campaigns designed to steal sensitive information.
- d. Money laundering providers who launder the proceeds of cybercrime, helping criminals convert stolen funds into assets that are difficult for law enforcement to trace back to criminal activity, including cryptocurrency mixing services.
- e. Botnet-for-hire and hacking-for-hire services, which are often advertised on internet forum communications and available on websites or Dark Web marketplaces, offering malicious actors the ability to attack any Internet-connected target. These services are obtained through a monetary transaction, usually in the form of online payment services or virtual currency.

II. HOTMAILBOX.ME AND 1stCAPTCHA.COM

10. Based on my training, experience, and participation in the investigation in this case, I believe and respectfully submit that the Defendants' CaaS model enables cybercriminals to obtain large numbers of Microsoft accounts ("MSAs") in bulk through two fee-based services, Hotmailbox.me and 1stCaptcha.com. The Hotmailbox.me service is available on the open Internet and is a marketplace where the Defendants directly sell verified MSAs. Once an account is created and funds are deposited, cybercriminals have access to active and verified email accounts that could be used to conduct criminal activities, including scams, phishing campaigns, and ransomware attacks, among others.

11. More sophisticated cybercriminals can navigate to the Defendants' CAPTCHA² solve service, 1stCAPTCHA.com, which offers a tool for solving CAPTCHA security challenges,

² I understand that Paragraphs 5–7 of the Declaration of Patrice Boffa in Support of Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Boffa Declaration")

including the CAPTCHA service used by Microsoft. Defendants provide detailed instructions on their 1stCaptcha.com website and on Defendant Duong Dinh Tu's YouTube channel, for how to use their tool against multiple types of CAPTCHA software, including reCAPTCHA, FunCAPTCHA, and hCAPTCHA.³

III. HOTMAILBOX.ME UNDERCOVER BUYS

12. As part of my work for Microsoft on this case, I conducted several undercover purchases of Defendants' services.

13. Specifically, on or about August 28, 2023, I navigated to www.hotmailbox.me and was prompted to, and did, create an account as reflected in Figure 1.

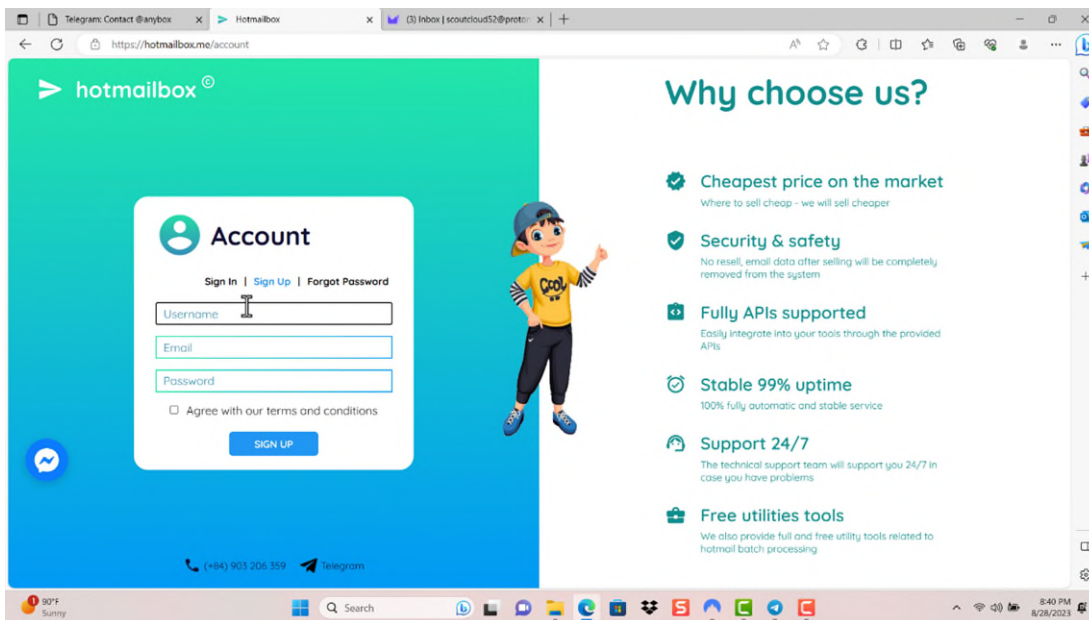


Fig. 1

contain a description of CAPTCHA, familiarity with which is presumed.

³ I understand that Paragraphs 9–17 of the Declaration of Maurice Mason in Support of Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause contain a description of the above-referenced YouTube videos (explaining how Defendants' CAPTCHA-defeating tools function).

14. To use the services provided by Hotmailbox.me, I initially deposited \$50.00 worth of Bitcoin (“BTC”) into my Hotmailbox.me account through payment processor Sellix. The recipient BTC address, which is a unique identifier that serves as a virtual location where cryptocurrency may be sent, was bc1qg74gv0ua5zl3cz8w7aj36fkz5e7ewwugkn5vq8. Following the deposit, I purchased 7,200 MSAs including 5,000 Outlook MSAs, 2,000 Hotmail Trusted MSAs, 100 Outlook MSAs containing the country code top-level domain (ccTLD) for the Federal Republic of Germany, and 100 Outlook MSAs containing the ccTLD for the Czech Republic.

15. Following my purchase, I received email addresses and passwords for each account, including (1) for the Outlook MSAs, the accounts mhaeykalan9@outlook.com and maudyverkku2@outlook.com, with the passwords CmJD2175 and IzoYtN36, respectively; (2) for the Hotmail Trusted MSAs, the accounts dnasihselnik8@hotmail.com and fikadubonanew@hotmail.com, with the passwords q7oAHPRH80 and eA3qnxCt56, respectively; (3) for the Outlook Germany MSAs, the accounts fieboramekoem@outlook.de and krusejouino@outlook.de, with the passwords bDZoCu05 and O3bEyK98, respectively; and (4) for the Outlook Czech MSAs, the accounts yezminrenishn@outlook.cz and eburethrane8@outlook.cz, with the passwords aAFpBP96 and Gg2tzV38, respectively.

16. Following these purchases, I tested the validity of two of the MSAs, which confirmed that I had successfully established an Outlook mailbox with the address mhaeykalan9@outlook.com and password, CmJD2175. I then successfully set up an Outlook mailbox with the address maudyverkku2@outlook.com and password, IzoYtN36. Finally, I successfully sent an email from maudyverkku2@outlook.com to a Proton Mail account I set up for testing.

17. My review of MSA registration logs provided by Microsoft confirmed that the maudyverkku2@outlook.com account was created on or about August 29, 2023, at or about 12:13:14 AM and the mhaeykalan9@outlook.com account was created on or about August 29, 2023, at or about 12:13:15 AM.

18. On or about September 5, 2023, while located in New York City, I navigated to www.hotmailbox.me and viewed the landing page, noting the scrolling banner at the top of the page that read, “Recently, microsoft [sic] is fixing, the account may be locked after a few hours. We are trying to fix it . . . ,” as seen in Figure 2. From a link on the website, I contacted a Hotmailbox support contact, AnyBox Support, through its Telegram channel, and asked about the banner. AnyBox Support responded, “I will reffund [sic],” as seen in Figure 3.

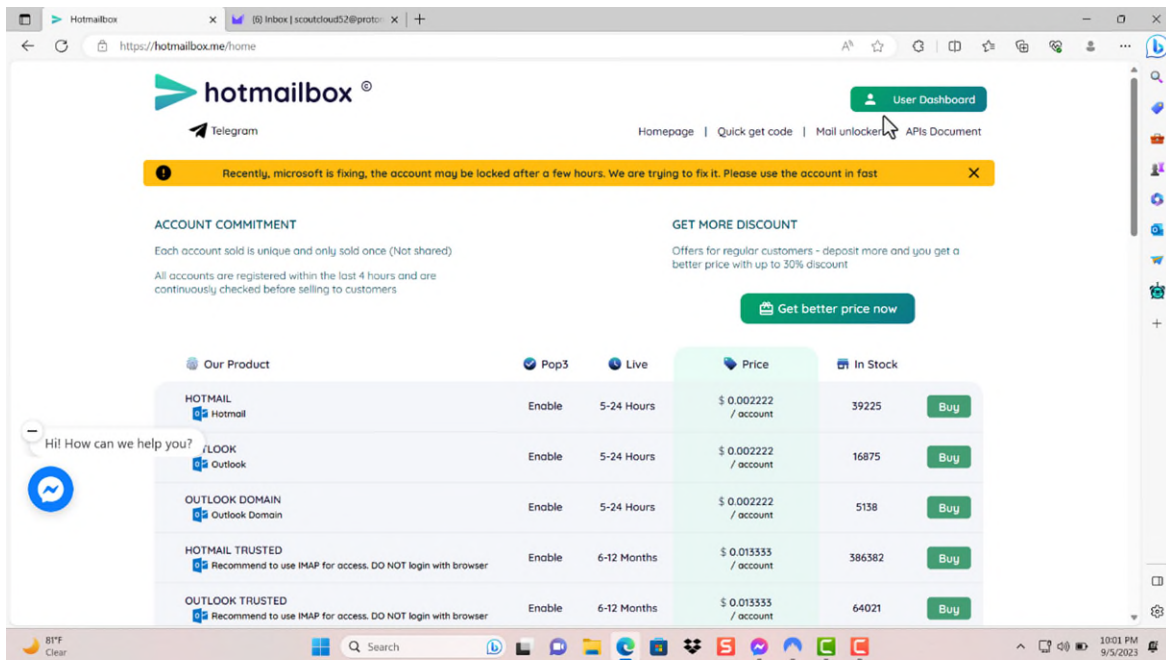


Fig. 2

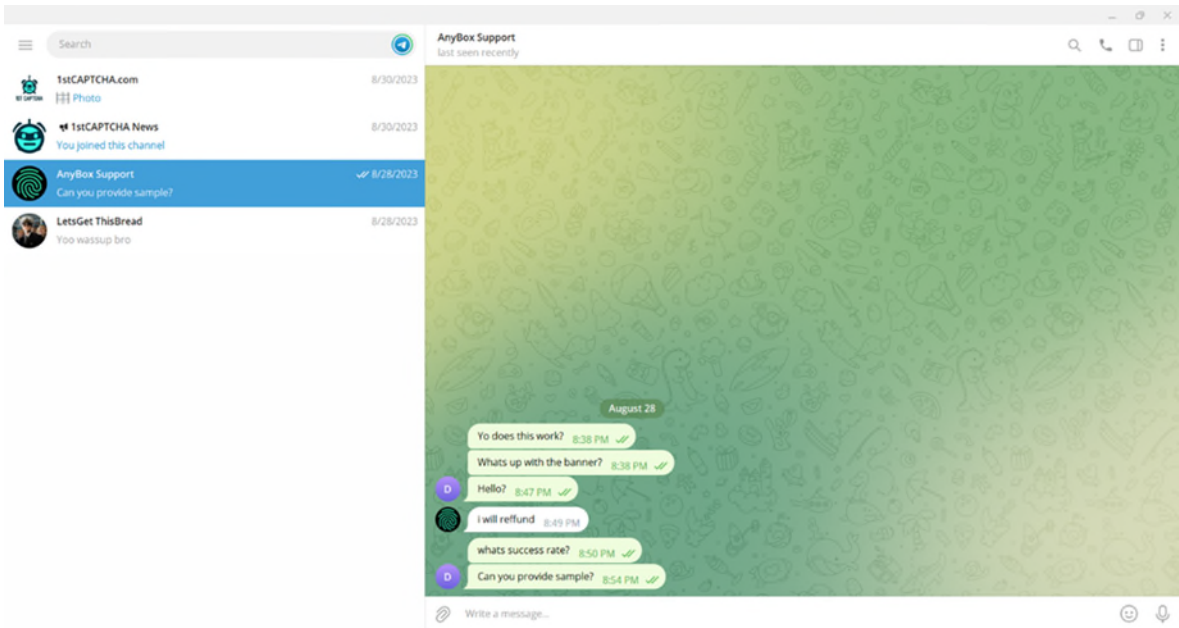


Fig. 3

19. Also on or about September 5, 2023, while still located in New York City, I navigated to the Hotmailbox payment portal, as seen in Figure 4, and deposited \$50.00 USD in BTC through payment processor Cryptomus Pay. The recipient BTC address was bc1qclne6hdnr9jvrgmr8q0z2xcdwzkkjm382p9ysc, as seen in Figure 4A. I received a payment confirmation, as seen in Figure 4B.

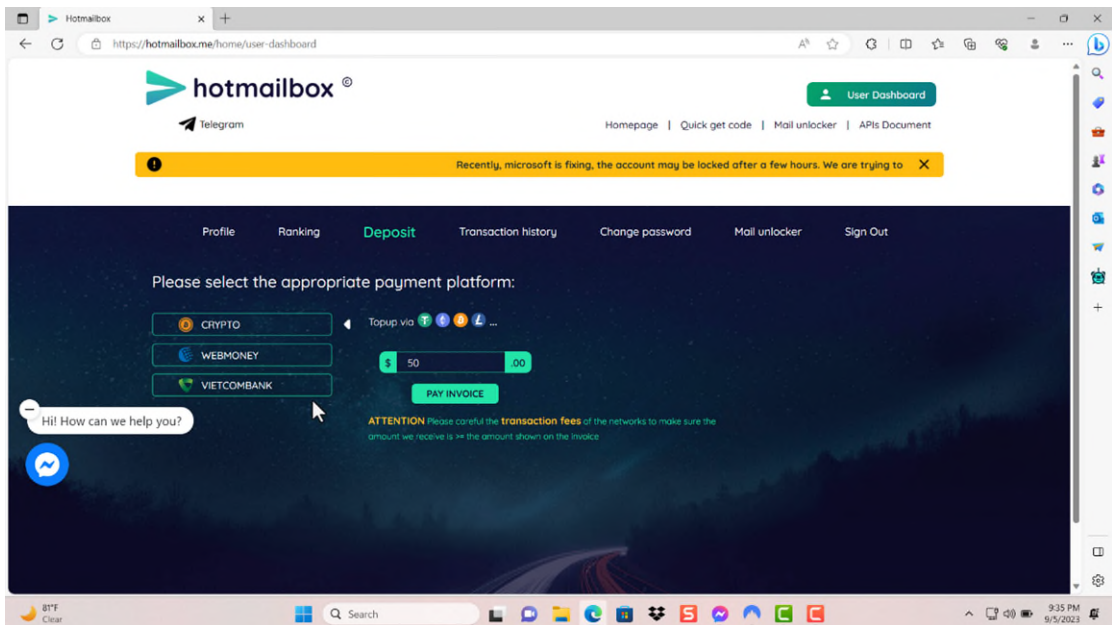


Fig. 4

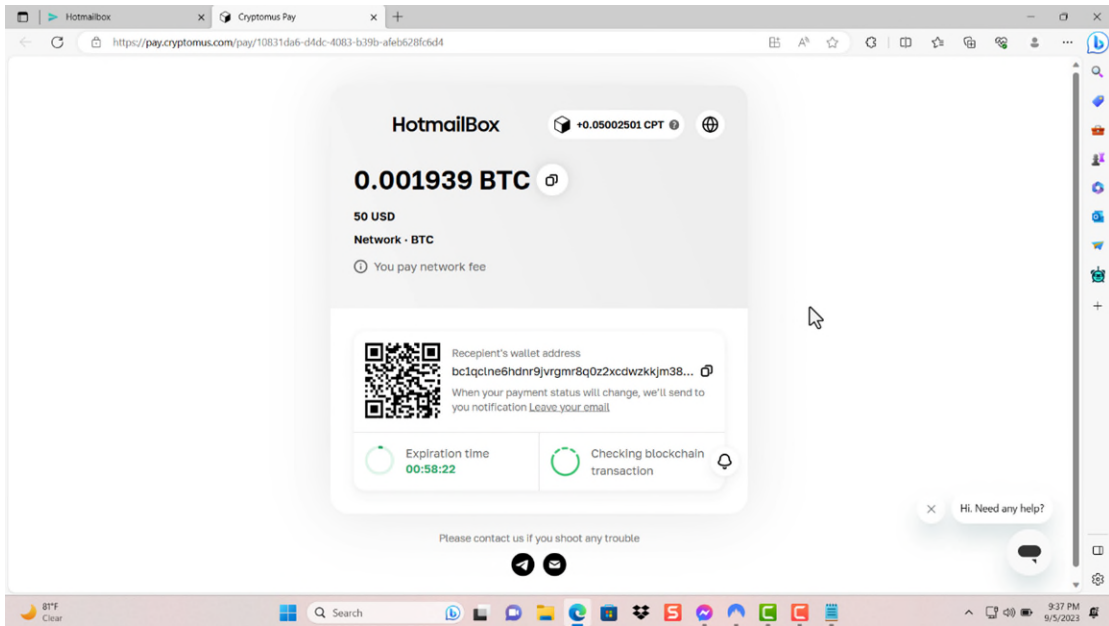


Fig. 4A

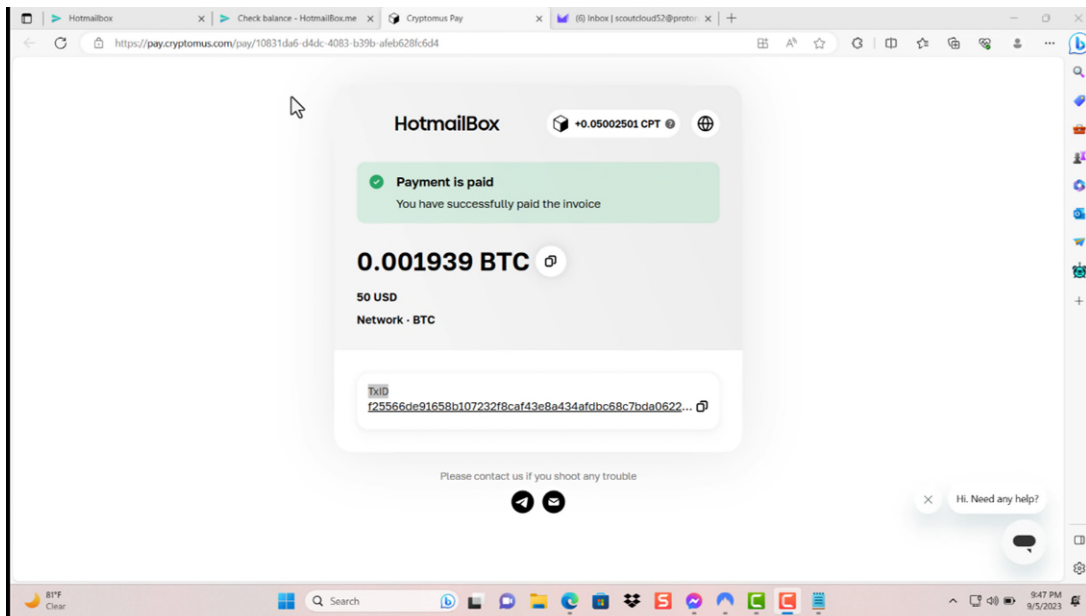


Fig. 4B

20. Following the deposit, I navigated to the Hotmailbox main page where I was able to buy MSAs, as seen in Figure 5. I purchased 9,300 MSAs, including 2,500 Outlook MSAs, as seen in Figure 5A and Figure 5B; 2,500 Outlook Domain MSAs; 2,500 Hotmail MSAs; 1,500

Outlook Trusted MSAs; 150 Outlook MSAs containing the country code top-level domain (ccTLD) for the country of Spain, and 150 Outlooks MSAs containing the ccTLD for the Republic of Korea.

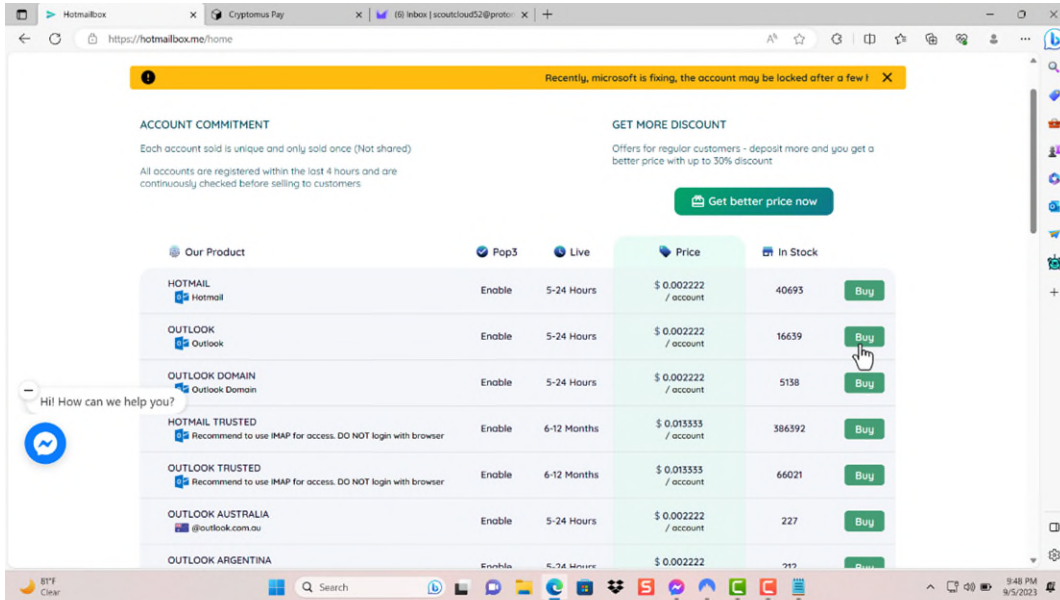


Fig. 5

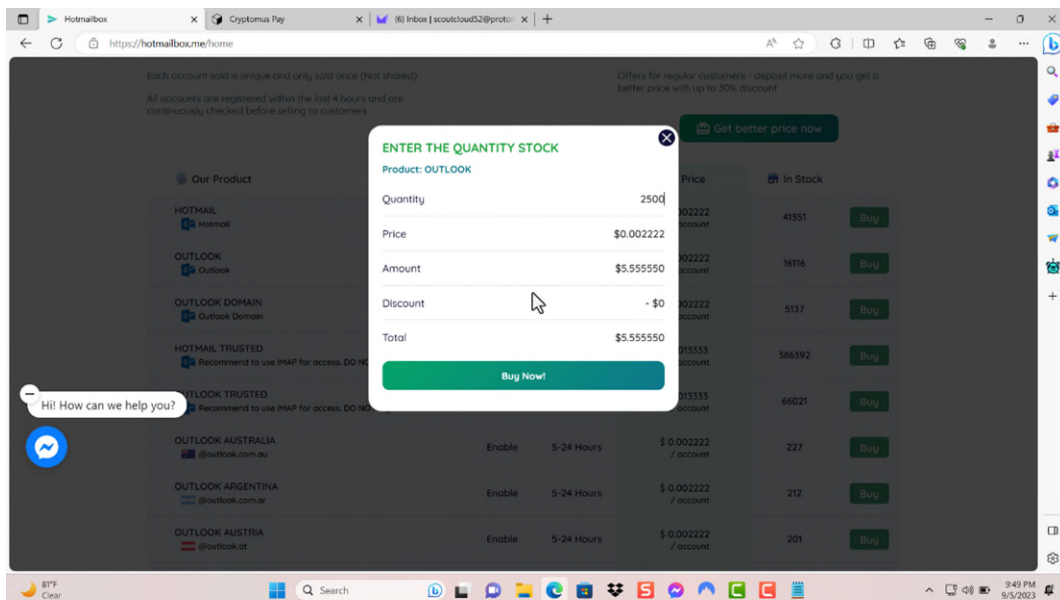


Fig. 5A

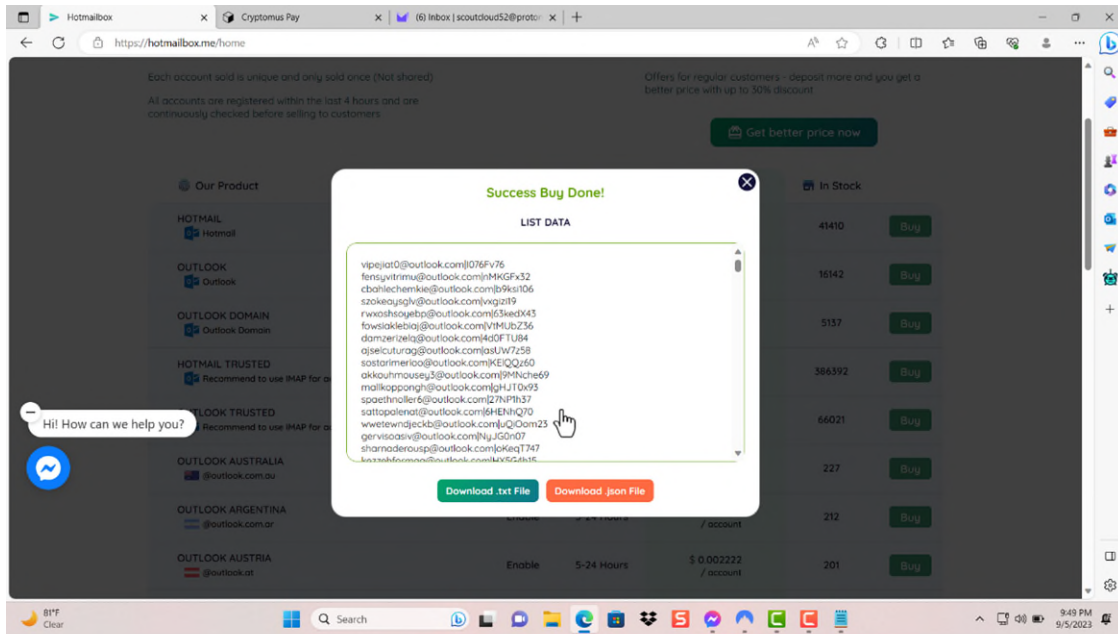


Fig. 5B

21. My review of MSA registration logs provided by Microsoft relating to the first two Outlook accounts listed in Fig. 5B confirmed that the vipejiat0@outlook.com account was created on or about September 6, 2023, at or about 12:52:10 AM, and the fensyvitrimu@outlook.com account was also created on or about September 6, 2023, at or about 12:52:10 AM.

IV. 1stCAPTCHA UNDERCOVER BUYS

22. On or about August 24, 2023, I navigated to www.1stCAPTCHA.com and viewed the landing page, as seen in Figure 6. I scrolled down the page to see the “Supported CAPTCHA Types & Pricing” and specifically observed one of the supported CAPTCHA types was

FunCAPTCHA for Outlook with a price of \$2.50 per 1,000 tokens and a touted accuracy of 100%, as noted in Figure 6A.

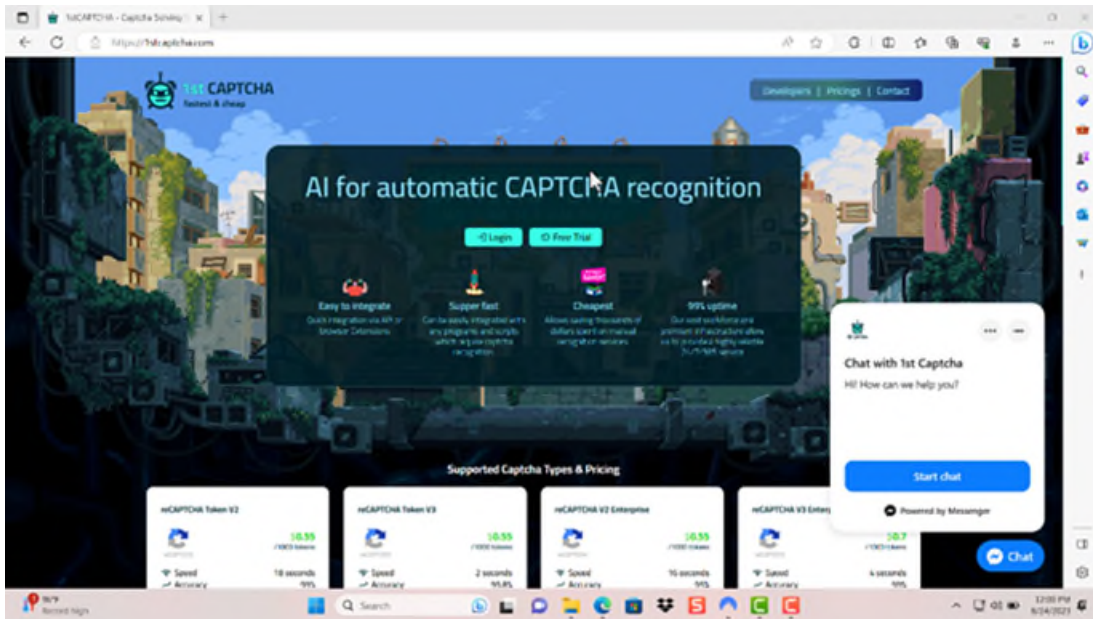


Fig. 6

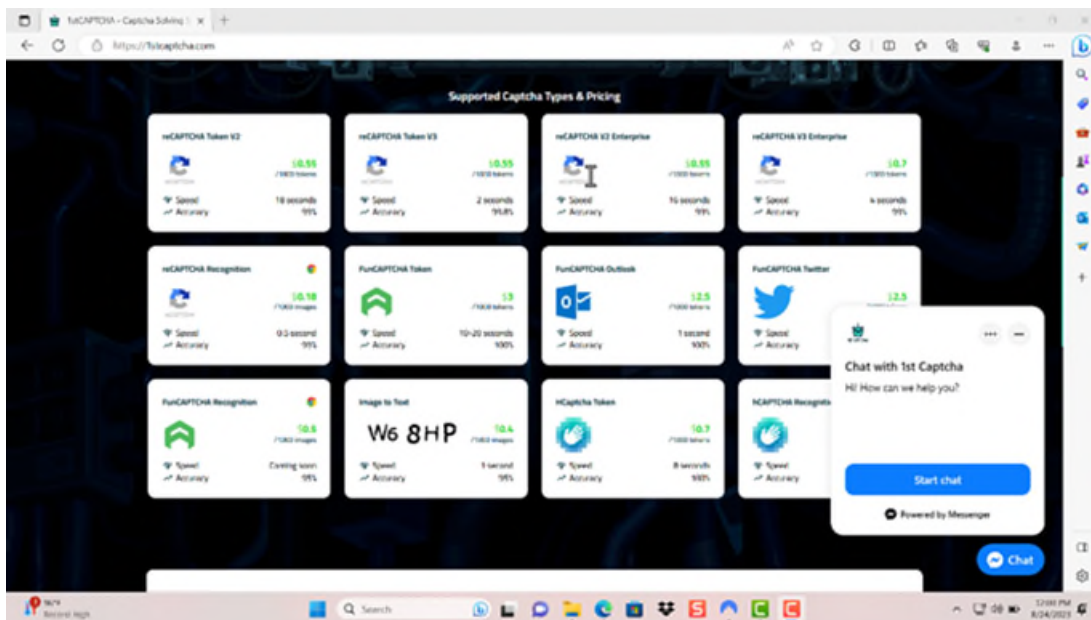


Fig. 6B

23. On or about August 30, 2023, I navigated back to 1stCAPTCHA and created an account, as seen in Figure 7. I deposited \$50.00 USD worth of BTC into my 1stCAPTCHA

account using the payment processor Sellix. The recipient BTC address, which is a unique identifier that serves as a virtual location where cryptocurrency may be sent, was bc1q6agg5ng0lgylc3uudrxelc9gr5ky9ltejhau5l. I also deposited \$50.00 USD worth of BTC into my 1stCAPTCHA account using the payment processor Cryptomus Pay. The recipient BTC address was bc1q0rme2vjlc2jpgfpv4x452hl6q02npgjrfa9zkq.

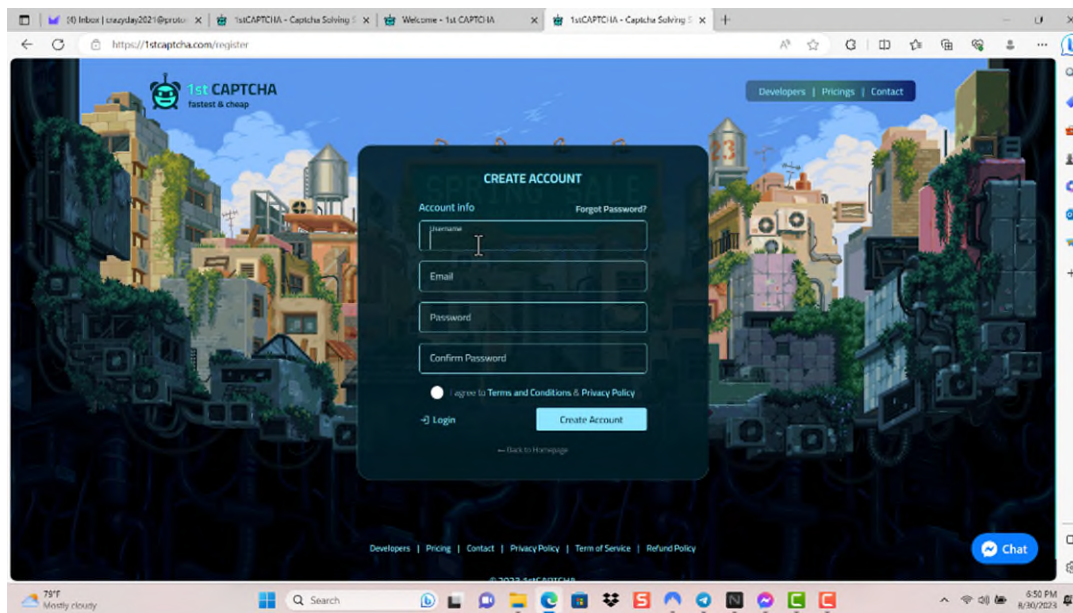


Fig 7

24. While investigating how to buy tokens on 1stCAPTCHA, I sent a message to the 1stCAPTCHA provided Telegram contact, 1stCAPTCHA.com, @the_1stcaptcha. When I asked where I could purchase FunCAPTCHA tokens, the 1stCAPTCHA contact responded, “Bypass reCAPTCHA, HCAPTCHA, FunCAPTCHA, Image CAPTCHA for the cheapest price and fastest. No user interaction required...,” as seen on Figure 8. I also communicated with the 1stCAPTCHA Messenger contact and asked about a tutorial. The 1st Captcha contact responded on or about August 31, 2023 that “you deposit money and then use the default apikey. For each successful request, the system will automatically deduct money,” as seen in Figure 9.

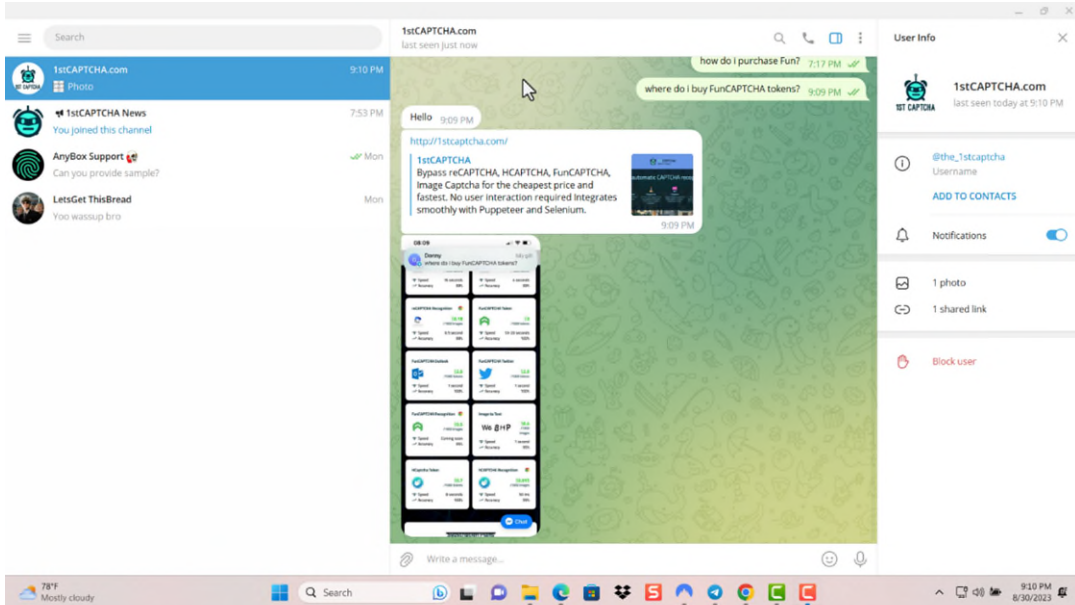


Fig. 8

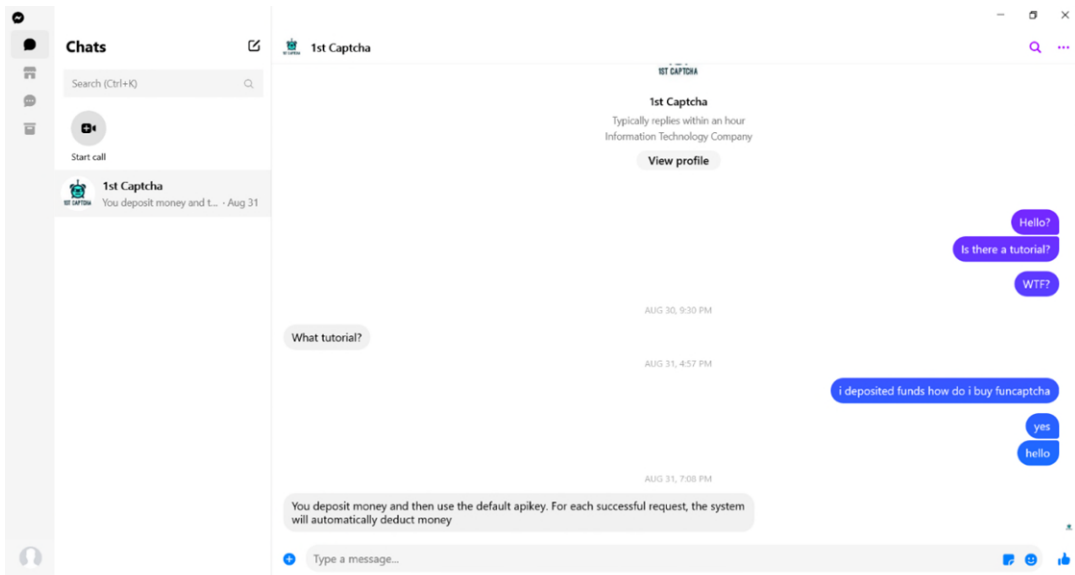


Fig. 9

25. On or about October 10, 2023, I logged into 1stCAPTCHA.com and navigated to docs.1stcaptcha.com where I located instructions to create a script to integrate with the 1stCAPTCHA Application Programming Interface (API). I know from my training and experience that an API is a set of rules and specifications that allow different software applications

to interact with each other and exchange data. Specifically, 1stCAPTCHA provides a token API that allows a user to input three parameters into a string of code that when executed in my browser, will return certain values, such as a TaskID and a token, as well as an indication of success or failure. As seen in Figure 10, the required parameters are (1) an API Key (or an “apikey,” which authenticates the user and allows their API to interact with other software applications) unique to my user account, to be used for accounting and payment; (2) a FunCAPTCHA sitekey, which is in the target website; and (3) the siteURL, which is the browser address where the FunCAPTCHA appears.

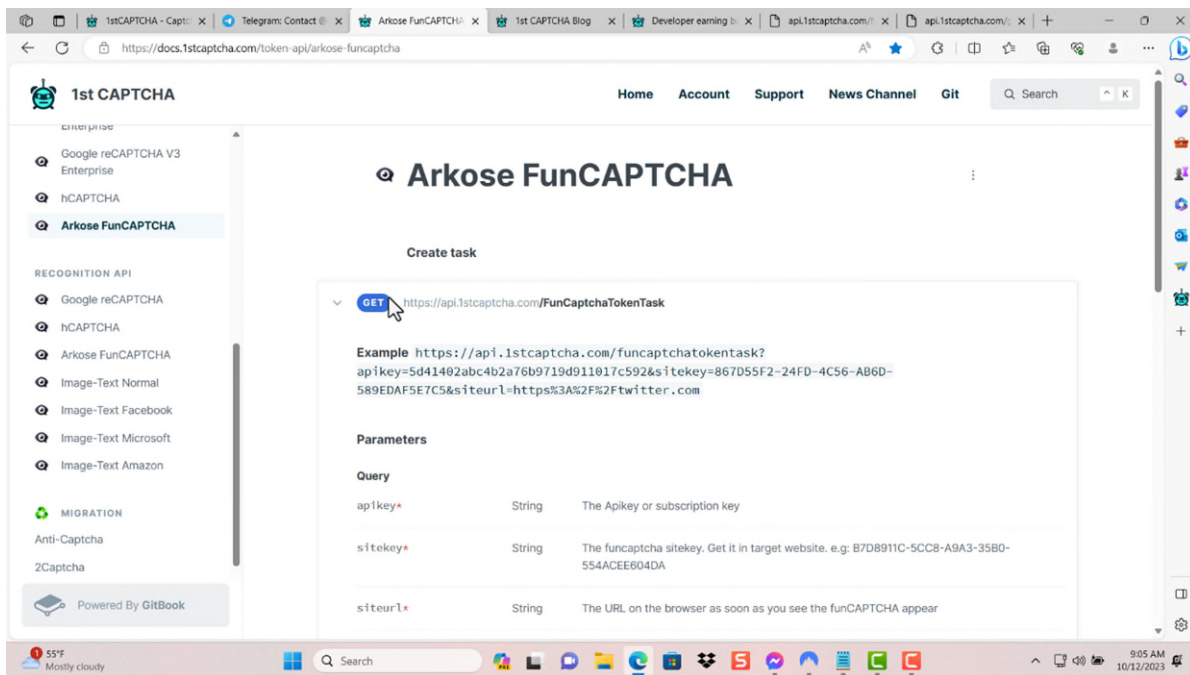


Fig. 10

26. Obtaining the token is a two-step process. First, using the input parameters discussed in Figure 10, a user enters a string of code to return a unique TaskID, as seen in Figure 11. Second, the TaskID is added to a new string of code that, when run, will return a token, as

seen in Figure 12, that is submitted in the webpage via JavaScript, which then indicates that the CAPTCHA puzzle was solved successfully.



Fig. 11



Fig.12

27. After running Step 2, in Figure 12, I successfully obtained a “token,” as seen in Figure 13.⁴ On or about October 12, 2023, a representative from Arkose Labs (Microsoft’s

⁴ I understand that Paragraph 5 of the Boffa Declaration contains a description of the how these CAPTCHA-defeating “tokens” function, familiarity with which is presumed.

CAPTCHA provider) confirmed that the token I purchased from 1stCAPTCHA on or about October 10, 2023, was valid.

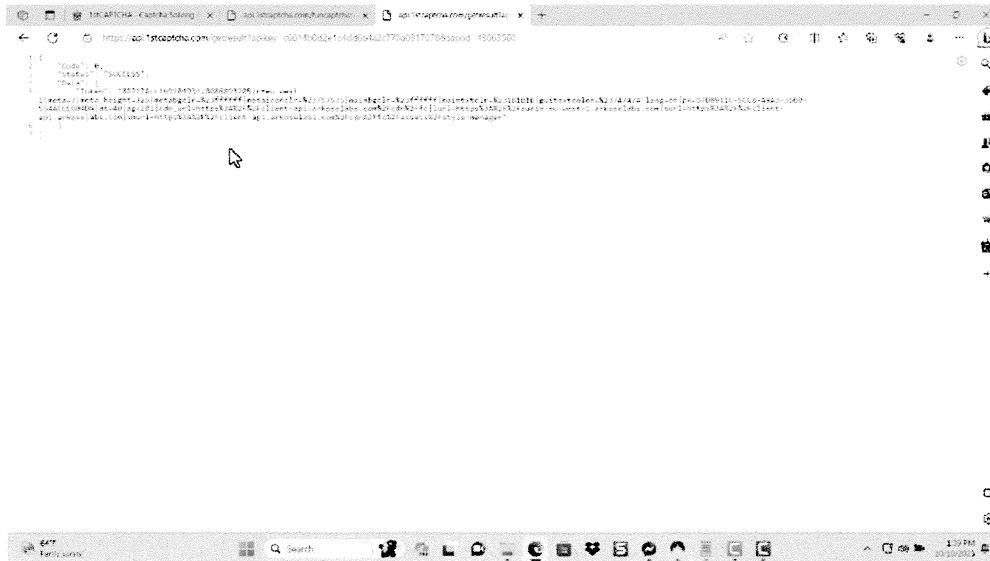
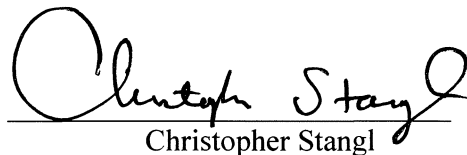


Fig. 13

28. On or about October 12, 2023, while located in New York City, I logged into 1stCAPTCHA.com and purchased ten additional tokens in the same manner described above.

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct.

Executed on this 1st day of December, 2023 in Washington, D.C.


Christopher Stangl