**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

|  |  |  |
|---|---|---|
| ------------------------------------------x |  |  |
| MICROSOFT CORPORATION, | : |  |
|  | : |  |
| Plaintiff, | : | **Case No.** |
| -against- | : |  |
|  | : |  |
| DUONG DINH TU, | : |  |
| LINH VAN NGUYEN, and | : |  |
| TAI VAN NGUYEN, | : | **<u>REQUEST TO FILE UNDER SEAL</u>** |
|  | : |  |
| Defendants. | : |  |
| ------------------------------------------x |  |  |

# DECLARATION OF MAURICE MASON IN SUPPORT OF PLAINTIFF MICROSOFT'S MOTION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

I, Maurice Mason, declare as follows:

1. I am a Senior Investigator in the Digital Crimes Unit ("DCU") Cybercrime Enforcement Team ("CET") at Microsoft Corporation. I respectfully submit this declaration in support of Microsoft's motion for an emergency *ex parte* temporary restraining order and order to show cause why a preliminary injunction should not be entered in the above-captioned case.

2. I have been employed by Microsoft since August 2021. In my role, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft's online service assets from network-based attacks. Prior to my current role, I worked as a Senior Consultant on Microsoft's Incident Response Team, where I was a lead digital forensic analyst managing multiple incident response and threat-hunting engagements that included performing incident response and forensic analysis for Fortune 500, Fortune 100, and Fortune 50 companies. Prior to joining Microsoft, I

held various positions, both in the private sector and in government, where I performed digital forensic analysis, including on malware and ransomware-related matters. A true and correct copy of my curriculum vitae is attached to this declaration as Exhibit 1.

3. Since in or about May 2023, I have been investigating the structure and function of an online criminal enterprise operated by Defendants—referred to herein as the "Fraudulent Enterprise" (or the "Enterprise")—that is in the business of using fraud to bypass Microsoft's security systems, open Microsoft accounts in the names of fictitious persons, and sell these fake Microsoft accounts to cybercriminals for a wide variety of internet-based crimes (the "Fraudulent Scheme").

4. I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during Microsoft's investigation of the Fraudulent Enterprise.

## I. **Background**

5. The Fraudulent Enterprise attacks Microsoft, its Outlook.com ("Outlook") email services, its customers, and third parties by using fraud to procure Microsoft email accounts, which it then sells, along with other security-bypassing technology, to cybercriminals. The Enterprise sells these cybercrime tools via websites associated with the domain name "hotmailbox.me" (the "Hotmailbox Website") and "1stcaptcha.com" (the "1stCAPTCHA Website," formerly "Anycaptcha.com," or the "AnyCAPTCHA Website").

## II. **Attribution of the Defendants to the CAPTCHA Fraud**

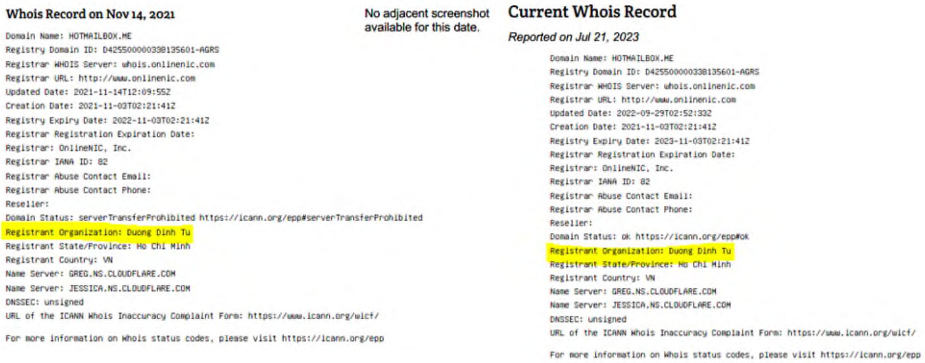
6. Based on research I conducted as part of Microsoft's investigation of the Fraudulent Enterprise, and based on information and belief, I have been able to draw the following

connections between Defendants Duong Dinh Tu, Linh Van Nguyen (a/k/a Nguyen Van Linh), and Tai Van Nguyen.

### A. Duong Dinh Tu

7. Based on my analysis of WHOIS results (which are internet record listings that provide information about website domains) for the Hotmailbox Website, Defendant Duong Dinh Tu has been the registrant of Hotmailbox.me from at least in or about November 2021 through in or about July 2023. A screenshot of these WHOIS results, indicating that Tu is the registrant of the Hotmailbox Website, is reflected in Figure 1 below.

**FIGURE 1**



**Whois Record on Nov 14, 2021**

```
Domain Name: HOTMAILBOX.ME
Registry Domain ID: D425500000338135601-AGRS
Registrar WHOIS Server: whois.onlinenic.com
Registrar URL: http://www.onlinenic.com
Updated Date: 2021-11-14T12:09:55Z
Creation Date: 2021-11-03T02:21:41Z
Registry Expiry Date: 2022-11-03T02:21:41Z
Registrar Registration Expiration Date:
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Registrant Organization: Duong Dinh Tu
Registrant State/Province: Ho Chi Minh
Registrant Country: VN
Name Server: GREG.NS.CLOUDFLARE.COM
Name Server: JESSICA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

For more information on Whois status codes, please visit https://icann.org/epp
```

No adjacent screenshot available for this date.

**Current Whois Record**

*Reported on Jul 21, 2023*

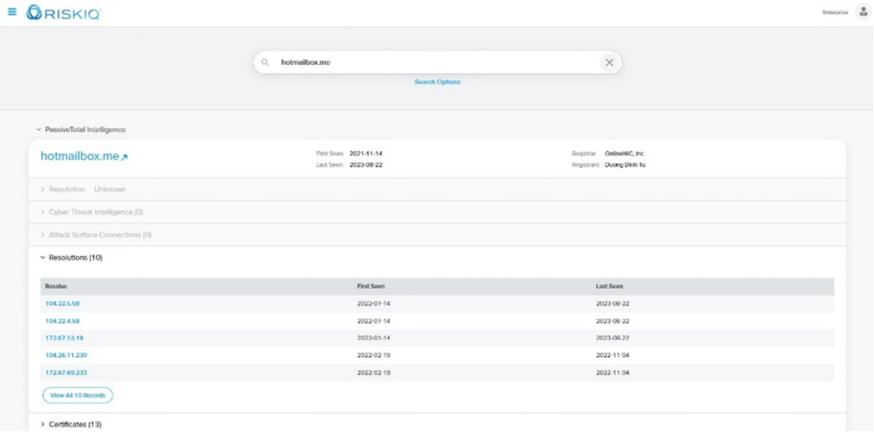
```
Domain Name: HOTMAILBOX.ME
Registry Domain ID: D425500000338135601-AGRS
Registrar WHOIS Server: whois.onlinenic.com
Registrar URL: http://www.onlinenic.com
Updated Date: 2022-09-29T02:52:33Z
Creation Date: 2021-11-03T02:21:41Z
Registry Expiry Date: 2023-11-03T02:21:41Z
Registrar Registration Expiration Date:
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registrant Organization: Duong Dinh Tu
Registrant State/Province: Ho Chi Minh
Registrant Country: VN
Name Server: GREG.NS.CLOUDFLARE.COM
Name Server: JESSICA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

For more information on Whois status codes, please visit https://icann.org/epp
```

8. I have also analyzed the Hotmailbox Website's registration and hosting information, as gathered from RiskIQ (a tool which provides internet reconnaissance and analytics). That information, as reflected in Figure 2 below, lists Defendant Duong Dinh Tu as the Hotmailbox Website's registrant. It also shows that the Website's registrar is OnlineNIC, Inc., and that the Website's Autonomous System Number ("ASN")[1] is provided by Cloudflare.

[1] An ASN is a collection of the Internet Protocol (IP) addresses that can be accessed from a particular network. An IP address is a unique identifying number that is assigned to every device connected to the internet.

**FIGURE 2**



RISKIQ

Enterprise

hotmailbox.me

Search Options

PassiveTotal Intelligence

hotmailbox.me

First Seen 2021-11-14
Last Seen 2023-08-22

Registrar OnlineNIC, Inc.
Registrant Duong Dinh Tu

Reputation Unknown

Cyber Threat Intelligence (0)

Attack Surface Connections (0)

Resolutions (10)

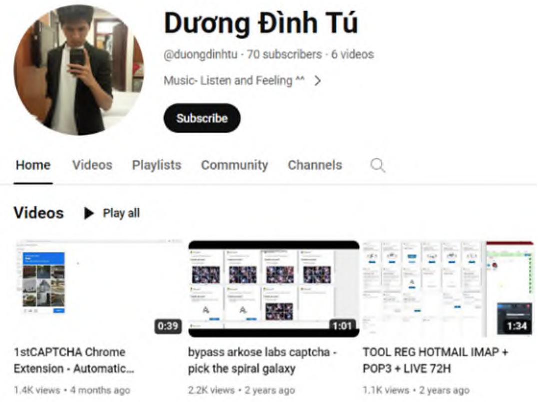
| Resolve | First Seen | Last Seen |
|---|---|---|
| 104.22.5.58 | 2022-01-14 | 2023-08-22 |
| 104.22.4.58 | 2022-01-14 | 2023-08-22 |
| 172.67.13.19 | 2022-01-14 | 2023-08-22 |
| 104.26.11.230 | 2022-02-19 | 2022-11-04 |
| 172.67.69.233 | 2022-02-19 | 2022-11-04 |

View All 10 Records

Certificates (13)

9. Defendant Duong Dinh Tu publicizes the Hotmailbox and 1stCAPTCHA tools—including instructional YouTube videos on how they can be used to bypass Microsoft's security measures (namely, its CAPTCHA defense system, which is operated by third party Arkose Labs)—on his personal YouTube page "@duongdinhtu" (which is available at https://www.youtube.com/@duongdinhtu). Those YouTube videos, as reflected in Figure 3 below, are (i) "TOOL REG HOTMAIL IMAP + POP3 + LIVE 72H" (posted on November 19, 2020); (ii) "bypass arkose labs captcha — pick the spiral galaxy" (posted on December 27, 2020); and (iii) 1stCAPTCHA Chrome Extension — Automatic reCAPTCHA Solver (posted on July 3, 2023).

**FIGURE 3**



Dương Đình Tú

@duongdinhtu · 70 subscribers · 6 videos

Music- Listen and Feeling ^^

Subscribe

Home Videos Playlists Community Channels

Videos ▶ Play all

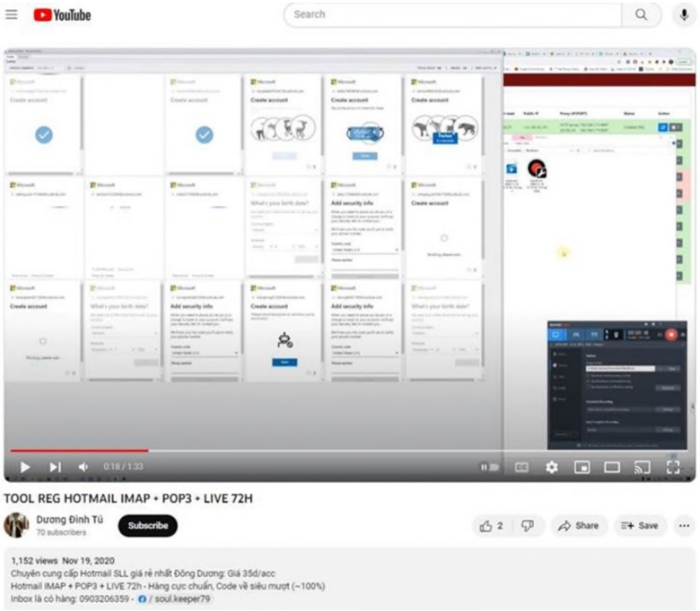
0:39
1stCAPTCHA Chrome Extension - Automatic...
1.4K views • 4 months ago

1:01
bypass arkose labs captcha - pick the spiral galaxy
2.2K views • 2 years ago

1:34
TOOL REG HOTMAIL IMAP + POP3 + LIVE 72H
1.1K views • 2 years ago

10. The YouTube video “TOOL REG HOTMAIL IMAP + POP3 + LIVE 72H,” which was posted on YouTube by Defendant Duong Dinh Tu on November 19, 2020,[2] shows a bot[3] simultaneously creating dozens of Microsoft accounts with unique usernames as each automatically proceeds through different stages of the Microsoft account creation process. In this video, the bot solves CAPTCHA[4] puzzles by correctly positioning animal pictures (as reflected in Figure 4 below), eventually leading to a false verification that the bot is a real person. The video also shows the bot automatically bypassing other steps of the account creation process by filling in randomly generated birth dates and by selecting “Vietnam” as its “Country/region.”

**FIGURE 4**



TOOL REG HOTMAIL IMAP + POP3 + LIVE 72H

Dương Đình Tú
70 subscribers

1,152 views Nov 19, 2020
Chuyên cung cấp Hotmail SLL giá rẻ nhất Đông Dương: Giá 35d/acc
Hotmail IMAP + POP3 + LIVE 72h - Hàng cực chuẩn, Code về siêu mượt (~100%)
Inbox là có hàng: 0903206359 - / soul.keeper79

[2] This video is available at https://www.youtube.com/watch?v=BH_QNZpO9TI.

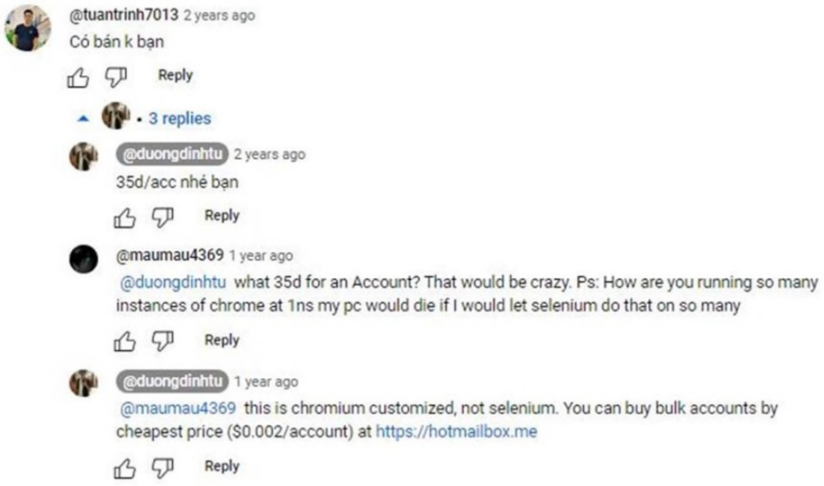
[3] Bots are software programs that simulate human user behavior and perform repetitive, automated tasks.

[4] I understand a description of CAPTCHA can be found in paragraphs 5 through 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.

11. The video's description states the following in Vietnamese: "Chuyên cung cấp Hotmail SLL giá rẻ nhất Đông Dương: Giá 35d/acc Hotmail IMAP + POP3 + LIVE 72h - Hàng cực chuẩn, Code về siêu mượt (~100%) Inbox là có hàng: 0903206359 - / soul.keeper79." According to Google's publicly available translation service, this means: "Specializing in providing Hotmail SLL at the cheapest price in Indochina: Price 35d/acc Hotmail IMAP + POP3 + LIVE 72h - Extremely standard product, Code delivery is super smooth (~100%) Inbox for availability: 0903206359 - /soul.keeper79[.]"

12. As reflected below in Figure 5, in or about November 2022, Defendant Dinh Tu left the following comment on the "TOOL REG HOTMAIL IMAP + POP3 + LIVE 72H" video: "You can buy bulk accounts by cheapest price ($0.002/account) at https://hotmailbox.me."

**FIGURE 5**



@tuantrinh7013 2 years ago
Có bán k bạn

@duongdinhtu 2 years ago
35d/acc nhé bạn

@maumau4369 1 year ago
@duongdinhtu what 35d for an Account? That would be crazy. Ps: How are you running so many instances of chrome at 1ns my pc would die if I would let selenium do that on so many

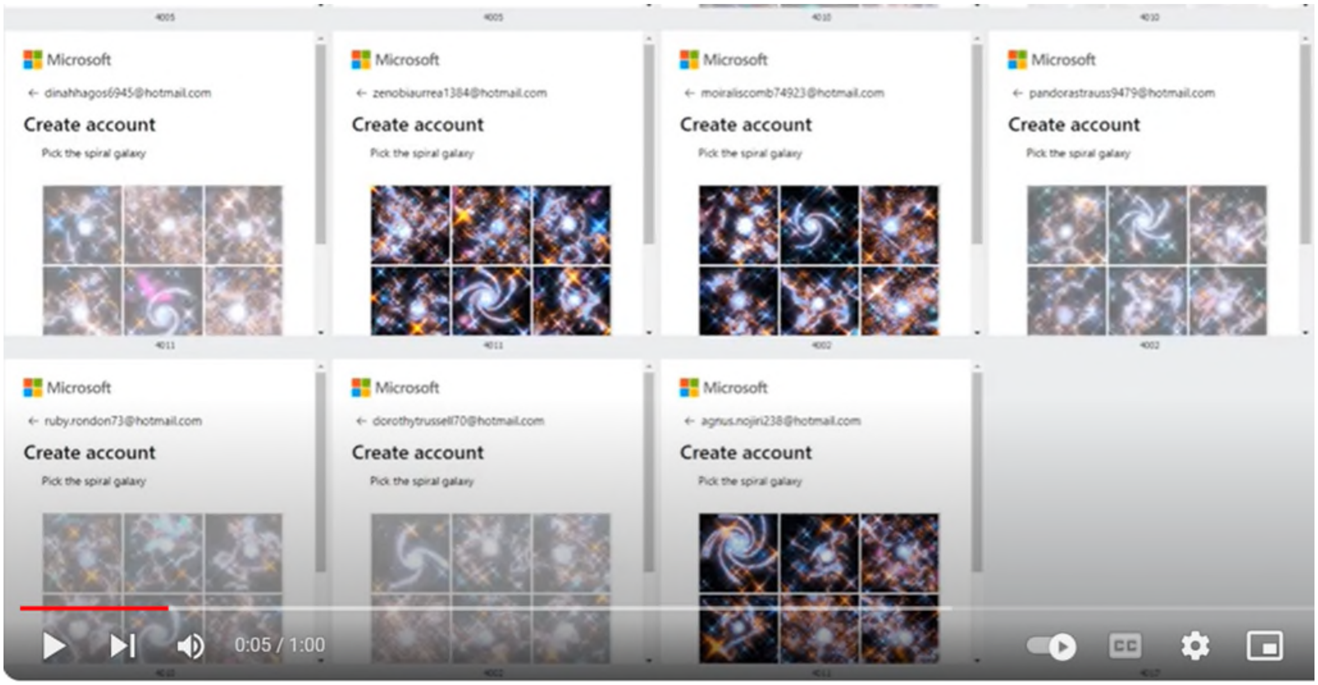
@duongdinhtu 1 year ago
@maumau4369 this is chromium customized, not selenium. You can buy bulk accounts by cheapest price ($0.002/account) at https://hotmailbox.me

13. The YouTube video "[B]ypass arkose labs captcha - pick the spiral galaxy," which was posted on YouTube by Defendant Duong Dinh Tu on December 27, 2020,[5] shows a bot simultaneously creating dozens of Microsoft accounts, which are each displayed on the screen with a unique email address and username. The usernames follow the general format of first name, last

[5] This video is available at https://www.youtube.com/watch?v=FaIp-Jcckk8.

name, and then a number. First, the bot is presented with a "Create account" screen, where it is asked to "Please solve the puzzle so we know you're not a robot." The video then shows the bot defeating the CAPTCHA puzzles, in which it must pick a spiral galaxy among several picture options, as reflected below in Figure 6. The video concludes by showing that the accounts were successfully created on the Microsoft website.

**FIGURE 6**



Microsoft
← dinahhagos6945@hotmail.com
Create account
Pick the spiral galaxy

Microsoft
← zenobiaurrea1384@hotmail.com
Create account
Pick the spiral galaxy

Microsoft
← moiraliscomb74923@hotmail.com
Create account
Pick the spiral galaxy

Microsoft
← pandorastrauss9479@hotmail.com
Create account
Pick the spiral galaxy

Microsoft
← ruby.rondon73@hotmail.com
Create account
Pick the spiral galaxy

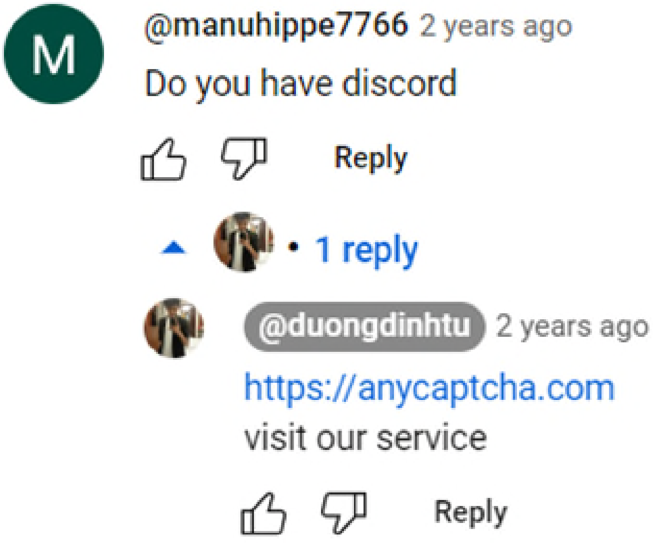
Microsoft
← dorothytrussell70@hotmail.com
Create account
Pick the spiral galaxy

Microsoft
← agnus.nojiri238@hotmail.com
Create account
Pick the spiral galaxy

14. The video's description states: "This captcha too ez for bypass!"

15. As reflected below in Figure 7, in or about November 2021, Defendant Dinh Tu left a comment in response to the video, directing viewers to the AnyCAPTCHA Website.

**FIGURE 7**



@manuhippe7766 2 years ago

Do you have discord

@duongdinhtu 2 years ago

https://anycaptcha.com

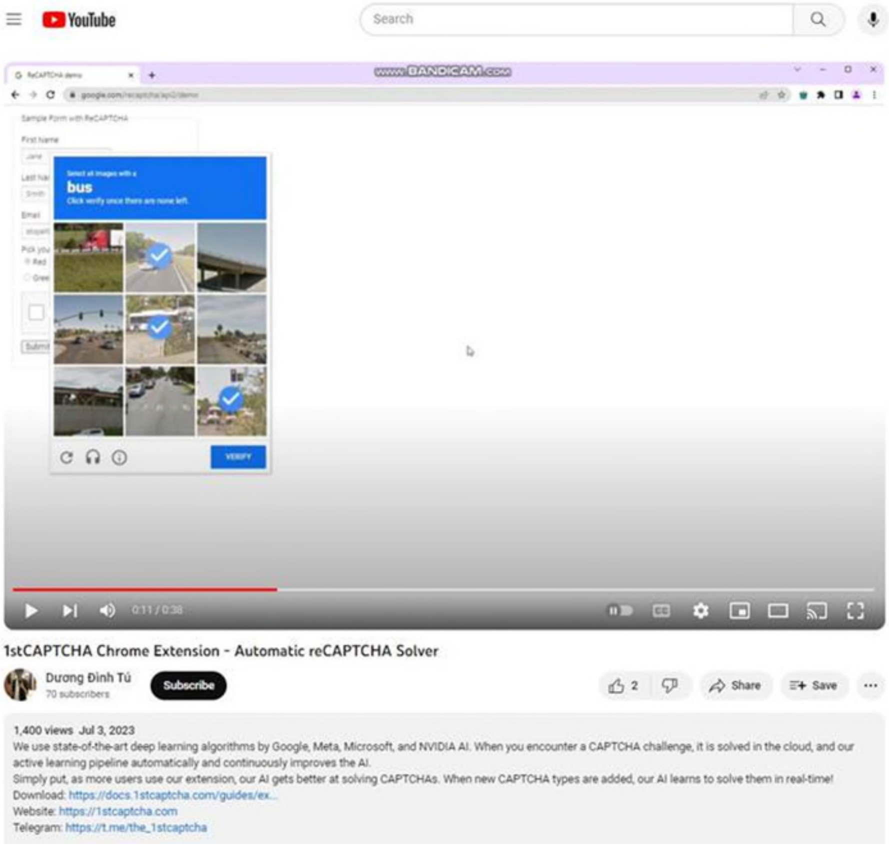
visit our service

16. The YouTube video "1stCAPTCHA Chrome Extension - Automatic reCAPTCHA Solver," which was posted on YouTube by Defendant Duong Dinh Tu on July 3, 2023,[6] shows a user clicking on the 1stCAPTCHA Google Chrome extension, which then displays a balance amount and a link to the CAPTCHA defeating software. The user then selects "reCAPTCHA" among the Chrome favorites on the Google homepage, which directs the user to a "Sample Form with ReCAPTCHA" page. At the 0:08 mark of the video, a sample reCAPTCHA appears in which the user is asked to "[s]elect all images with a bus," among nine different images, and to "[c]lick verify once there are none left." As reflected below in Figure 8, the video (at 0:11) shows the correct images being selected while the mouse remains to the right of the screen, away from the puzzle. Once the images are selected on the screen, the video shows a checkbox being filled in

[6] This video is available at https://www.youtube.com/watch?v=Me4qnLu3UKM.

automatically, next to the phrase "I'm not a robot." The video then shows the process a second time, with another reCAPTCHA puzzle of bus images.

**FIGURE 8**



1stCAPTCHA Chrome Extension - Automatic reCAPTCHA Solver

Dương Đình Tú
70 subscribers

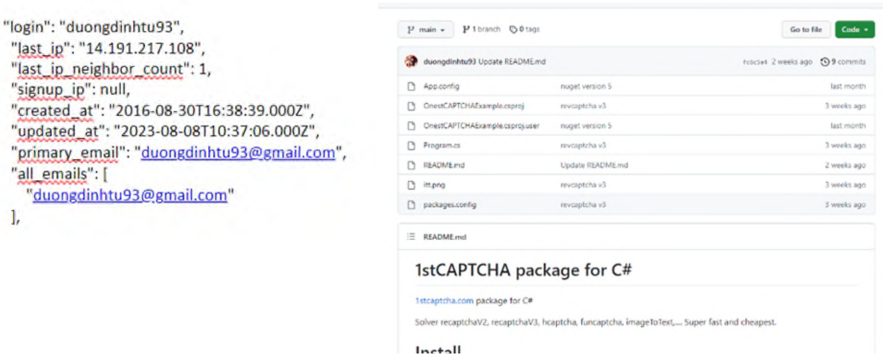
1,400 views Jul 3, 2023
We use state-of-the-art deep learning algorithms by Google, Meta, Microsoft, and NVIDIA AI. When you encounter a CAPTCHA challenge, it is solved in the cloud, and our active learning pipeline automatically and continuously improves the AI.
Simply put, as more users use our extension, our AI gets better at solving CAPTCHAs. When new CAPTCHA types are added, our AI learns to solve them in real-time!
Download: https://docs.1stcaptcha.com/guides/ex...
Website: https://1stcaptcha.com
Telegram: https://t.me/the_1stcaptcha

17. The video's description states: "We use state-of-the-art deep learning algorithms by Google, Meta, Microsoft, and NVIDIA AI. When you encounter a CAPTCHA challenge, it is solved in the cloud, and our active learning pipeline automatically and continuously improves the AI. Simply put, as more users use our extension, our AI gets better at solving CAPTCHAs. When new CAPTCHA types are added, our AI learns to solve them in real-time!"

18. Based on my review of information within and derived from the 1stCAPTCHA GitHub webpage—which houses source code for software programs run by 1stCaptcha.com to bypass Microsoft's CAPTCHA defense system, as seen below in Figure 9—an individual with the

username “duongdinhtu93,” and with the email address “duongginhtu93@gmail.com,” has edited the 1stCAPTCHA source code several times, including as recently as August 8, 2023. I believe this individual to be Defendant Duong Dinh Tu.

**FIGURE 9**



```
"login": "duongdinhtu93",
 "last_ip": "14.191.217.108",
 "last_ip_neighbor_count": 1,
 "signup_ip": null,
 "created_at": "2016-08-30T16:38:39.000Z",
 "updated_at": "2023-08-08T10:37:06.000Z",
 "primary_email": "duongdinhtu93@gmail.com",
 "all_emails": [
   "duongdinhtu93@gmail.com"
 ],
```

duongdinhtu93 Update README.md fc6c5a4 2 weeks ago 9 commits

| | | |
|---|---|---|
| App.config | nuget version 5 | last month |
| OnestCAPTCHAExample.csproj | revcaptcha v3 | 3 weeks ago |
| OnestCAPTCHAExample.csproj.user | nuget version 5 | last month |
| Program.cs | revcaptcha v3 | 3 weeks ago |
| README.md | Update README.md | 2 weeks ago |
| itt.png | revcaptcha v3 | 3 weeks ago |
| packages.config | revcaptcha v3 | 3 weeks ago |

README.md

1stCAPTCHA package for C#

1stcaptcha.com package for C#

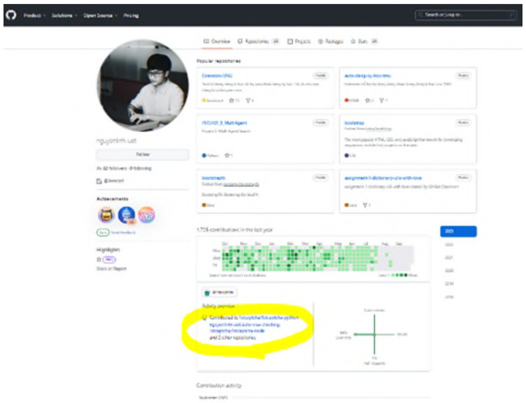
Solver recaptchaV2, recaptchaV3, hcaptcha, funcaptcha, imageToText,... Super fast and cheapest.

Install

## B. Linh Van Nguyen (a/k/a Nguyen Van Linh)

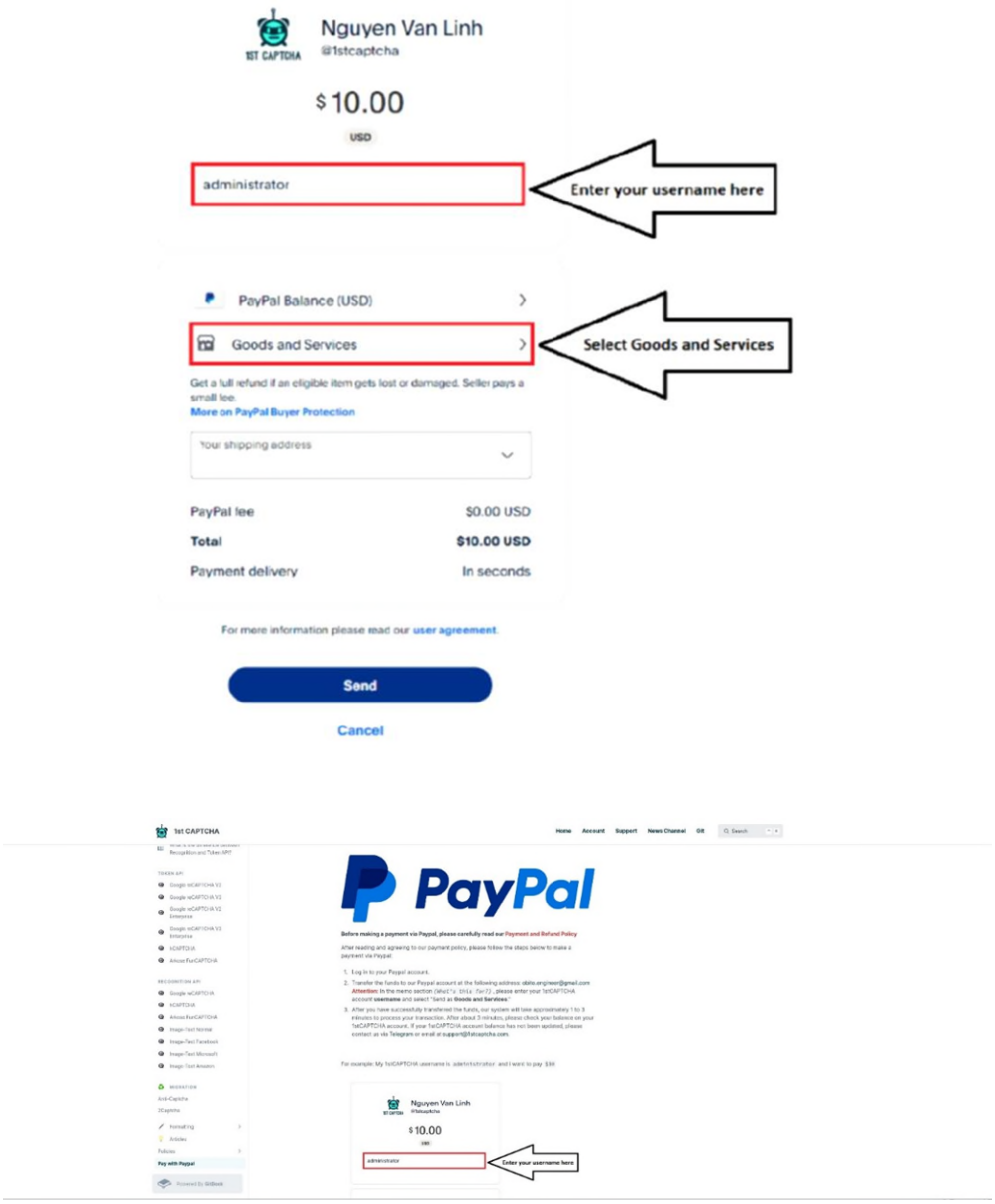
19. Based on my review of information within, derived from, and associated with the 1stCAPTCHA GitHub webpage, as seen below in Figure 10, an individual with the username “nguyenlinh-uet,” and with the email address “nguyenlinh.uet@gmail.com,” has edited the 1stCAPTCHA source code at least 115 times during the time span of approximately October 2020 through July 2023. The personal GitHub webpage of “nguyenlinh-uet” includes a link to the 1stCAPTCHA GitHub webpage, as further reflected in Figure 10. I believe this individual to be Defendant Linh Van Nguyen.

**FIGURE 10**



20. Based on my investigation of the 1stCAPTCHA Website and the methods of payment that may be used to purchase its services, and as reflected below in Figure 11, payments made to the 1stCAPTCHA Website through PayPal are made to "Nguyen Van Linh" as an "administrator" of the website. I believe "Nguyen Van Linh" to be Defendant Linh Van Nguyen (a/k/a Nguyen Van Linh).

**FIGURE 11**



Nguyen Van Linh
@1stcaptcha

$10.00
USD

administrator

Enter your username here

PayPal Balance (USD)

Goods and Services

Select Goods and Services

Get a full refund if an eligible item gets lost or damaged. Seller pays a small fee.
More on PayPal Buyer Protection

Your shipping address

| | |
|---|---|
| PayPal fee | $0.00 USD |
| Total | $10.00 USD |
| Payment delivery | In seconds |

For more information please read our user agreement.

Send

Cancel

**Before making a payment via Paypal, please carefully read our Payment and Refund Policy**

After reading and agreeing to our payment policy, please follow the steps below to make a payment via Paypal:

1. Log in to your Paypal account.
2. Transfer the funds to our Paypal account at the following address: obito.engineer@gmail.com
   Attention: In the memo section (What's this for?), please enter your 1stCAPTCHA account **username** and select "Send as **Goods and Services**."
3. After you have successfully transferred the funds, our system will take approximately 1 to 3 minutes to process your transaction. After about 3 minutes, please check your balance on your 1stCAPTCHA account. If your 1stCAPTCHA account balance has not been updated, please contact us via Telegram or email at support@1stcaptcha.com.

For example: My 1stCAPTCHA username is administrator and I want to pay $10

Nguyen Van Linh
@1stcaptcha

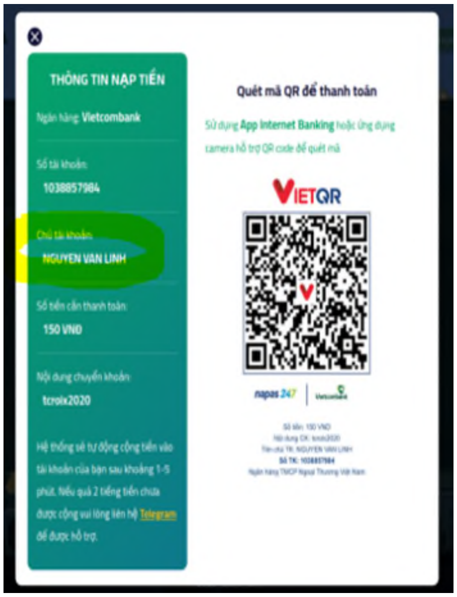
$10.00
USD

administrator

Enter your username here

21. Similarly, based on my investigation of the 1stCAPTCHA Website and the methods of payment that may be used to purchase its services, and as reflected below in Figure 12, payments made to the 1stCAPTCHA Website through Vietcombank are made to "NGUYEN VAN LINH." I believe "NGUYEN VAN LINH" to be Defendant Linh Van Nguyen (a/k/a Nguyen Van Linh).

**FIGURE 12**



THÔNG TIN NẠP TIỀN

Ngân hàng: Vietcombank

Số tài khoản:
1038857984

Chủ tài khoản:
NGUYEN VAN LINH

Số tiền cần thanh toán:
150 VND

Nội dung chuyển khoản:
tcroix2020

Hệ thống sẽ tự động cộng tiền vào tài khoản của bạn sau khoảng 1-5 phút. Nếu quá 2 tiếng tiền chưa được cộng vui lòng liên hệ Telegram để được hỗ trợ.

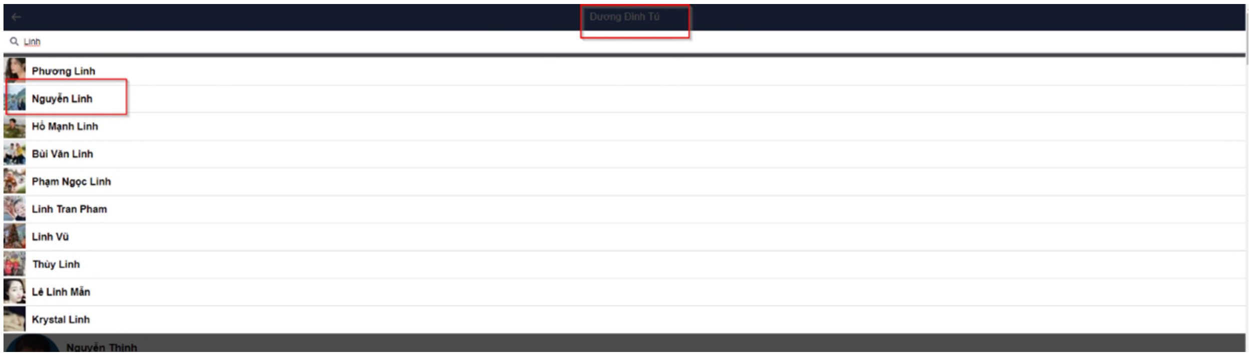
Quét mã QR để thanh toán

Sử dụng App Internet Banking hoặc ứng dụng camera hỗ trợ QR code để quét mã

Số tiền: 150 VND
Nội dung CK: tcroix2020
Tên chủ TK: NGUYEN VAN LINH
Số TK: 1038857984
Ngân hàng TMCP Ngoại Thương Việt Nam

22. Defendants Linh Van Nguyen (a/k/a Nguyen Van Linh) and Duong Dinh Tu are "friends" on Facebook, according to Duong Dinh Tu's Facebook "friends" list. A screenshot from the Facebook account of Duong Dinh Tu, showing that Tu is "friends" with "Nguyen Linh," is depicted in Figure 13 below. I believe "Nguyen Linh" to be Defendant Linh Van Nguyen.

**FIGURE 13**



Dương Đình Tú

Linh

Phương Linh
Nguyễn Linh
Hồ Mạnh Linh
Bùi Văn Linh
Phạm Ngọc Linh
Linh Tran Pham
Linh Vũ
Thùy Linh
Lê Linh Mẫn
Krystal Linh
Nguyễn Thịnh

### C. Tai Van Nguyen

23. TVN, like his co-Defendants, has edited the source code for the 1stCAPTCHA service via the 1stCAPTCHA GitHub page. TVN has a GitHub account registered to his email account "nvt.kscntt@gmail.com." According to data retrieved from TVN's GitHub account, he edited the 1stCAPTCHA's source code as recently as July 2023.

## III. The Fraudulent Enterprise's Use of Social Media

24. The Fraudulent Enterprise actively markets its unlawful sale of Hotmailbox, 1stCAPTCHA, and AnyCAPTCHA services through various social media websites including Facebook, Telegram, YouTube, LinkedIn, and Twitter.

## IV. Other Criminals' Use of Defendants' Crime-as-a-Service

25. My team has gathered evidence that email accounts sold by the Fraudulent Enterprise have been used by sophisticated cybercriminals—including groups that Microsoft refers to as Storm-0252,[7] Storm-0455, and Octo Tempest—that have historically been known to perpetrate ransomware attacks. For example, we have confirmed that ASNs linked to the Microsoft accounts created by the Fraudulent Enterprise match ASNs linked to email accounts that were used to perpetrate certain cybercrime activity.

26. The malicious actor Microsoft tracks as Storm-0252 encompasses a group that has employed a phishing[8] campaign known as BazaCall, which has historically tricked unsuspecting users into downloading malware[9] through phone calls that provide step-by-step instructions for

[7] Microsoft uses "Storm-####" as a temporary designation to track newly discovered, unknown, or emerging clusters of threat activity.

[8] Phishing is the fraudulent practice of sending emails or other messages, purporting to be from a certain source, for the purpose of inducing individuals to reveal sensitive information, such as passwords and credit card numbers.

[9] Malware, including BazaLoader malware, which is a particular type of malware that has been

installing malware onto their devices. The group often uses Rclone (a data exfiltration tool) to exfiltrate data and historically has deployed Ryuk, which is a particular type of ransomware.[10]

27. The actor Microsoft tracks as Storm-0455 is a financially-motivated cybercriminal group that targets numerous industries globally. Storm-0455 obtains and leverages infrastructure for cybercriminal operations with the ultimate intent to deploy ransomware. Storm-0455 is known to use programs known as Cobalt Strike and malware such as BazaLoader, Trickbot, and Bumblebee, which have led to ransomware attacks known as Conti, QuantumLocker, and Royal. Storm-0455 is tracked by other security companies as EXOTIC LILY and TA580.[11]

28. The actor that Microsoft tracks as Octo Tempest is a financially motivated cybercriminal group that has been observed targeting large scale organizations with varying criminal objectives, including conducting SIM swaps, stealing cryptocurrency, or exfiltrating data prior to extortion or ransomware operations. Octo Tempest has been tied to cyberattacks against flagship Microsoft customers. During these attacks, the computer systems of those customers were infected with ransomware that disabled operation critical systems, resulting in service disruptions that inflicted hundreds of millions of dollars of damage. Microsoft has observed a significant shift since the beginning of summer 2023, such that Octo Tempest is now attacking and compromising

used increasingly in sophisticated threat campaigns, is software that is designed specifically to disrupt, damage, or gain unauthorized access to a computer system.

[10] *See BazaCall: Phony call centers lead to exfiltration and ransomware*, Microsoft Security Blog (July 29, 2021) (describing illicit activities connected to Storm-0252), a true and correct copy of which is attached as Exhibit 2.

[11] *See HTML smuggling surges: Highly evasive loader technique increasingly used in banking malware, targeted attacks*, Microsoft Security Blog (Nov. 11, 2021) (describing illicit activities connected to Storm-0455), a true and correct copy of which is attached hereto as Exhibit 3.

victims at a rapid pace with the intent to steal data for extortion and/or to deploy ransomware known as ALPHV/Blackcat in a matter of hours.[12]

29. As noted, based on our investigation, ASNs associated with emails used in attacks by Storm-0252, Storm-0455, and Octo Tempest match ASNs associated with accounts sold by Defendants, indicating that these groups have used emails acquired from the Fraudulent Scheme to conduct their cybercriminal activities.

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 5 day of December, 2023 in New York, New York.

Maurice Mason

[12] *See Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction*, Microsoft Security Blog (Oct. 25, 2023) (describing illicit activities connected to Octo Tempest), a true and correct copy of which is attached hereto as Exhibit 4.