UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

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

I, Jason Lyons, declare as follows:

1. I am a Principal Manager of Investigations in the Digital Crimes Unit ("DCU") Cybercrime Enforcement Team 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. In my role at Microsoft, 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. I also participate in the investigation of malware[1] and in court-authorized countermeasures to neutralize and disrupt malware. For example, I have personally investigated and assisted in the court-authorized

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

takedown of several families of malware or botnets while at Microsoft, including the malware families and botnets known as Ramnit, ZeroAccess, Dorkbot, and Necurs.

3. Before joining Microsoft, I held cybersecurity-related positions for Xerox and Affiliated Computer Services ("ACS"), and in those roles I provided in-court testimony in connection with a temporary restraining order application concerning the misappropriation of ACS's intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense. A true and correct copy of my curriculum vitae is attached to this declaration as Exhibit 1.

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

5. 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. <u>Overview of the Fraudulent Enterprise</u>

6. As explained below, the Fraudulent Enterprise is in the business of using fraud to obtain Microsoft accounts for resale to cybercriminals.

7. A Microsoft account is a single sign-on personal user account that provides access to a variety of Microsoft services. Microsoft accounts may be used, among other ways, to access consumer Microsoft services (e.g., Outlook.com ("Outlook"), formerly known as Hotmail, which is a personal information manager software system), devices running on Microsoft's operating systems (e.g., Microsoft Windows computers and tablets), and Microsoft application software (e.g., Word and Excel).

8. In order to ensure that human customers are opening Microsoft accounts for legitimate purposes, Microsoft employs a variety of security measures, including CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) challenges that are powered by Arkose Labs.[2] Users cannot access Microsoft's services without agreeing to the Microsoft Services Agreement, which prohibits, among other things, "us[ing] any false, inaccurate or misleading information when signing up for [a] Microsoft account," "creating fake accounts," and "automating inauthentic activity."[3]

9. Fraudulent Microsoft accounts obtained in bulk by cybercriminals can be used as a Trojan horse for disseminating computer viruses, ransomware, and other malware. The Fraudulent

[2] CAPTCHA is a security measure used to verify that the entity attempting to enter a particular service or ecosystem is a human being. I understand that background on CAPTCHA can be found in the declaration of Patrice Boffa in support of Microsoft's motion for an emergency *ex parte* temporary restraining order and order to show cause, familiarity with which is presumed.

[3] A true and correct copy of Microsoft's Services Agreement, published July 30, 2023 and effective September 30, 2023, is attached to this declaration as Exhibit 2, and is also available at https://www.microsoft.com/en-us/servicesagreement/.

Enterprise meets this demand by using automated processes, bots, and CAPTCHA-defeating software to circumvent Microsoft's security measures and obtain Microsoft accounts based on misrepresentations—namely, that the Enterprise is a legitimate human Microsoft customer when, in fact, it is an automated crime service. Defendants sell these fraudulent Microsoft accounts, as well as individual CAPTCHA-defeating tokens that can be used to procure fraudulent Microsoft accounts,[4] to cybercriminals for use as tools in perpetrating a wide variety of online crimes.

10. The Fraudulent Enterprise attacks Microsoft, its Outlook email services, its customers, and third parties by selling fraudulent Microsoft accounts and 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" (the "AnyCAPTCHA Website")).

11. The Fraudulent Enterprise's first step is to initiate the Microsoft account registration process, which triggers a CAPTCHA challenge. The Enterprise then uses a bot to procure a token from that CAPTCHA challenge. The bot subsequently uses that token to defeat the challenge, which inherently misrepresents to Microsoft that a human customer, rather than a bot, is attempting to create an account. The Enterprise repeats this process instantaneously, creating millions of accounts at a time.

II. <u>Microsoft Services Agreement</u>

12. The Fraudulent Enterprise's sale of fraudulently-created Microsoft accounts violates multiple provisions of the Microsoft Services Agreement. As noted above, users cannot access Microsoft's services without agreeing to the Microsoft Services Agreement. (*See* Ex. 2

[4] I understand that the Boffa Declaration contains a description of how the CAPTCHA-defeating tokens sold by the Fraudulent Enterprise are procured and how they function.

("You accept these Terms by creating a Microsoft account, through your use of the Services, or by continuing to use the Services after being notified of a change to these Terms.")). The Microsoft Services Agreement states that users may not, "when using [Microsoft's] Services":

a. "use any false, inaccurate or misleading information when signing up for your Microsoft account" (Ex. 2 at ¶ 4(a)(i));

b. "transfer your Microsoft account credentials to another user or entity" (*id.* ¶ 4(a)(i));

c. "do anything illegal, or try to generate or share content that is illegal" (*id.* ¶ 3(a)(i));

d. "engage in activity that is fraudulent, false or misleading (*e.g.*, asking for money under false pretenses, impersonating someone else, ***creating fake accounts***, ***automating inauthentic activity***, generating or sharing content that is intentionally deceptive, manipulating the Services to increase play count, or affect rankings, ratings, or comments)" (*id.* ¶ 3(a)(v) (emphasis added));

e. "circumvent any restrictions on access to, usage, or availability of the Services (e.g., attempting to 'jailbreak' an AI system or impermissible scraping)" (*id.* ¶ 3(a)(vi));

f. "infringe upon the rights of others" (*id.* ¶ 3(a)(viii)); or

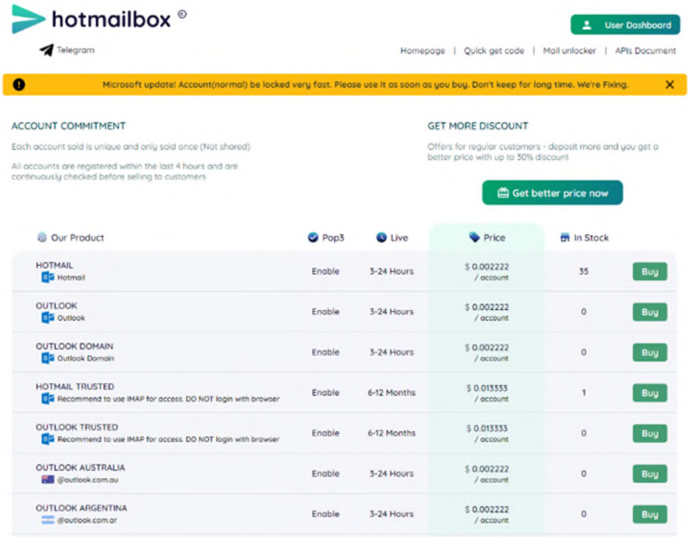
g. "help others break these rules" (*id.* ¶ 3(a)(x)).

III. The Fraudulent Enterprise's Criminal Infrastructure

A. The Hotmailbox Website

13. The Fraudulent Enterprise sells these fraudulently-obtained Microsoft accounts from a registration and hosting website called Hotmailbox.me, which is available on the public web. Figure 1 below reflects the Hotmailbox Website home page.

FIGURE 1



hotmailbox ©

User Dashboard

Telegram

Homepage | Quick get code | Mail unlocker | APIs Document

Microsoft update! Account(normal) be locked very fast. Please use it as soon as you buy. Don't keep for long time. We're Fixing.

ACCOUNT COMMITMENT

Each account sold is unique and only sold once (Not shared)

All accounts are registered within the last 4 hours and are continuously checked before selling to customers

GET MORE DISCOUNT

Offers for regular customers - deposit more and you get a better price with up to 30% discount

Get better price now

Our Product	Pop3	Live	Price	In Stock	
HOTMAIL Hotmail	Enable	3-24 Hours	$ 0.002222 / account	35	Buy
OUTLOOK Outlook	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
OUTLOOK DOMAIN Outlook Domain	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
HOTMAIL TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	1	Buy
OUTLOOK TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	0	Buy
OUTLOOK AUSTRALIA @outlook.com.au	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
OUTLOOK ARGENTINA @outlook.com.ar	Enable	3-24 Hours	$ 0.002222 / account	0	Buy

14. Based on my team's assessment of dedicated Internet Protocol (IP) addresses[5] used by the Fraudulent Enterprise and the distinctive Password Unique Identifiers ("PUIDs")[6] with sign-ins from these accounts, we estimate that the Fraudulent Enterprise has created and sold roughly 750 million fraudulent Microsoft accounts to date.

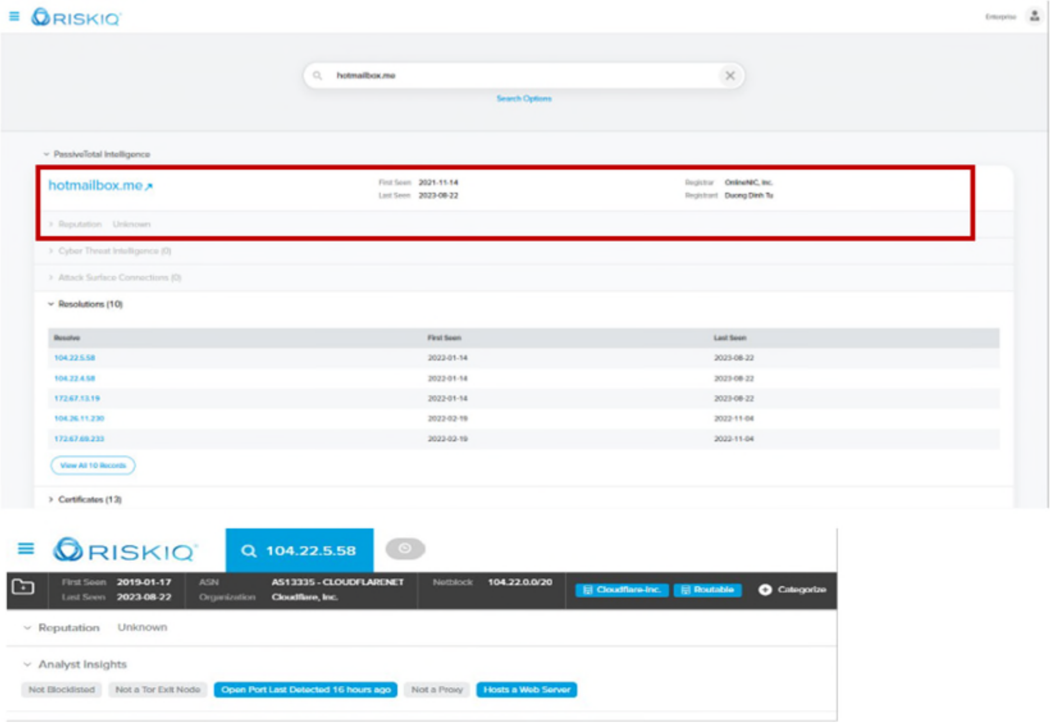
15. As reflected below in Figure 2 (depicting registration and hosting information provided by RiskIQ, which is a tool that provides Internet reconnaissance and analytics), the

[5] An IP address is a unique identifying number that is assigned to every device connected to the internet. IP addresses may be used to identify the geographic location of the user.

[6] Every Microsoft account has its own unique PUID code.

Hotmailbox Website is hosted by domain registrars and service providers located in the United States—specifically, (i) OnlineNIC Inc., which, on information and belief, is located at 3027 Teagarden Street, San Leandro, CA 94577, United States, and which, on information and belief, is managed and operated by Identity Digital (formerly Afilias Inc.) as the owner of the ".me" top-level domain ("TLD")[7]; and (ii) Cloudflare, Inc., which, on information and belief, is associated with various IP addresses, including 104.22.5.58, 104.22.4.58, 172.67.13.19, 104.26.11.230, and 172.67.69.233, and which has an office located at 101 Townsend Street, San Francisco, CA 94107.

FIGURE 2



hotmailbox.me

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

Certificates (13)

104.22.5.58

First Seen 2019-01-17
Last Seen 2023-08-22

ASN AS13335 - CLOUDFLARENET
Organization Cloudflare, Inc.

Netblock 104.22.0.0/20

Cloudflare-Inc. Routable

Reputation Unknown

Analyst Insights

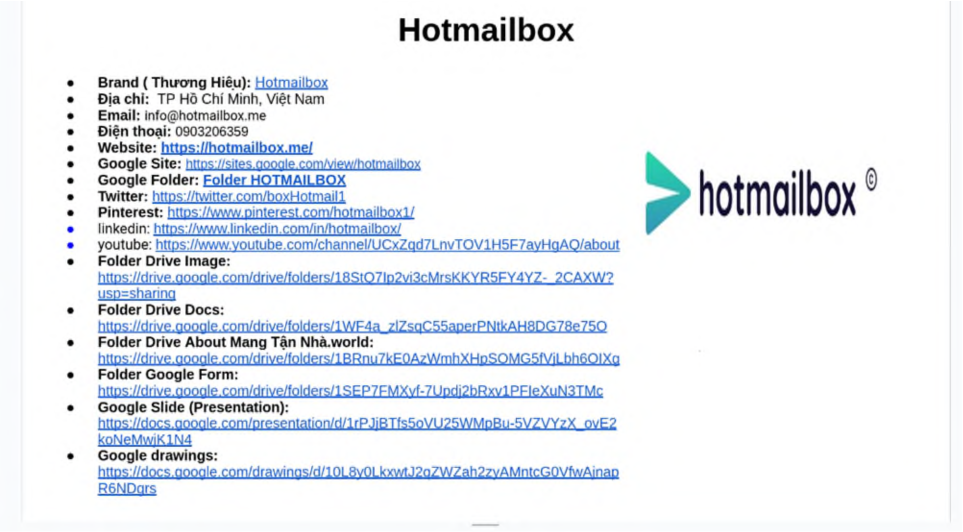
Not Blocklisted · Not a Tor Exit Node · Open Port Last Detected 16 hours ago · Not a Proxy · Hosts a Web Server

16. As reflected below in Figure 3, various additional websites, including social media sites, support the Hotmailbox Website's illicit infrastructure—specifically, Google, Twitter (now "X"), Pinterest, LinkedIn, and YouTube.[8]

[7] TLD refers to the last segment of text in a domain name, such as ".me," ".com," ".net," or ".org."

[8] There is no evidence suggesting that these sites are in any way complicit in Defendants' scheme.

FIGURE 3



Hotmailbox

- **Brand (Thương Hiệu):** Hotmailbox
- **Địa chỉ:** TP Hồ Chí Minh, Việt Nam
- **Email:** info@hotmailbox.me
- **Điện thoại:** 0903206359
- **Website:** **https://hotmailbox.me/**
- **Google Site:** https://sites.google.com/view/hotmailbox
- **Google Folder:** **Folder HOTMAILBOX**
- **Twitter:** https://twitter.com/boxHotmail1
- **Pinterest:** https://www.pinterest.com/hotmailbox1/
- linkedin: https://www.linkedin.com/in/hotmailbox/
- youtube: https://www.youtube.com/channel/UCxZqd7LnvTOV1H5F7ayHgAQ/about
- **Folder Drive Image:** https://drive.google.com/drive/folders/18StO7Ip2vi3cMrsKKYR5FY4YZ-_2CAXW?usp=sharing
- **Folder Drive Docs:** https://drive.google.com/drive/folders/1WF4a_zlZsqC55aperPNtkAH8DG78e75O
- **Folder Drive About Mang Tận Nhà.world:** https://drive.google.com/drive/folders/1BRnu7kE0AzWmhXHpSOMG5fVjLbh6OIXg
- **Folder Google Form:** https://drive.google.com/drive/folders/1SEP7FMXyf-7Updj2bRxv1PFIeXuN3TMc
- **Google Slide (Presentation):** https://docs.google.com/presentation/d/1rPJjBTfs5oVU25WMpBu-5VZVYzX_ovE2koNeMwjK1N4
- **Google drawings:** https://docs.google.com/drawings/d/10L8y0LkxwtJ2gZWZah2zyAMntcG0VfwAjnapR6NDgrs

17. The Fraudulent Enterprise accepts payments via the Hotmailbox Website through cryptocurrency payment processors Cryptomus and Sellix, and through payment processors WebMoney and Vietcombank.

18. There is evidence that the Fraudulent Enterprise is aware that its account-creation and sale scheme violates Microsoft's Services Agreement. From April 2023 through June 2023, Microsoft attempted to disrupt the Enterprise by suspending fraudulent accounts believed to be tied to the Enterprise. In or around August 2023, and as reflected above in Figure 1, the Enterprise subsequently posted an instruction on the Hotmailbox Website to use the fraudulent Microsoft accounts "as soon as you buy" to avoid suspension.

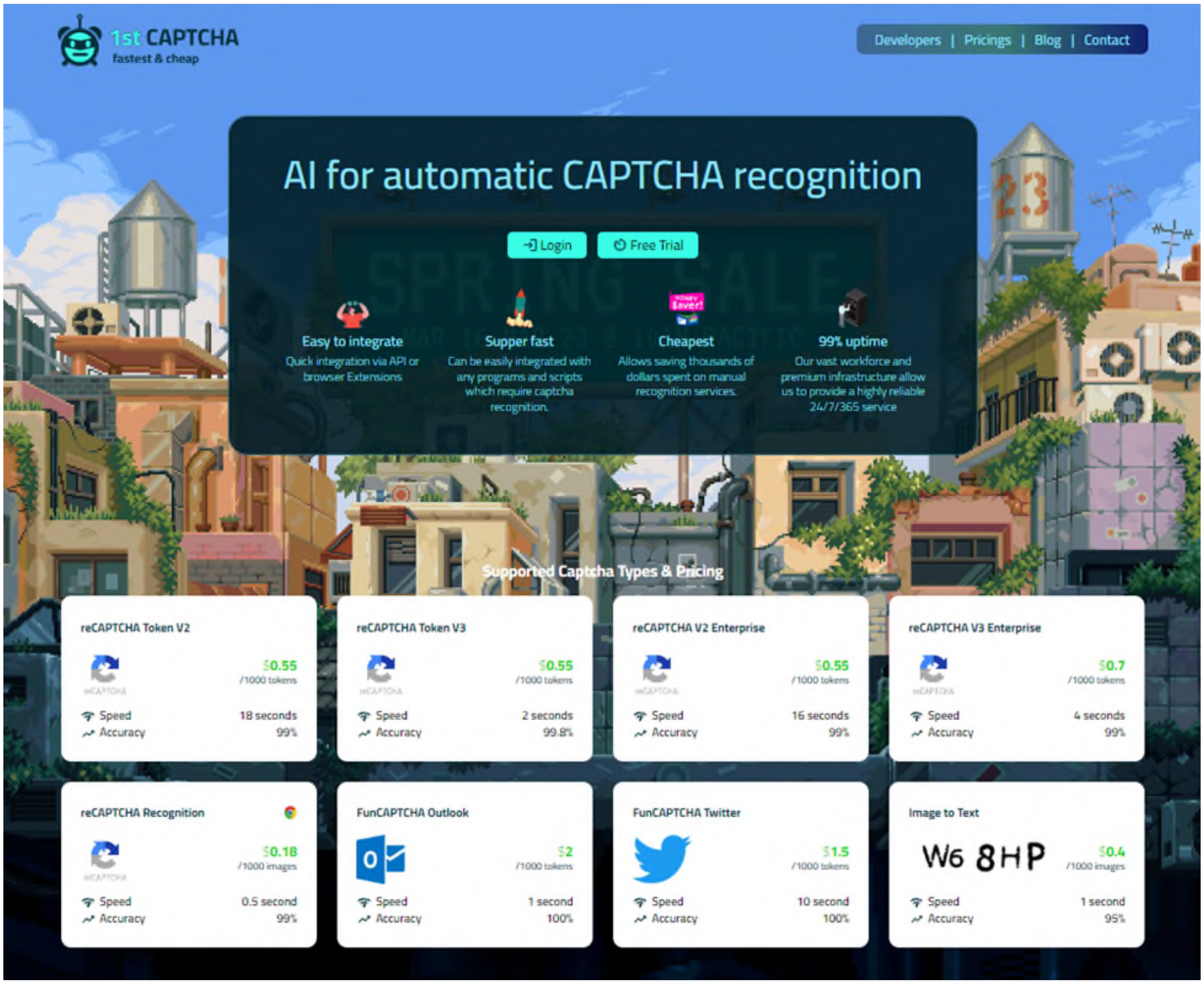
B. The 1stCAPTCHA Website

19. In addition to selling fraudulent Microsoft Outlook accounts via the Hotmailbox Website, the Fraudulent Enterprise has also been selling CAPTCHA-solving tokens procured by the Enterprise's bots—through the fraudulent steps described above—to cybercriminals so they

can have their own bots deploy them to bypass Microsoft's CAPTCHA challenges and procure fraudulent Microsoft Outlook email accounts.

20. One cannot register for a Microsoft account without defeating a CAPTCHA challenge. The Fraudulent Enterprise sells fraudulently-procured CAPTCHA-solving tokens from a publicly-available website called 1stcaptcha.com. The 1stCAPTCHA Website's homepage is reflected below in Figure 4.

FIGURE 4



AI for automatic CAPTCHA recognition

Easy to integrate
Quick integration via API or browser Extensions

Supper fast
Can be easily integrated with any programs and scripts which require captcha recognition.

Cheapest
Allows saving thousands of dollars spent on manual recognition services.

99% uptime
Our vast workforce and premium infrastructure allow us to provide a highly reliable 24/7/365 service

Supported Captcha Types & Pricing

reCAPTCHA Token V2
$0.55 /1000 tokens
Speed 18 seconds
Accuracy 99%

reCAPTCHA Token V3
$0.55 /1000 tokens
Speed 2 seconds
Accuracy 99.8%

reCAPTCHA V2 Enterprise
$0.55 /1000 tokens
Speed 16 seconds
Accuracy 99%

reCAPTCHA V3 Enterprise
$0.7 /1000 tokens
Speed 4 seconds
Accuracy 99%

reCAPTCHA Recognition
$0.18 /1000 images
Speed 0.5 second
Accuracy 99%

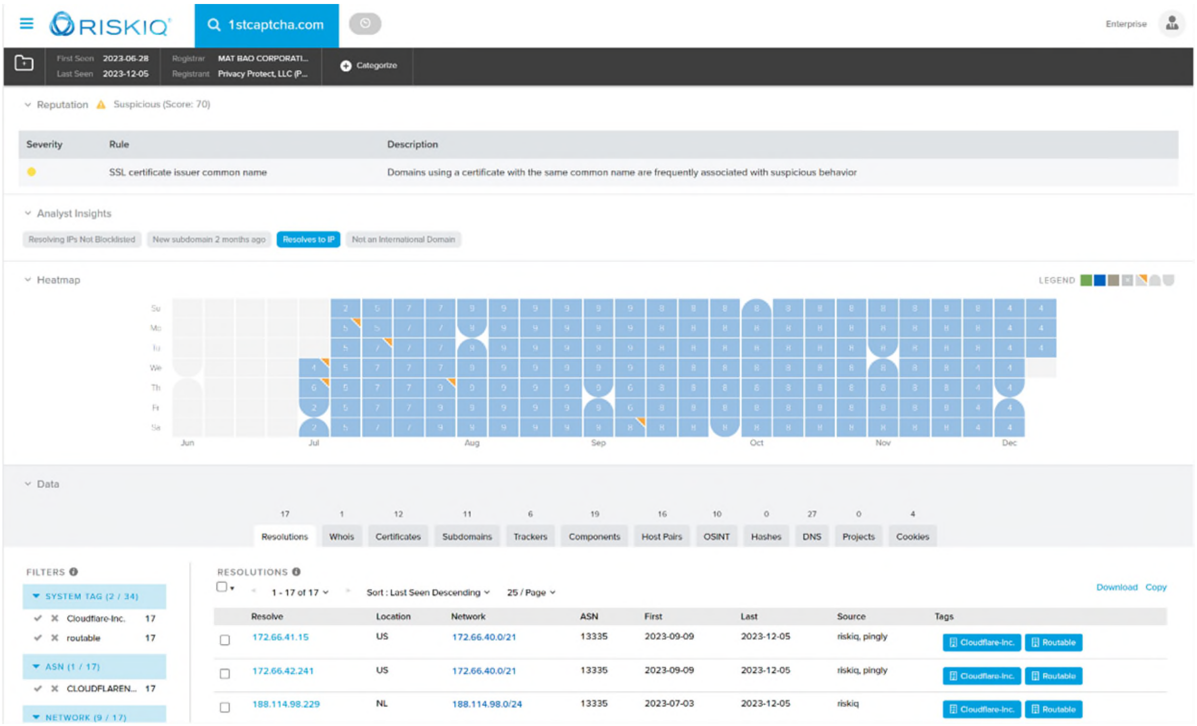
FunCAPTCHA Outlook
$2 /1000 tokens
Speed 1 second
Accuracy 100%

FunCAPTCHA Twitter
$1.5 /1000 tokens
Speed 10 second
Accuracy 100%

Image to Text
W6 8HP
$0.4 /1000 images
Speed 1 second
Accuracy 95%

21. As reflected in Figure 5 (depicting registration and hosting information provided by RiskIQ), the 1stCAPTCHA and AnyCAPTCHA Websites are hosted by domain registrants and service providers located in the United States—specifically, (i) Privacy Protect LLC, which, on information and belief, is a privacy protection service for domain registrants that is associated with various IP addresses, including 172.66.41.15, 172.66.42.241, 188.114.98.229, 104.26.13.192, 172.67.72.186, 104.26.12.192, 188.114.98.229, and 188.114.99.229, is located at 10 Corporate Dive, Burlington, MA 01803, and which, on information and belief, is managed and operated by VeriSign, Inc. as the owner of the TLD ".com"; and (ii) Cloudflare, Inc., which, on information and belief, is associated with various IP addresses, including 172.67.12.153, and which is located at 101 Townsend Street, San Francisco, CA 94107.

FIGURE 5



1stcaptcha.com

First Seen 2023-06-28
Last Seen 2023-12-05
Registrar MAT BAO CORPORATI...
Registrant Privacy Protect, LLC (P...

Reputation ⚠ Suspicious (Score: 70)

Severity	Rule	Description
●	SSL certificate issuer common name	Domains using a certificate with the same common name are frequently associated with suspicious behavior

Analyst Insights

Resolving IPs Not Blocklisted | New subdomain 2 months ago | Resolves to IP | Not an International Domain

17	1	12	11	6	19	16	10	0	27	0	4
Resolutions	Whois	Certificates	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

FILTERS

SYSTEM TAG (2 / 34)

✓ ✕	Cloudflare-Inc.	17
✓ ✕	routable	17

ASN (1 / 17)

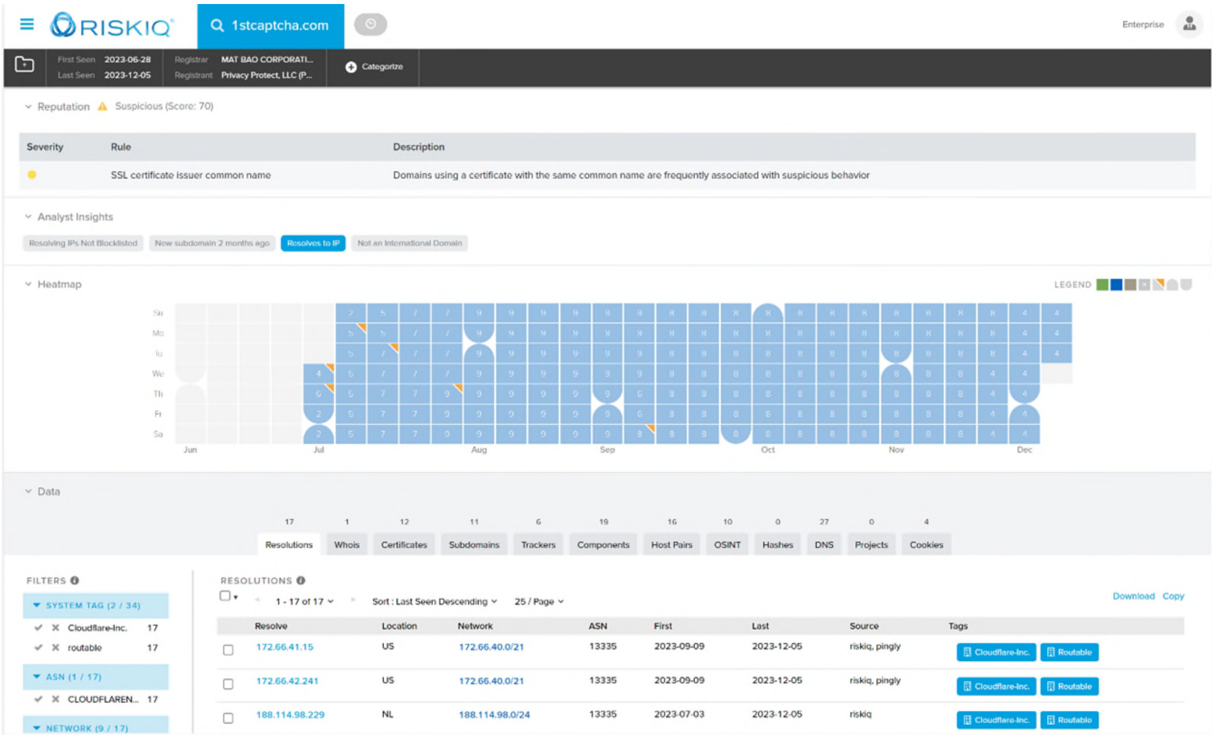
✓ ✕	CLOUDFLAREN...	17

NETWORK (9 / 17)

RESOLUTIONS

□ ▾ 1 - 17 of 17 Sort : Last Seen Descending 25 / Page

	Resolve	Location	Network	ASN	First	Last	Source	Tags
□	172.66.41.15	US	172.66.40.0/21	13335	2023-09-09	2023-12-05	riskiq, pingly	Cloudflare-Inc. Routable
□	172.66.42.241	US	172.66.40.0/21	13335	2023-09-09	2023-12-05	riskiq, pingly	Cloudflare-Inc. Routable
□	188.114.98.229	NL	188.114.98.0/24	13335	2023-07-03	2023-12-05	riskiq	Cloudflare-Inc. Routable



RISKIQ 1stcaptcha.com Enterprise

First Seen 2023-06-28
Last Seen 2023-12-05
Registrar MAT BAO CORPORATI...
Registrant Privacy Protect, LLC (P...
Categorize

Reputation Suspicious (Score: 70)

Severity	Rule	Description
●	SSL certificate issuer common name	Domains using a certificate with the same common name are frequently associated with suspicious behavior

Analyst Insights

Resolving IPs Not Blocklisted · New subdomain 2 months ago · Resolves to IP · Not an International Domain

Heatmap

Data

17	1	12	11	6	19	16	10	0	27	0	4
Resolutions	Whois	Certificates	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

FILTERS

SYSTEM TAG (2 / 34)
✓ ✕ Cloudflare-Inc. 17
✓ ✕ routable 17

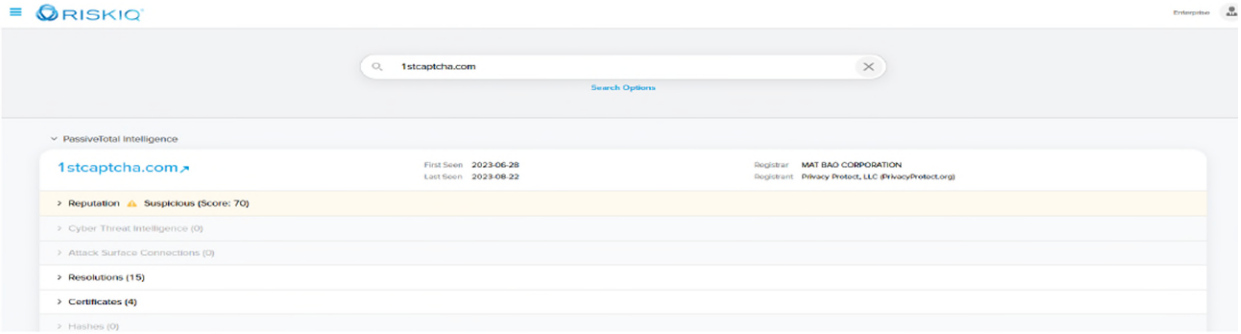
ASN (1 / 17)
✓ ✕ CLOUDFLAREN... 17

NETWORK (9 / 17)

RESOLUTIONS

□ 1 - 17 of 17 Sort : Last Seen Descending 25 / Page Download Copy

	Resolve	Location	Network	ASN	First	Last	Source	Tags
□	172.66.41.15	US	172.66.40.0/21	13335	2023-09-09	2023-12-05	riskiq, pingly	Cloudflare-Inc. Routable
□	172.66.42.241	US	172.66.40.0/21	13335	2023-09-09	2023-12-05	riskiq, pingly	Cloudflare-Inc. Routable
□	188.114.98.229	NL	188.114.98.0/24	13335	2023-07-03	2023-12-05	riskiq	Cloudflare-Inc. Routable



RISKIQ Enterprise

1stcaptcha.com

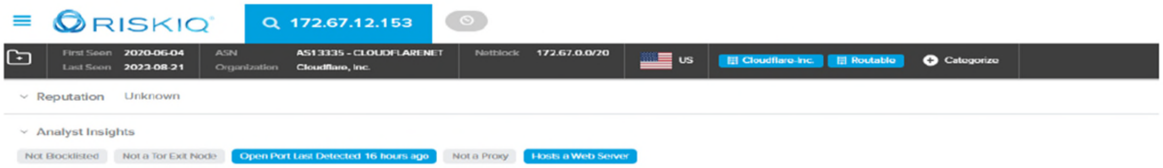
Search Options

PassiveTotal Intelligence

1stcaptcha.com

First Seen 2023-06-28
Last Seen 2023-08-22
Registrar MAT BAO CORPORATION
Registrant Privacy Protect, LLC (PrivacyProtect.org)

› Reputation Suspicious (Score: 70)
› Cyber Threat Intelligence (0)
› Attack Surface Connections (0)
› Resolutions (15)
› Certificates (4)
› Hashes (0)



RISKIQ 172.67.12.153

First Seen 2020-06-04
Last Seen 2023-08-21
ASN AS13335 - CLOUDFLARENET
Organization Cloudflare, Inc.
Netblock 172.67.0.0/20
US
Cloudflare-Inc. Routable Categorize

Reputation Unknown

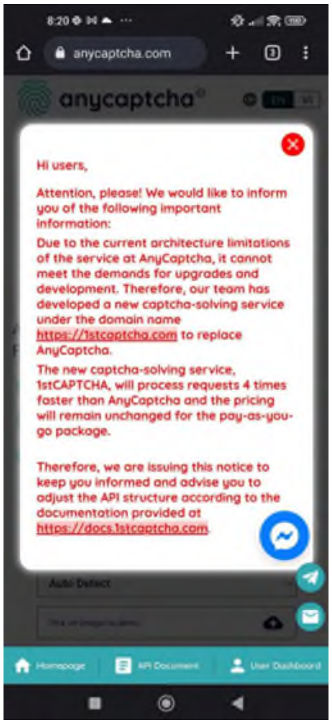
Analyst Insights

Not Blocklisted · Not a Tor Exit Node · Open Port Last Detected 16 hours ago · Not a Proxy · Hosts a Web Server

22. On information and belief, the websites “Nonecaptcha.com” and “Anycaptcha.com” both redirect to the 1stCAPTCHA Website. For instance, I have been advised by Microsoft’s cybersecurity vendor Arkose Labs that on July 4, 2023, Arkose observed a message, which appeared on the Anycaptcha.com website, directing users to the 1stCAPTCHA

Website. A screenshot of the message, which has been provided to me by Arkose, is reflected in Figure 6 below.

FIGURE 6



Hi users,

Attention, please! We would like to inform you of the following important information:

Due to the current architecture limitations of the service at AnyCaptcha, it cannot meet the demands for upgrades and development. Therefore, our team has developed a new captcha-solving service under the domain name https://1stcaptcha.com to replace AnyCaptcha.

The new captcha-solving service, 1stCAPTCHA, will process requests 4 times faster than AnyCaptcha and the pricing will remain unchanged for the pay-as-you-go package.

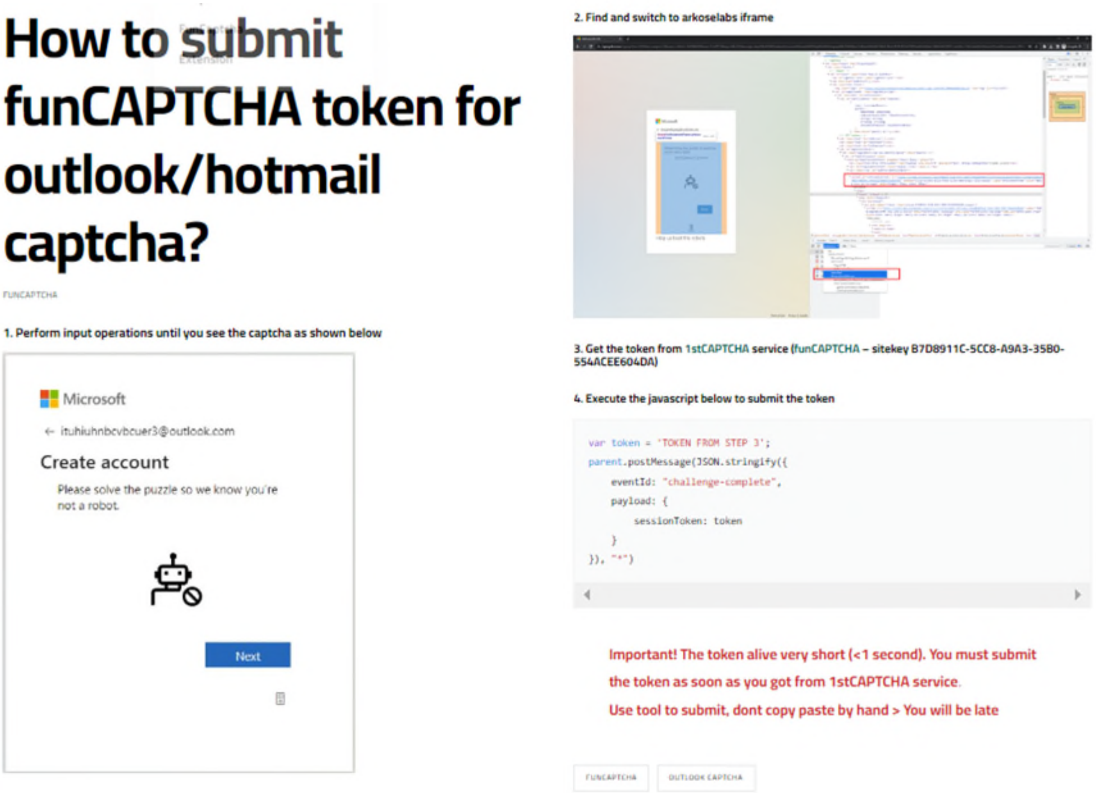
Therefore, we are issuing this notice to keep you informed and advise you to adjust the API structure according to the documentation provided at https://docs.1stcaptcha.com.

23. The 1stCAPTCHA Website maintains a "blog" that explains in detail how its services may be used to bypass Microsoft's CAPTCHA-fortified security measures.[9] As reflected below in Figure 7, the blog instructs users to (i) "[p]erform input operations until you see [Microsoft's] captcha," (ii) "[f]ind and switch to arkoselabs iframe," (iii) "[g]et the token from 1stCAPTCHA service," and (iv) "[e]xecute the javascript [provided by the 1stCAPTCHA Website] to submit the token." Defendants' blog also contains entries explaining how to defeat the CAPTCHA defenses employed by Twitter and Google.[10]

[9] *See How to submit funCAPTCHA token for outlook/hotmail captcha?*, 1stCaptcha (Sept. 6, 2023), https://1stcaptcha.com/blog/how-to-submit-funcaptcha-token-for-outlook-hotmail-captcha/. A true and correct copy of this webpage is attached hereto as Exhibit 3.

[10] *See How to bypass Twitter FunCAPTCHA using 1stCAPTCHA*, 1stCaptcha (Sept. 17, 2023), https://1stcaptcha.com/blog/how-to-bypass-twitter-funcaptcha-using-1stcaptcha/; *How to*

FIGURE 7



How to submit funCAPTCHA token for outlook/hotmail captcha?

FUNCAPTCHA

1. Perform input operations until you see the captcha as shown below

Microsoft

← ituhiuhnbcvbcuer3@outlook.com

Create account

Please solve the puzzle so we know you're not a robot.

2. Find and switch to arkoselabs iframe

3. Get the token from 1stCAPTCHA service (funCAPTCHA – sitekey B7D8911C-5CC8-A9A3-35B0-554ACEE604DA)

4. Execute the javascript below to submit the token

```
var token = 'TOKEN FROM STEP 3';
parent.postMessage(JSON.stringify({
    eventId: "challenge-complete",
    payload: {
        sessionToken: token
    }
}), "*")
```

Important! The token alive very short (<1 second). You must submit the token as soon as you got from 1stCAPTCHA service.

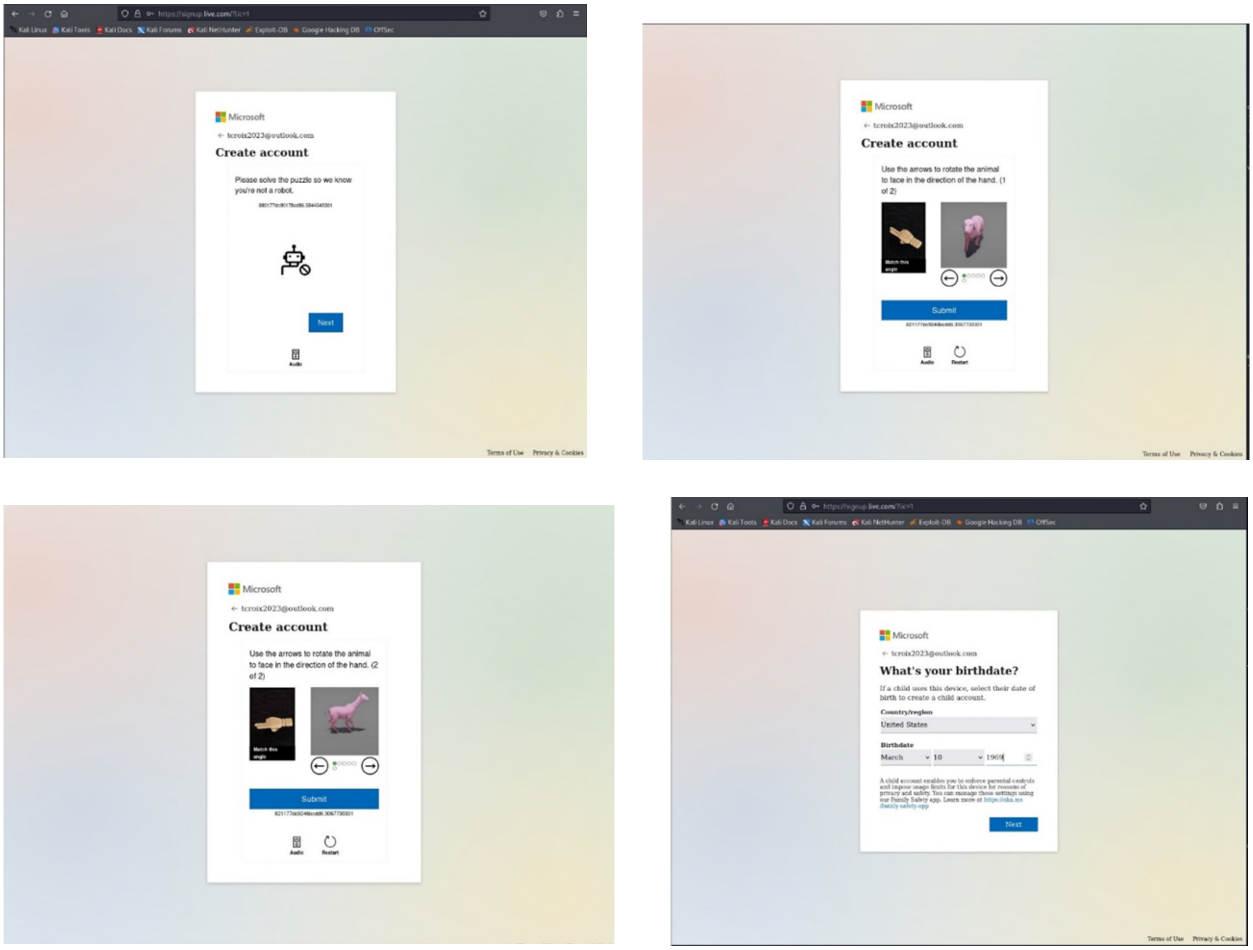
Use tool to submit, dont copy paste by hand > You will be late

24. Through the use of sophisticated automation technology, 1stCAPTCHA deceives Microsoft's security into believing that a human customer, rather than a malicious computer algorithm, is attempting to create a Microsoft account and use Microsoft's services. 1stCAPTCHA bypasses Microsoft's CAPTCHA defenses by (i) solving authentication puzzles, (ii) rotating

distinguish between different types of reCAPTCHA: v2, v3, enterprise, 1stCaptcha (Sept. 6, 2023), https://1stcaptcha.com/blog/how-to-distinguish-recaptcha-v2-v3-enterprise/ ("Google's reCAPTCHA, an evolved iteration of this idea, takes a more advanced approach, delivering heightened security while preserving user convenience intact. . . . Using element inspector, you will see an iframe element with a src attribute in the form of src=https://www.google.com/recaptcha/api2/anchor?). True and correct copies of these webpages are attached hereto as Exhibits 4 and 5, respectively.

figures to align the figure with the direction displayed on screen, and (iii) inputting dates of birth. Figure 8 below reflects examples of different CAPTCHA challenges used by Microsoft.

FIGURE 8



https://signup.live.com/?lic=1

Create account

Please solve the puzzle so we know you're not a robot.

Use the arrows to rotate the animal to face in the direction of the hand. (1 of 2)

Use the arrows to rotate the animal to face in the direction of the hand. (2 of 2)

What's your birthdate?

If a child uses this device, select their date of birth to create a child account.

Country/region: United States

Birthdate: March 10 1969

A child account enables you to enforce parental controls and impose usage limits for this device for reasons of privacy and safety. You can manage those settings using our Family Safety app. Learn more at https://aka.ms/family-safety-app

25. The Fraudulent Enterprise uses GitHub—a public interactive website on which users can share and collaborate on computer source code—as a centralized repository to store the code necessary to effectuate the CAPTCHA-defeating tokens sold through the 1stCAPTCHA Website. Seizure of the 1stCAPTCHA GitHub page will render ineffective, on a going-forward basis, any CAPTCHA-defeating token sold by the 1stCAPTCHA Website.

26. Purchasers of the 1stCAPTCHA tool receive an Application Programming Interface ("API") key.[11] During the process of bypassing Microsoft's security measures, the 1stCAPTCHA tokens "call out" to the APIs located within the servers hosted by Privacy Protect LLC and Cloudflare, Inc. Disrupting the electronic "handshake" between these APIs will render ineffective the CAPTCHA-defeating tokens sold by the 1stCAPTCHA Website.

27. The 1stCAPTCHA Website accepts payment through cryptocurrency payment processor Cryptomus and Sellix, and through payment processors PayPal and Vietcombank.

IV. <u>Undercover Purchases</u>

28. During the investigation in this case, Microsoft retained external expert consultants at Berkeley Research Group ("BRG") to conduct undercover purchases of fraudulently-obtained Microsoft accounts and CAPTCHA-defeating tokens from the Fraudulent Enterprise. I have reviewed the data collected via BRG's undercover purchases of fraudulent Microsoft accounts from the Hotmailbox Website. As a result of these undercover purchases, BRG has come into possession of approximately 16,500 fraudulent Microsoft accounts. Of the approximately 16,500 accounts, approximately 16,495 were registered with unique IP addresses, which demonstrates the sophistication of the Fraudulent Enterprise's scheme—that is, in order to avoid detection, the Enterprise uses proxy services to constantly change the IP addresses from which the accounts are logging into Microsoft systems.

29. Despite these efforts to constantly recycle and mask IP addresses, the Enterprise cannot obfuscate the location of the Internet service provider (ISP) from which these IP addresses originate. Approximately 12,996 of the purchased accounts were registered with IP addresses

[11] An API is a software intermediary that permits two or more computer applications to communicate with each another.

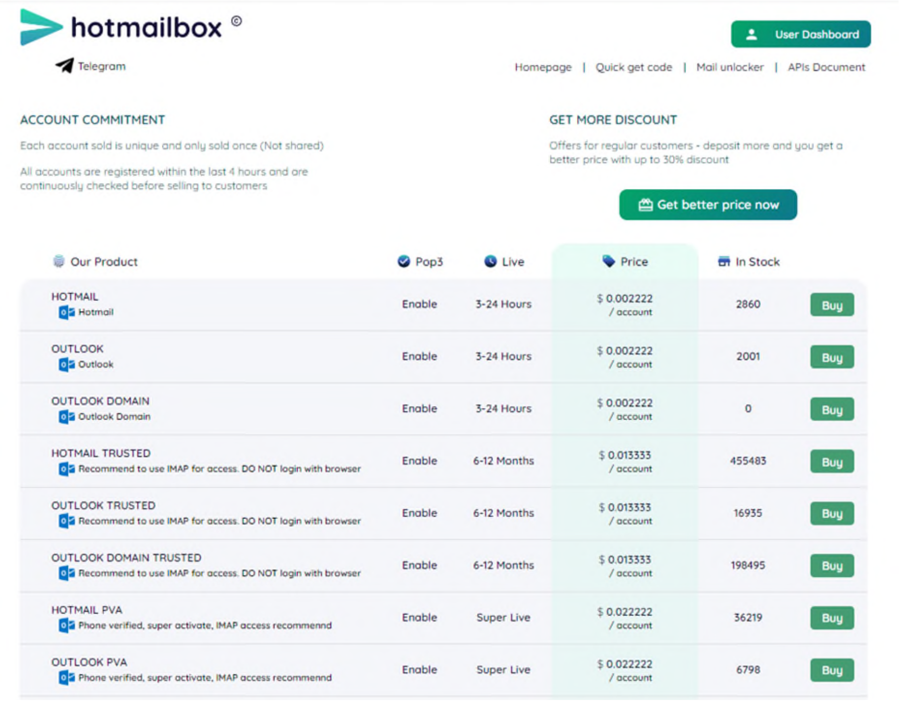
deriving from the New York, New York data center of an ISP called Hostkey. Those accounts, seconds after initial registration, were logged into from IP addresses—154.27.66.194 and 154.27.66.246—originating from the service provider Cloud South, which, on information and belief, is located at 424 Hampton Road, West Palm Beach, FL 33405.

V. **Microsoft Trademarks**

30. Microsoft holds registered trademarks with respect to its (i) Outlook launch icon mark, (ii) Outlook word mark, and (iii) Hotmail word mark. True and correct registration copies of each trademark are annexed as Appendix B to Microsoft's Complaint in the above-captioned case.

31. In selling fraudulent Microsoft accounts, the Hotmailbox Website uses several Microsoft trademarks without Microsoft's authorization, including Microsoft's Outlook launch icon trademark, its Outlook word trademark, and its Hotmail word trademark. A screenshot of the Hotmailbox Website illustrating how it misappropriates those trademarks, as well as a zoomed-in side-by-side comparison with Microsoft's trademarks are depicted in Figures 9 and 10 below.

FIGURE 9



ACCOUNT COMMITMENT

Each account sold is unique and only sold once (Not shared)

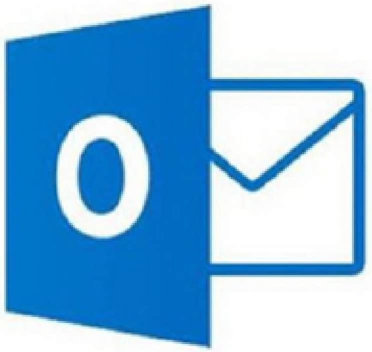
All accounts are registered within the last 4 hours and are continuously checked before selling to customers

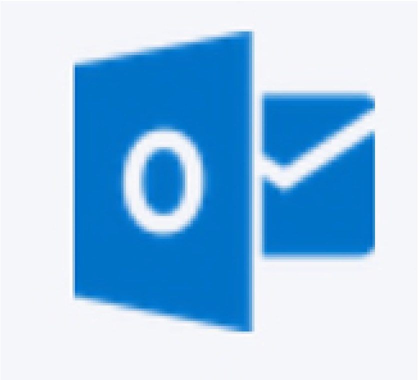
GET MORE DISCOUNT

Offers for regular customers - deposit more and you get a better price with up to 30% discount

Our Product	Pop3	Live	Price	In Stock	
HOTMAIL Hotmail	Enable	3-24 Hours	$ 0.002222 / account	2860	Buy
OUTLOOK Outlook	Enable	3-24 Hours	$ 0.002222 / account	2001	Buy
OUTLOOK DOMAIN Outlook Domain	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
HOTMAIL TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	455483	Buy
OUTLOOK TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	16935	Buy
OUTLOOK DOMAIN TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	198495	Buy
HOTMAIL PVA Phone verified, super activate, IMAP access recommennd	Enable	Super Live	$ 0.022222 / account	36219	Buy
OUTLOOK PVA Phone verified, super activate, IMAP access recommennd	Enable	Super Live	$ 0.022222 / account	6798	Buy

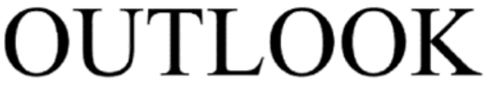
FIGURE 10

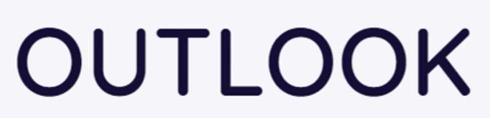




Microsoft’s Registered Trademark

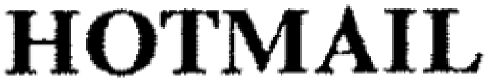
Hotmailbox Website



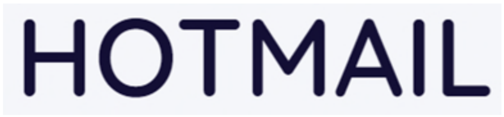


Microsoft’s Registered Trademark

Hotmailbox Website



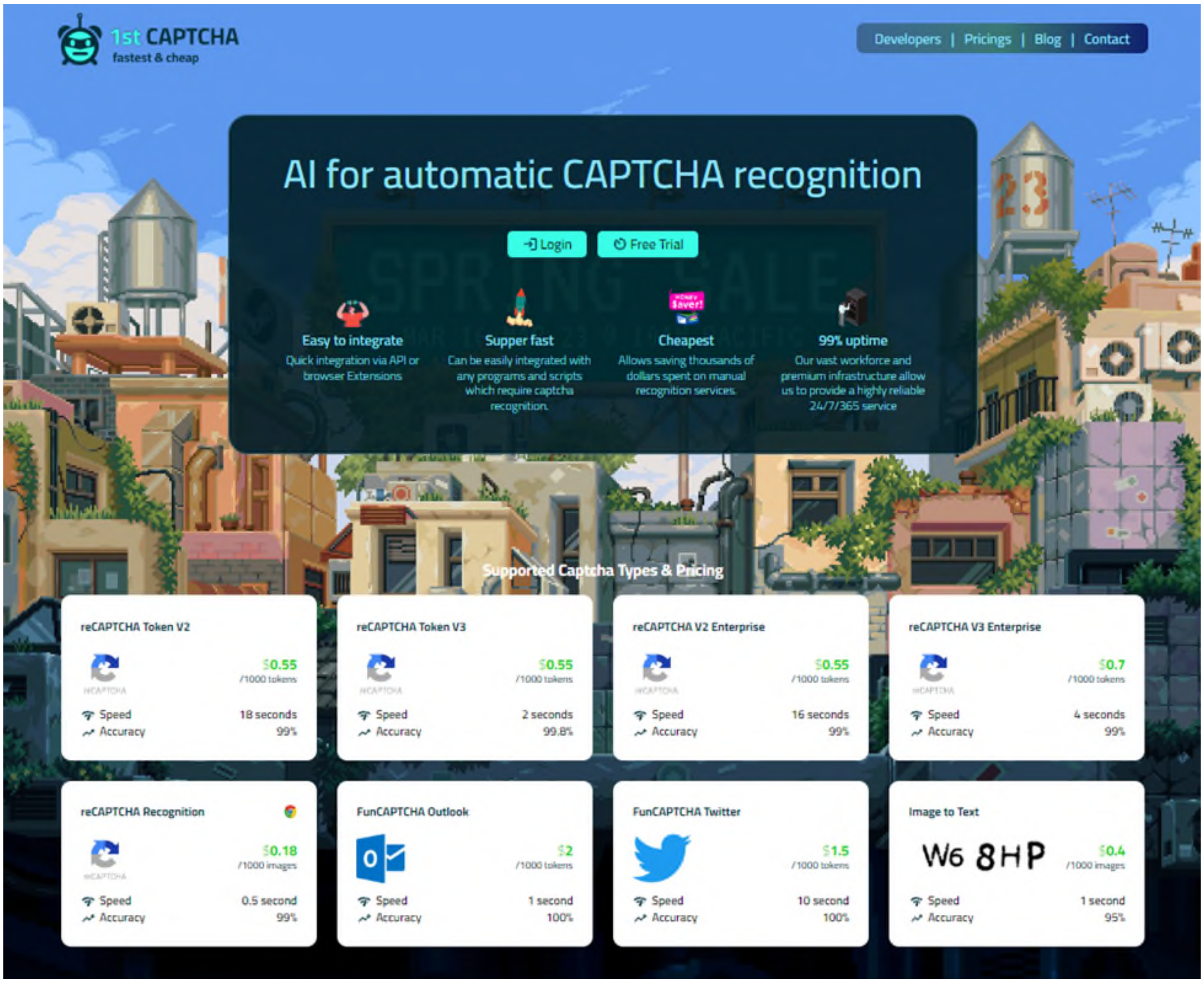
Microsoft’s Registered Trademark



Hotmailbox Website

32. The 1stCAPTCHA Website uses Microsoft’s Outlook launch icon trademark without Microsoft’s authorization to sell fraudulently-obtained CAPTCHA-defeating tools. A screenshot of the 1stCAPTCHA Website illustrating how it misappropriates that trademark, as well as a zoomed-in side-by-side comparison with Microsoft’s trademark are depicted in Figures 11 and 12 below.

FIGURE 11



1st CAPTCHA
fastest & cheap

Developers | Pricings | Blog | Contact

AI for automatic CAPTCHA recognition

Login Free Trial

Easy to integrate
Quick integration via API or browser Extensions

Supper fast
Can be easily integrated with any programs and scripts which require captcha recognition.

Cheapest
Allows saving thousands of dollars spent on manual recognition services.

99% uptime
Our vast workforce and premium infrastructure allow us to provide a highly reliable 24/7/365 service

Supported Captcha Types & Pricing

reCAPTCHA Token V2
$0.55 /1000 tokens
Speed 18 seconds
Accuracy 99%

reCAPTCHA Token V3
$0.55 /1000 tokens
Speed 2 seconds
Accuracy 99.8%

reCAPTCHA V2 Enterprise
$0.55 /1000 tokens
Speed 16 seconds
Accuracy 99%

reCAPTCHA V3 Enterprise
$0.7 /1000 tokens
Speed 4 seconds
Accuracy 99%

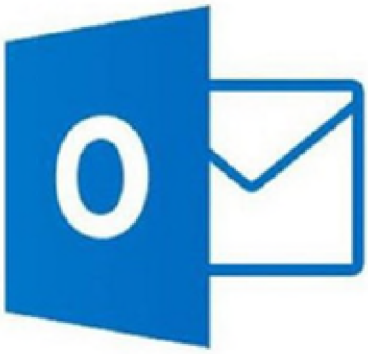
reCAPTCHA Recognition
$0.18 /1000 images
Speed 0.5 second
Accuracy 99%

FunCAPTCHA Outlook
$2 /1000 tokens
Speed 1 second
Accuracy 100%

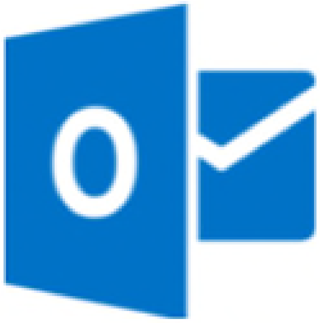
FunCAPTCHA Twitter
$1.5 /1000 tokens
Speed 10 second
Accuracy 100%

Image to Text
W6 8HP
$0.4 /1000 images
Speed 1 second
Accuracy 95%

FIGURE 12



Microsoft's Registered Trademark



1stCAPTCHA Website

VI. Disrupting the Fraudulent Enterprise

33. Through this lawsuit, Microsoft is requesting judicial authorization to direct several providers of infrastructure used by the Fraudulent Enterprise to take actions that would disrupt this scheme. It is imperative that the requested actions be closely coordinated, such that the malicious IP addresses in various locations are directed by the Court to be turned off immediately upon receipt of any order issued by the Court and in coordination with other efforts, such that these IP addresses are turned off simultaneously. It is also critical that these actions be shielded from anyone associated with the Enterprise—including the Defendants named in this action—until the takedown of the Enterprise's infrastructure is complete. If Defendants become aware of these efforts prior to the completion of these requested actions, there is a substantial risk that they will relocate the infrastructure to alternative domains and these efforts to stop the Fraudulent Enterprise will be thwarted. The proposed *ex parte* temporary restraining order ("Proposed Order") is framed in a manner that enables coordinated efforts that will maximize the effectiveness of the relief sought.

34. In the aggregate, the steps set forth in the Proposed Order, which will be carried out upon entry of the requested Proposed Order, will prevent Defendants from operating the Fraudulent Enterprise. For instance, as soon as the 1stCAPTCHA Website is seized, the APIs underpinning the unlawfully-sold CAPTCHA-defeating tokens will not be able to communicate with the 1stCAPTCHA Website, and the tokens will be rendered ineffective.

35. I believe that the steps described in the Proposed Order are appropriate and necessary to suspend the ongoing harm cause by the Fraudulent Enterprise on Microsoft, its consumers, and the public.

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.

Jason Lyons