

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.

4. In connection with Plaintiff’s December 2023 motion for an emergency *ex parte* temporary restraining order and order to show cause (“TRO Motion”), I was involved in 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, opening Microsoft accounts in the names of fictitious users, and then selling these fraudulent Microsoft accounts to cybercriminals for use in a wide variety of internet-based crimes. The Fraudulent Enterprise has caused, and continues to cause, substantial damage to Microsoft and other parties, which, if permitted to continue, will compound over time.

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.

6. On December 12, 2023, Microsoft worked with third-party registry operators and service providers to execute this Court’s Temporary Restraining Order (“TRO”). While the fraudulent activity attributable to the Fraudulent Enterprise ceased following the TRO, I and other Microsoft investigators have recently discovered that Defendants reconstituted their unlawful infrastructure under a new domain, “rockcaptcha.com” (the “RockCAPTCHA Website”), and are again engaging in the same fraudulent conduct prohibited by the TRO. To investigate and identify this new infrastructure and domain, I and other Microsoft investigators used the same investigative methods described in connection with my previous declaration in support of the TRO Motion.

7. Using those same investigative methods, I discovered, on an internet forum that I know is commonly used for the sale of tools used for cybercrime, the blog post reflected in Figure 1. The post, when roughly translated into English,² states, “recently . . . ha[ve] lost two important resource sites, 1st***.com and ***box.me. . . . For the above reason, today I would like to launch . . . the brand new captcha solving site <https://rockcaptcha.com> developed by my team[.]” I understand the post’s references to “1st***.com” and “***box.me” to be referring to 1stcaptcha.com and hotmailbox.me, which were the websites targeted by our initial infrastructure disruption effort in this matter. Based on my experience and these investigative methods, which include internal tools available to me at Microsoft, I have concluded that the Defendants are both the authors of this post and the creators of the RockCAPTCHA Website.

² The post is publicly available in Vietnamese at the following link: <https://mmo4me.com/threads/rockcaptcha-com-giai-captcha-twitter-hotmail-recaptcha-toc-do-ban-tho-gia-sieu-re.475942/> (Jan. 29, 2024).

FIGURE 1

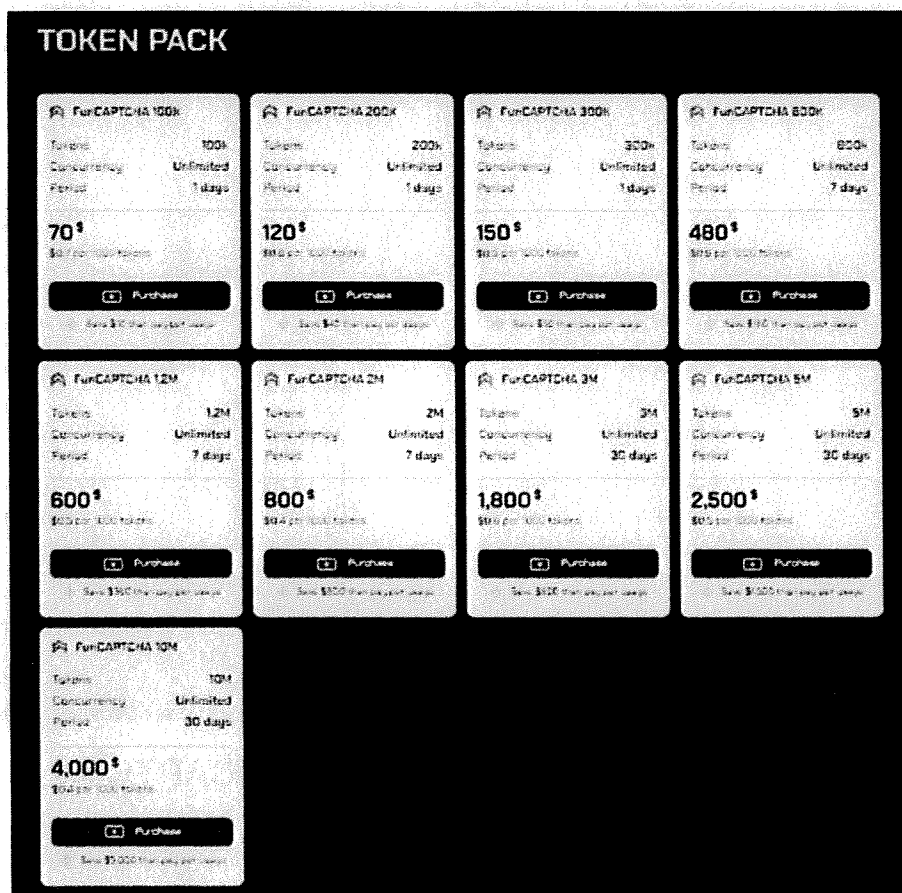


8. The RockCAPTCHA Website targets Microsoft by offering services specifically designed to defeat the CAPTCHA security measures of Arkose Labs, which are employed by Microsoft as described in the original TRO Motion. Below at Figures 2 and 3 are screenshots of portions of the RockCAPTCHA Website.

FIGURE 2

PAY PER USAGE		Price/1000	Speed	Valid rate
☆	 reCAPTCHA Token V2	\$ 0.30	10 seconds	99%
☆	 reCAPTCHA Token V3	\$ 0.30	2 seconds	99.8%
☆	 reCAPTCHA V2 Enterprise	\$ 0.30	16 seconds	99%
☆	 reCAPTCHA V3 Enterprise	\$ 0.30	4 seconds	99%
☆	 reCAPTCHA Recognition	\$ 0.18	0.5 second	99%
☆	 reCAPTCHA Token	\$ 0.80	1 seconds	100%
☆	 Image to Text	\$ 0.30	1 second	95%

FIGURE 3



9. Moreover, a video titled “RockCAPTCHA Extension to Bypass FunCAPTCHA,” which is publicly available at <https://www.youtube.com/watch?v=JLulSoca3wg>, and which was posted by the YouTube channel, @ROCKCAPTCHA, on April 4, 2024, demonstrates that the services provided by the RockCAPTCHA Website are intended to be used for Microsoft Outlook in particular. The video’s description states, “[t]his video will guide you on how to set up the Rock CAPTCHA Extension to bypass Fun CAPTCHA on the Outlook/Hotmail [] creation page.” A screenshot of the portion of the video dedicated to explaining how to defeat Microsoft’s CAPTCHA security measures can be seen below at Figure 4. This video also demonstrates that Defendants make unauthorized use of Microsoft’s registered trademark. A zoomed-in side-by-side comparison of the screenshot below with Microsoft’s trademark is depicted in Figure 5.

FIGURE 4

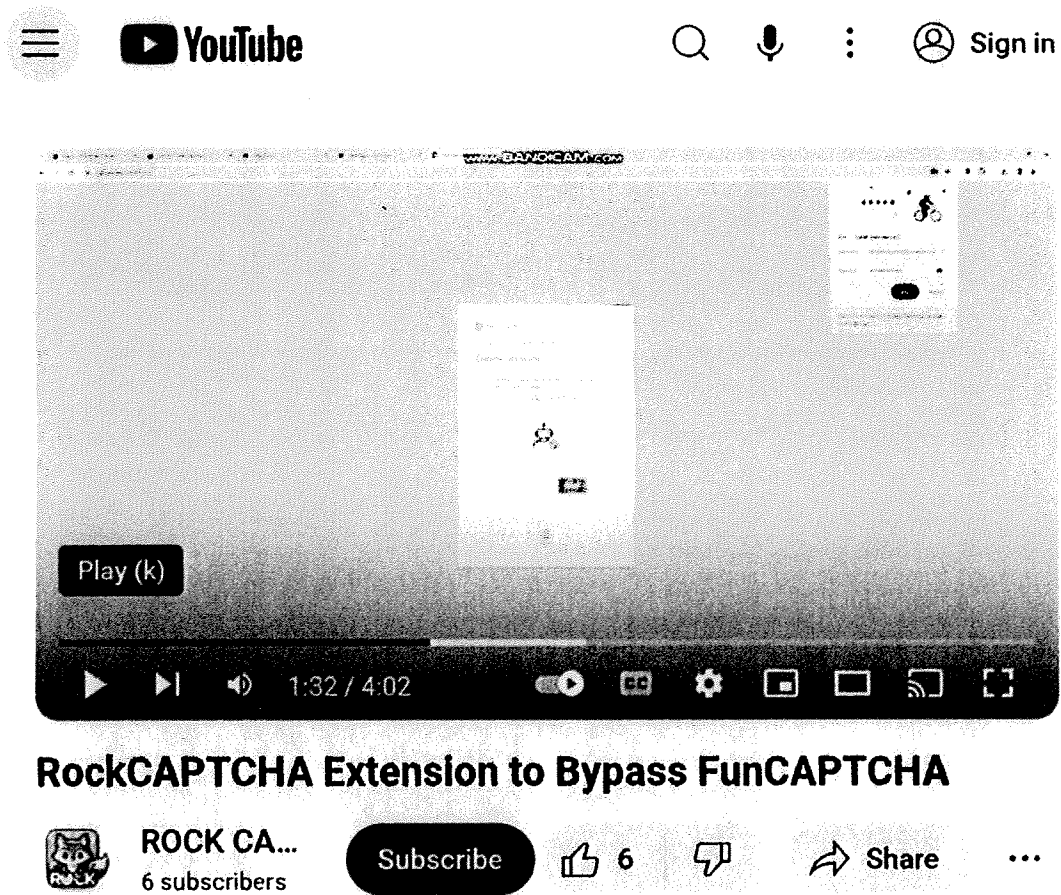


FIGURE 5



10. As reflected below in Figures 6 and 7, Defendants are also actively marketing the RockCAPTCHA Website through the Facebook page, "RockCaptcha," which is publicly available at https://www.facebook.com/people/RockCaptcha/61557799251236/?_rdr. The RockCaptcha Facebook page was created on March 21, 2024.

FIGURE 6

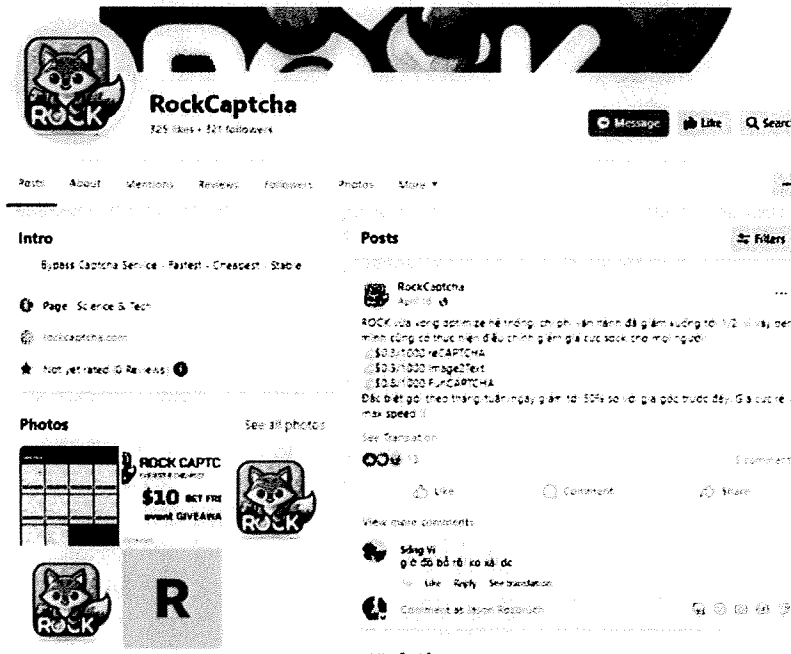
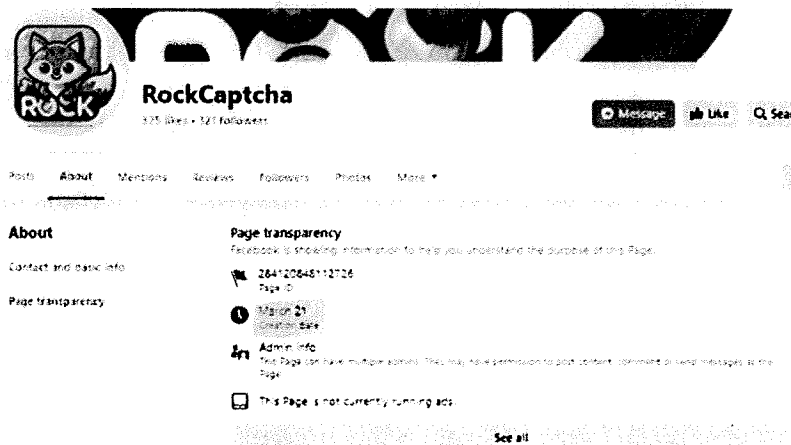


FIGURE 7



11. This conduct gives rise to the same harm to Microsoft that was described in detail in my December 5, 2023 Declaration (ECF No. 15).

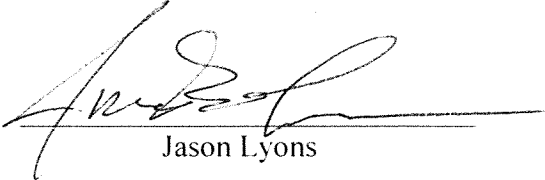
12. Through this lawsuit, Microsoft is requesting judicial authorization to direct VeriSign, Inc., the registry operator for .com domain names, including rockcaptcha.com, and Vultr, the RockCAPTCHA Website’s hosting provider, to take specific actions that would disrupt

this scheme. It is critical that these actions be shielded from anyone associated with the Enterprise—including the Defendants named in this action—until complete. If Defendants become aware of these efforts prior to their completion, there is a substantial risk that Defendants will relocate the infrastructure to alternative domains prior to the effectuation of this Court’s Order, and these efforts to stop the Fraudulent Enterprise will be thwarted. The actions set forth in the Proposed *Ex Parte* Supplemental Preliminary Injunction Order (“Proposed Order”) will be carried out immediately upon entry and will prevent Defendants from operating the RockCAPTCHA Website, which directly supports their Fraudulent Enterprise. Although the Defendants have already demonstrated an ability to reconstitute their malicious infrastructure following Microsoft’s disruption efforts, their new, reconstituted websites operate on a much lesser scale, with far fewer customers. I believe based on my experience that additional, unannounced disruptions of these illicit operations will further frustrate Defendants’ efforts to maintain and add customers, weaken their credibility in the marketplace, and ultimately cause the Fraudulent Enterprise to fail.

13. I believe that the steps described in the Proposed Order are appropriate and necessary to suspend the ongoing harm caused 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 17 day of July, 2024 in Redmond, WA.


Jason Lyons