

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

Microsoft Corporation, a Washington State  
Corporation and Health-ISAC, a Florida non-  
profit,

Plaintiffs,

v.

Joshua Ogundipe,

and

John Does 1-4, Controlling A Computer  
Network and Thereby Injuring Plaintiffs and  
Their Customers,

Defendants.

Civil Action No.

**FILED UNDER SEAL PURSUANT TO  
LOCAL RULE 5**

**DECLARATION OF NICK MONACO IN SUPPORT OF PLAINTIFFS' *EX PARTE*  
APPLICATION FOR TEMPORARY RESTRAINING ORDER**

I, Nick Monaco, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration in support of Plaintiffs' *Ex Parte* Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. Microsoft's Digital Crimes Unit ("DCU") is the Microsoft division responsible for protecting Microsoft and its customers against cybercrime threats. DCU is an international team of technical, legal, and business experts that has been fighting cybercrime, protecting individuals

and organizations and safeguarding the integrity of Microsoft services since 2008.<sup>1</sup> One of DCU's responsibilities is to investigate cybersecurity threats and identify and attribute attacks, like it has done here with the RaccoonO365 Defendants. DCU also collaborates with the Microsoft Threat Intelligence Center (MSTIC), which is made up of thousands of world-class experts, security researchers, analysts, and threat hunters. MSTIC regularly publishes threat intelligence blogs alerting customers and the public of cybersecurity threats.<sup>2</sup>

3. In my role at Microsoft as part of DCU, I assess technological security threats to Microsoft and the effect of such threats on Microsoft's business and customers. Among my responsibilities is protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of malware and participate in court-authorized countermeasures to neutralize and disrupt malware. For example, I have personally investigated and assisted in the court-authorized takedown of malware or botnets including campaigns from financially motivated actors using the Lumma infostealer, the most widely used infostealer globally.<sup>3</sup>

4. Before joining Microsoft, I worked for Miburo Solutions as the Chief Innovation Officer (CIO) and Director of China Research. I also worked for Institute for the Future (IFTF) as the Research Director of the Digital Intelligence Lab. Prior to working for IFTF, I worked for Graphika as a Disinformation and Intelligence Analyst. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

---

<sup>1</sup> *Digital Crimes Unit: Leading the fight against Cybercrime*, Microsoft, available at <https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fightscybercrime/> (May 3, 2022).

<sup>2</sup> See Microsoft, *Threat Intelligence Blog*, available at <https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/> (last accessed Oct. 10, 2024).

<sup>3</sup> See *Microsoft Corporation v. John Does 1-10*, Case No. 25-cv-2695-MHC (N.D. Ga. 2025) (Cohen, J.)


5. My declaration concerns the investigation into a foreign-cybercriminal organization comprised of Joshua Ogundipe and a series of unknown individuals—John Does 1-4—who are collectively known as “RaccoonO365 Defendants.” I have investigated the structure and function of RaccoonO365 Defendants’ criminal organization, including completing four test buys of their kits and investigating RaccoonO365’s cryptocurrency transactions.



#### **I. TEST BUYS AND FINANCIAL ANALYSIS**

6. RaccoonO365 sells two tools that make up the phishing kit: the Postman Mass Mailer and the Links Credential Capture. As part of my investigation, I made four controlled purchases or “test buys” of the RaccoonO365-branded phishing kits. This included one purchase of the Postman Mass Mailer and three test buys of the Links Credential Capture kit. Because RaccoonO365 Defendants offer the Links Credential Capture kit for a shorter-term subscription (compared to a one-year subscription for Postman Mass Mailer), I made three separate purchases of Links Credential Capture to track any upgrades or developments to the kits.


7. I began this process by accessing the RaccoonO365 online store where I began anonymously communicating via Telegram with the RaccoonO365 Defendants. The Defendants use Telegram to advertise their service offerings, including their abilities to bypass Microsoft’s security protections. **Figure 1** is a screenshot of the Telegram channel that RaccoonO365 Defendants use to sell their phishing kits.

Group Info




RaccoonO365  2FA/MFA 

843 members





Don't let Microsoft Office 365 2FA/MFA security barriers hinder your spamming operations. We provide Microsoft 365 (Office365) & Hotmail (Outlook) 2FA link service.

Description




Notifications






5 shared links




ADMINISTRATORS





RaccoonO365 PayMate

has access to messages

admin



RaccoonO365  2FA/MFA  For ...


 owner

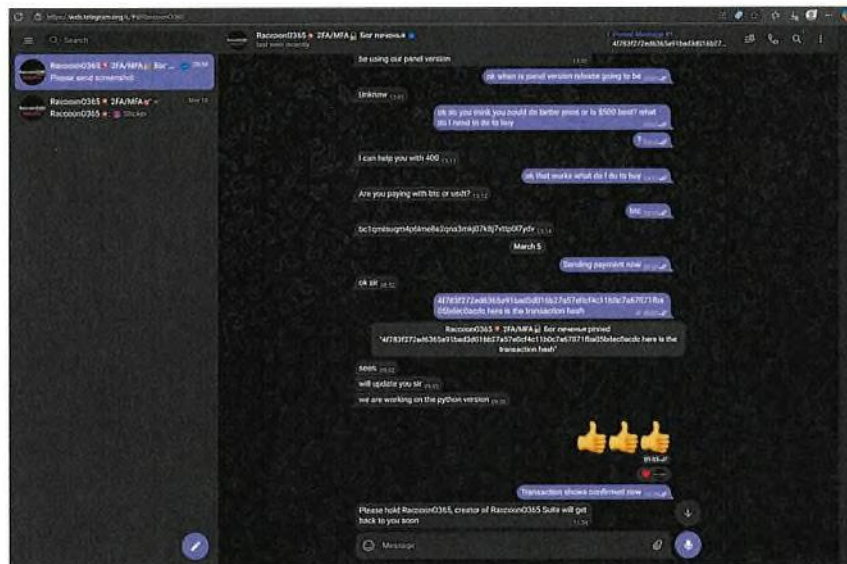
Figure 1

8. As described herein, I used the cryptocurrency account information provided to me by RaccoonO365 Defendants to conduct a further financial analysis of the transactions and the cryptocurrency wallets used by RaccoonO365 Defendants. I conducted this analysis using the information RaccoonO365 Defendants provided to me, open-source information, and Chainalysis Reactor, a tool that facilitates the tracing of cryptocurrency funds.

9. Chainalysis Reactor groups (“clusters”) cryptocurrency addresses that are controlled by the same entity (“clustering”) and then ties those clusters to specific real-world entities based on information gleaned from other sources. Those sources amass information regarding cryptocurrency addresses through test transactions, open source-intelligence (OSINT), collecting and verifying evidence from third parties that have conducted transactions with entities on the blockchain, and exchanging information with law enforcement agencies (“attribution”).

**a. Postman Mass Mailer Test Buy and Investigation**

10. On March 5, 2025, I purchased the Postman Mass Mailer kit via RaccoonO365 Defendants’ Telegram chat. After I demonstrated my interest in purchasing a phishing kit, I made a payment via bitcoin (BTC)<sup>4</sup> to RaccoonO365 Defendants’ deposit address bc1qmlsuqm4p6lme8e2qna3mkj07k8j7vttp017ydv. *See Figure 2.*



**Figure 2**

<sup>4</sup> Bitcoin is a decentralized cryptocurrency that operates a public distributed ledger of transactions, which is referred to a “blockchain.”



11. Using Chainalysis Reactor, I investigated the cryptocurrency transaction associated with the purchase of the Postman Mass Mailer. Through this analysis, I identified that the BTC address `bc1qmlsuqm4p6lme8e2qna3mkj07k8j7vttp0l7ydv`, is likely hosted by a third-party cryptocurrency exchange Bitnob, which is based in Nigeria. **Figure 3** is a screenshot of the Chainalysis Reactor graph showing the tracing of transactions to the RaccoonO365 Defendants BTC deposit address.



**Figure 3**

**b. Links Credential Capture Test Buy and Investigation**

12. Between April and August 2025, I purchased three Links Credential Capture kits.

13. On April 10, 2025, I purchased a Links Credential Capture phishing kit via Telegram. Similar to my prior test buy, once I demonstrated my interest in purchasing a phishing kit, I received payment information from RaccoonO365 Defendants and made a payment via BTC. The RaccoonO365 Defendant provided the previous BTC address `bc1qmlsuqm4p6lme8e2qna3mkj07k8j7vttp0l7ydv` for payment which again was hosted by the third-party cryptocurrency exchange Bitnob, based in Nigeria. **Figure 4.**

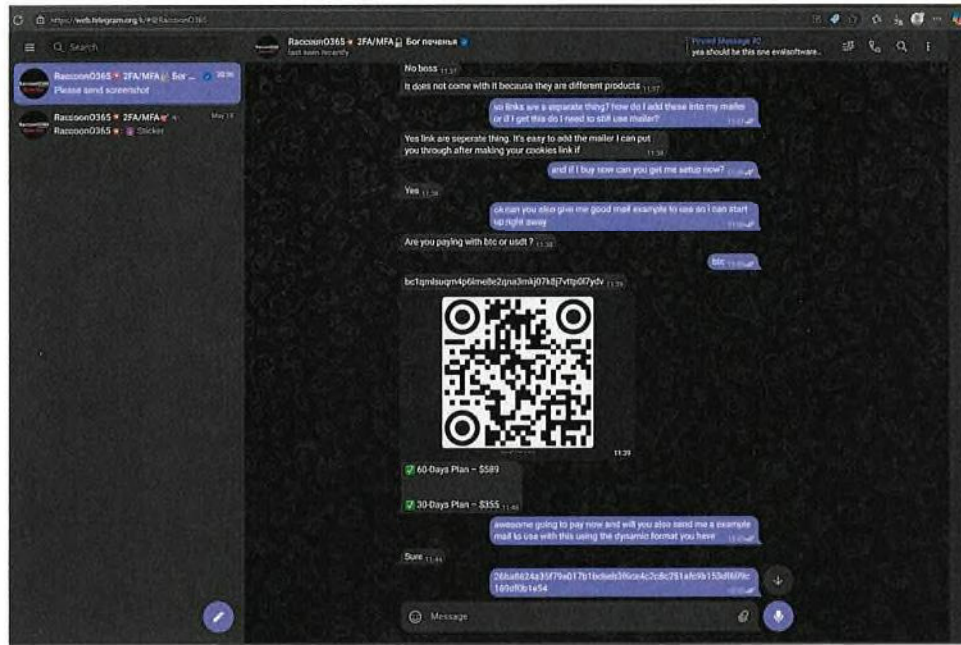
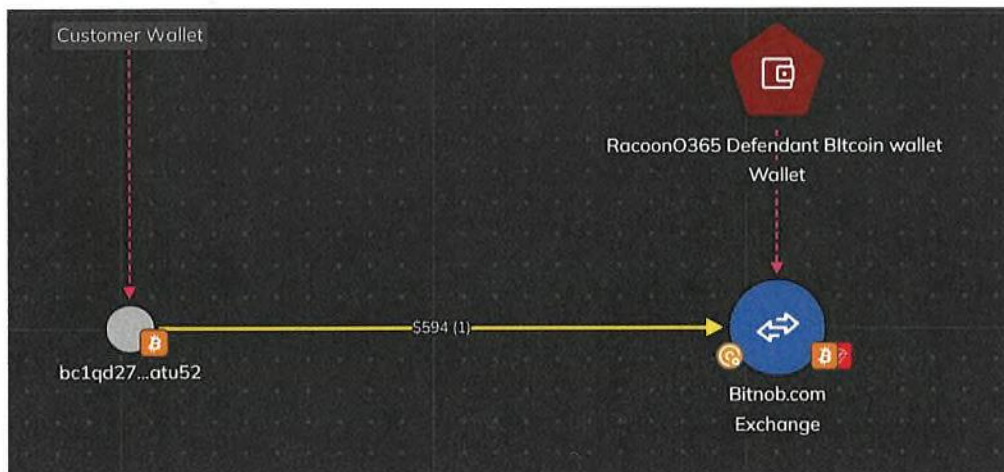


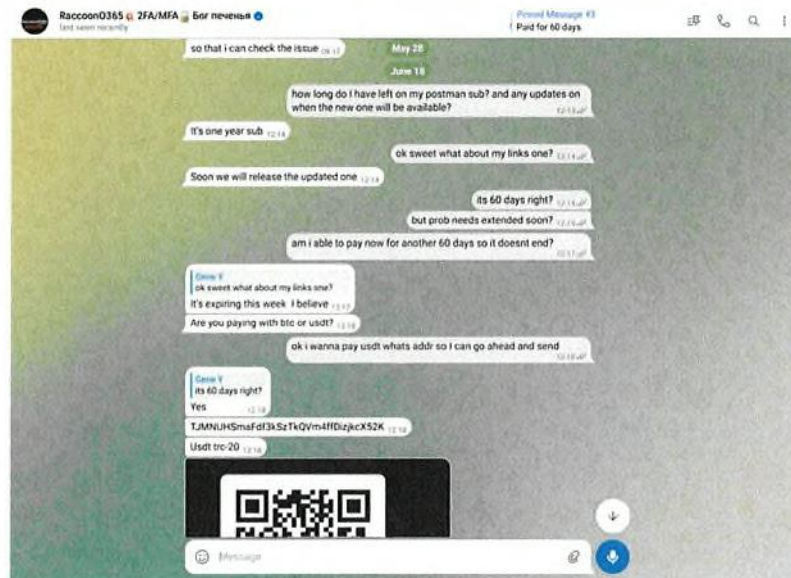
Figure 4

14. I also analyzed this purchase using Chainalysis Reactor to investigate the cryptocurrency transaction associated with the purchase of the Links Credential Capture tool. I determined that the BTC address `bc1qndsuqm4p6lme8e2qna3mkj07k8j7vtp0l7ydv`, linked to the Raccoon0365 Defendants, had received approximately \$33,921 USD in BTC since the creation of the wallet in October 2024. **Figure 5** displays a screenshot from Chainalysis Reactor, illustrating the transaction flow and connections to the Raccoon0365 Defendants' BTC address.



**Figure 5**

15. On June 18, 2025, I purchased a second Links Credential Capture kit through the RaccoonO365 Defendants' Telegram channel. Like before, once I had demonstrated my interest in purchasing a phishing kit, the chat administrator provided me with payment information that would allow me to make a payment via a Tether USDT (TRC-20)<sup>5</sup> address. A screenshot of my Telegram conversation documenting the test buy is included as **Figure 6**.



**Figure 6**

16. During the negotiation phase of this purchase, the RaccoonO365 Defendants initially provided me with the USDT (TRC-20) address TJMNUHSmaFdf3kSzTkQVmf4ffDizjkeX52K. As shown in **Figure 6**, the RaccoonO365 Defendants subsequently provided me with an alternative cryptocurrency address: the USDT (TRC-20) address 0xf5C2E3749F332175D94C7de7bf7AA8d679E460B7, designated for the acquisition of the Links Credential Capture. I believe that the first address was provided to me in error, likely a lapse in operational security on the part of RaccoonO365 Defendants. Because I

<sup>5</sup> Tether (USDT) is a digital currency and stablecoin that is tied to the US Dollar.



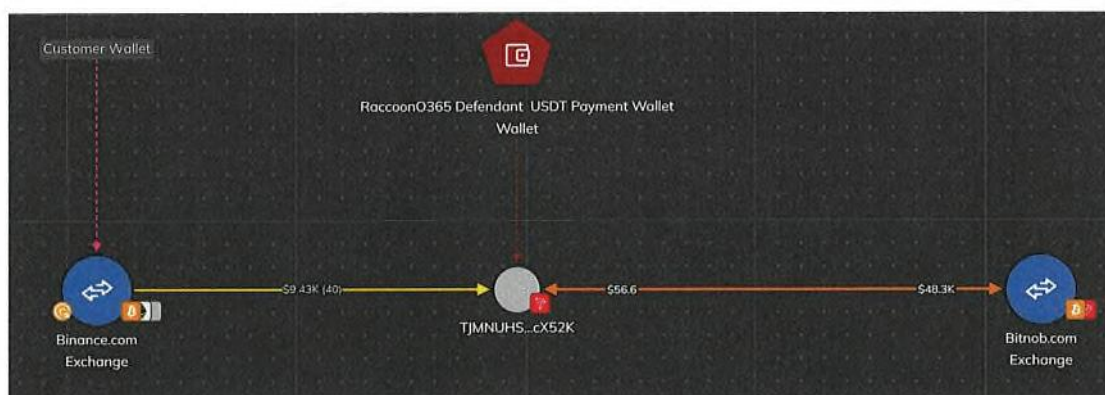
now had two data points (the initial wallet address and the later-provided wallet address), I was able to conduct additional analysis of the financial aspect of RaccoonO365 Defendants operations, which revealed important operational attributes.

17. Using Chainalysis Reactor, I investigated the USDT (TRC-20) address TJMNUHSmaFdf3kSzTkQVm4ffDizjkcX52K, initially provided by the RaccoonO365 Defendants. Blockchain analysis revealed that this address had received approximately \$48,312 USD in USDT since its creation in June 2024. Transaction tracing showed that the full balance of approximately \$48,375 USD was subsequently transferred to a USDT address hosted on the Nigerian cryptocurrency exchange Bitnob. This exchange had previously been linked to the RaccoonO365 Defendants through BTC transactions, as established in earlier analysis.

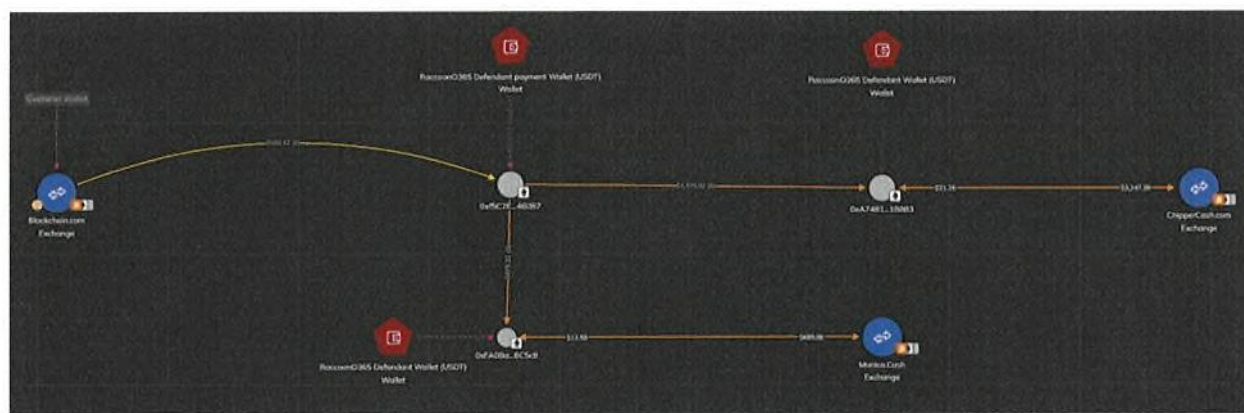
18. In addition, I examined the USDT (TRC-20) address 0xf5C2E3749F332175D94C7de7bf7AA8d679E460B7, which was designated for the acquisition of the Links Credential Capture tool.

19. This address received approximately \$2,545 USD in USDT since its creation in May 2025. Transaction tracing revealed that approximately \$1,888 USD was transferred to the recipient address 0xA748128Dcc07D8dD7956ff227AE4066bE601B883. The recipient address exhibited a total transactional flow of approximately \$3,255 USD, indicating that it received additional funds beyond the initial transfer. Subsequent tracing confirmed that funds from this recipient address were forwarded to another wallet associated with the cryptocurrency exchange ChipperCash.com. Further analysis identified a separate transaction in which the payment address 0xf5C2E3749F332175D94C7de7bf7AA8d679E460B7 transferred \$675 USD in USDT to the address 0xFA0Ba0f689D1c3A932023583fccFB8622dD6C5c8. This latter address then transferred the full amount to a USDT address hosted by the merchant service Monica.cash, which

is based in Nigeria. Chainalysis graphs tracing of the USDT(TRC-20) addresses are provided below in **Figure 7** and **Figure 8**.



**Figure 7**



**Figure 8**

20. On August 11, 2025, I purchased a third Links Credential Capture kit through the RaccoonO365 Defendants' Telegram channel. The chat administrator provided me with payment information that would allow me to make a payment via a Tether USDT (TRC-20). The screenshots of my Telegram conversation documenting this test buy are included as **Figure 9** and **Figure 10**. This test buy revealed that RaccoonO365 Defendants had updated their business model. First, as shown in **Figure 10**, RaccoonO365 now offers different subscription terms for the Links Credential Capture kit. The offering of different subscriptions at different price points suggests that RaccoonO365 Defendants are growing the operation and seeking to sell to more

customers. Second, RaccoonO365 Defendants added alternative cryptocurrency payment options. This also indicates that RaccoonO365 is growing its operations, by making itself more accessible to users of different currencies (for example, the same way that businesses may grow their reach by accepting multiple credit cards or different global currencies).

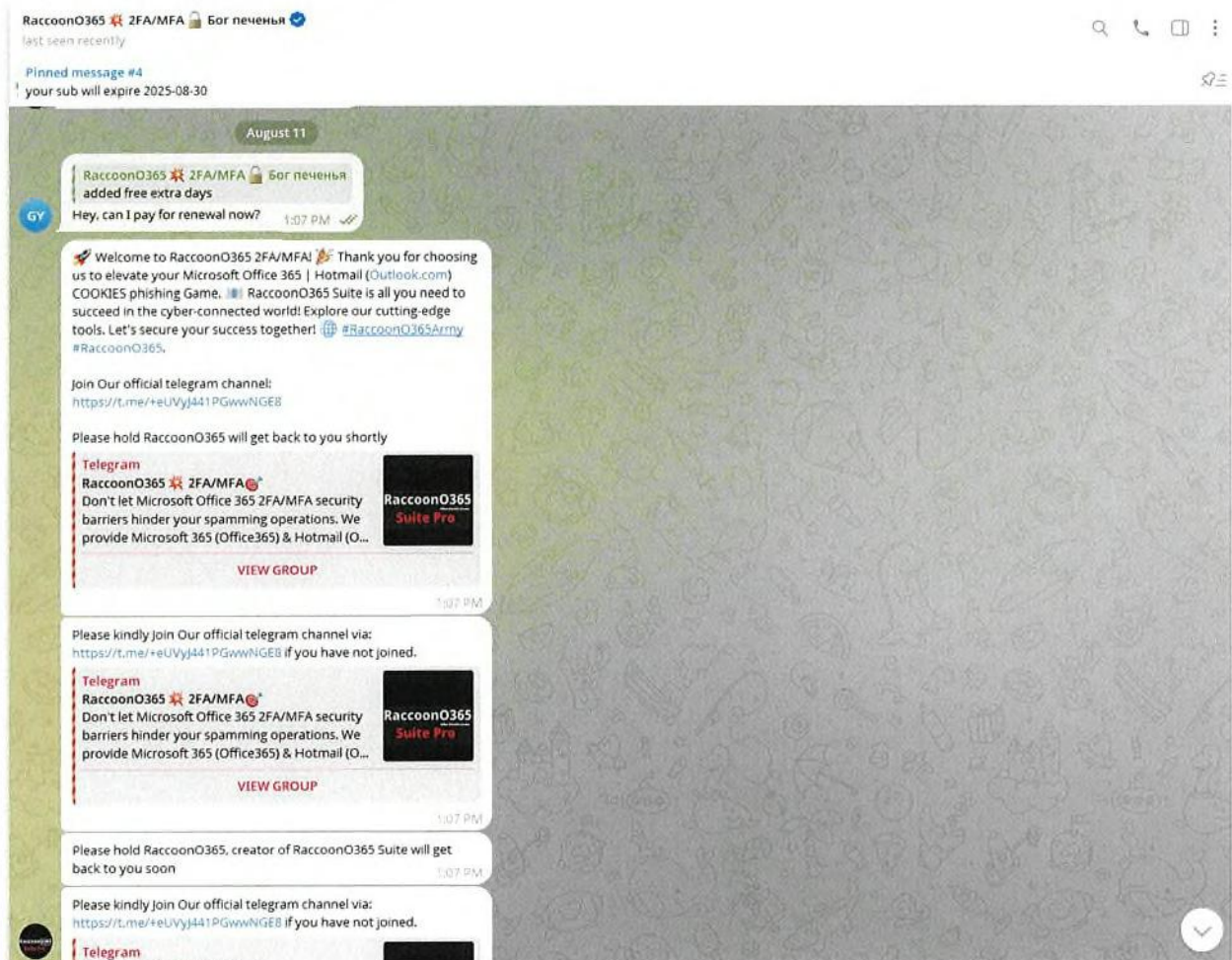
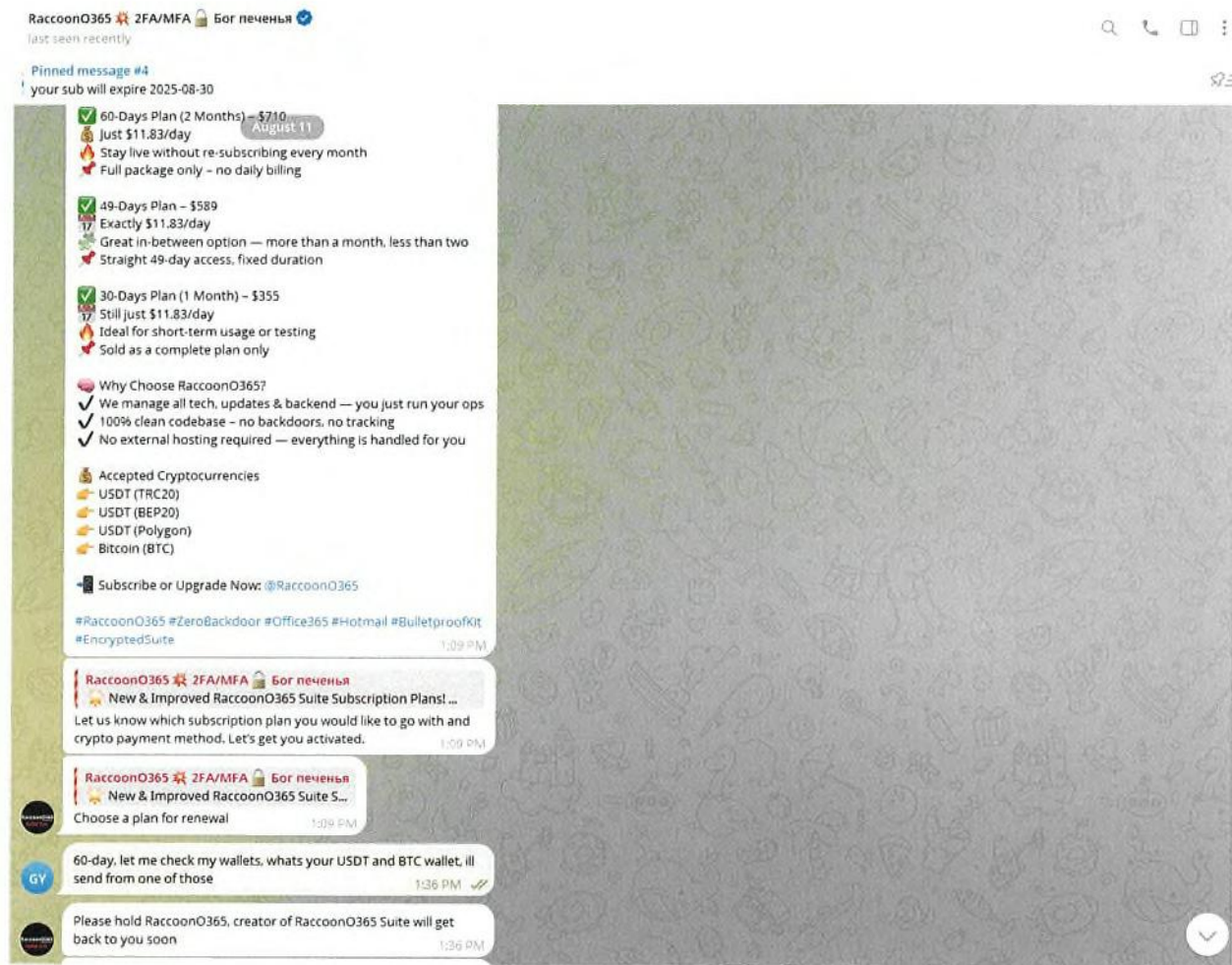


Figure 9





**Figure 10**

21. During the negotiation phase of the controlled purchase, I requested both USDT and BTC addresses from the RaccoonO365 defendants. In response, they provided the USDT (TRC-20) address TBB5T28b9n2SK8shXb9oq867EcsNE5dZie and the BTC address bc1qjtlzug5wu7ag8yskn5h2xjd27uetq5cc4sahh5. As illustrated in **Figure 11** and **Figure 12**, these addresses differ from those previously used by the Defendants in earlier test purchases, indicating



that they had changed or added to their cryptocurrency payment accounts.

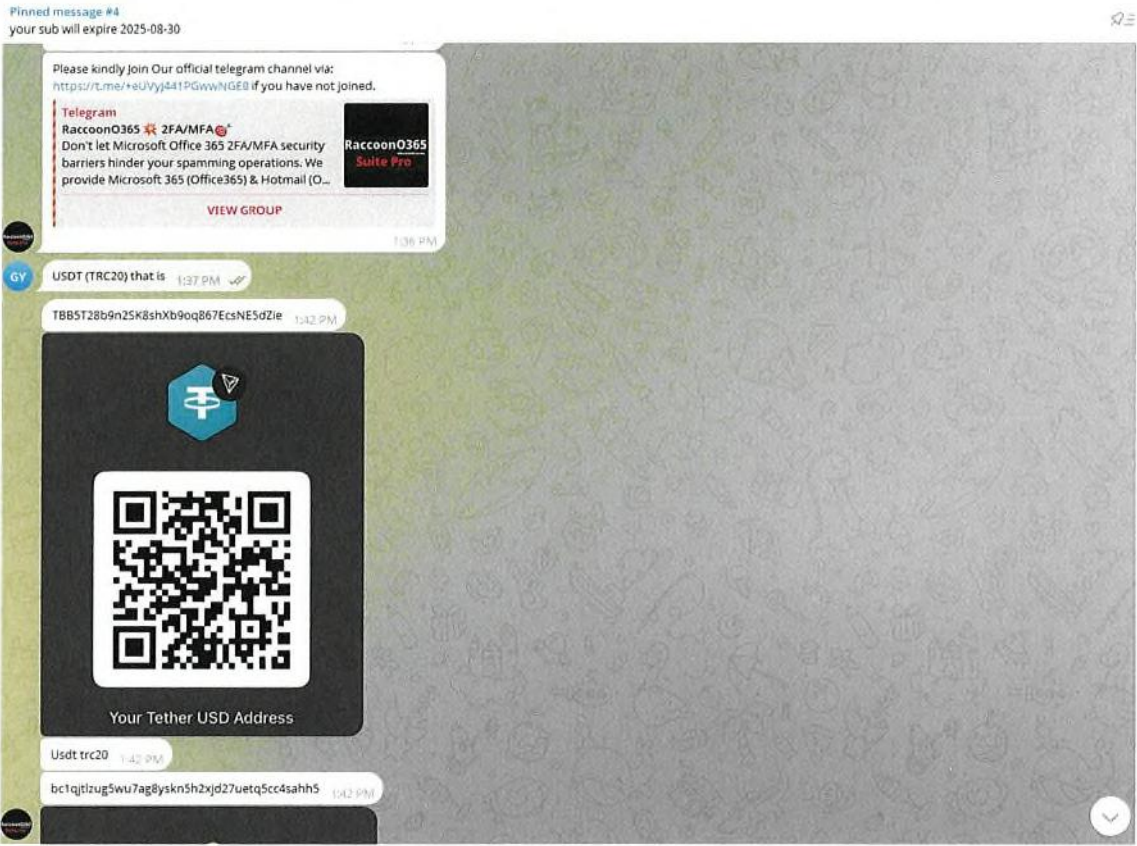
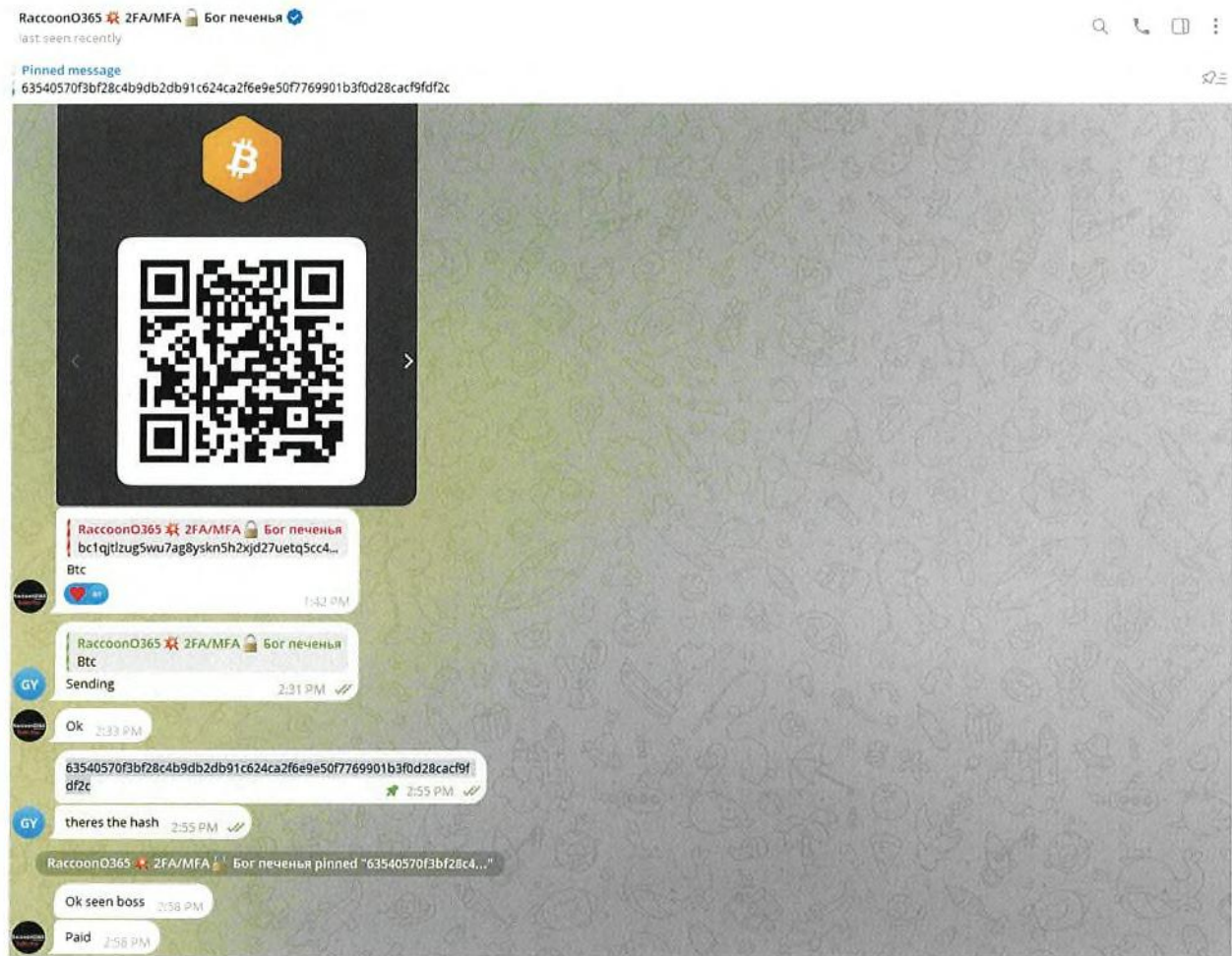


Figure 11

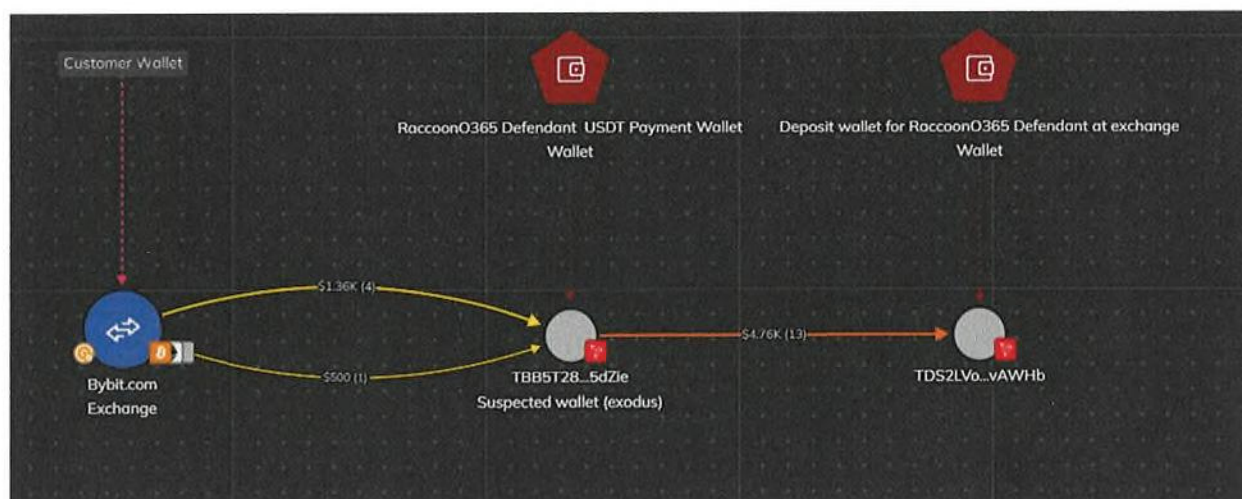


**Figure 12**

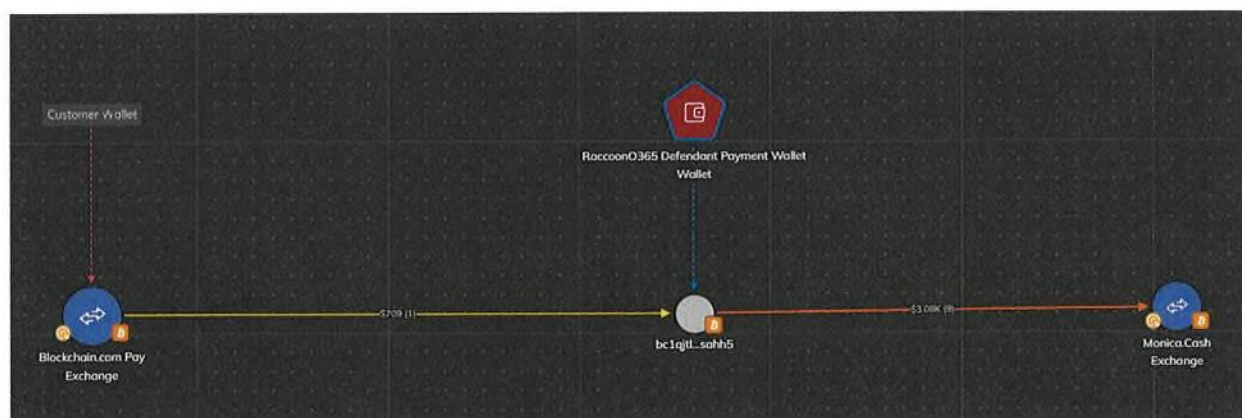
22. Using Chainalysis Reactor, I investigated the USDT (TRC-20) address TBB5T28b9n2SK8shXb9oq867EcsNE5dZie that the RaccoonO365 Defendants provided. Blockchain analysis revealed that this address had received approximately \$5,933 USD in USDT since its creation in July 2025. This shows the RaccoonO365 Defendants have added additional addresses since our last purchase. Additionally, I examined the BTC address bc1qjtlzug5wu7ag8yskn5h2xjd27uetq5cc4sahh5 provided by RaccoonO365 Defendants in connection with my purchase of the Links Credential Capture tool. This address received approximately \$5,442 USD in BTC since its creation in July 2025. Transaction tracing revealed that approximately \$3,957 USD has been transferred from this address to another BTC address



that is likely hosted at a merchant service called Monica.cash which is located in Nigeria. A Chainalysis graph tracing of the USDT(ERC-20) address and BTC address is provided below in **Figure 13** and **Figure 14**.



**Figure 13**



**Figure 14**

23. In total, I have been able to trace approximately \$100,000 in cryptocurrency payments attributed to purchases of the RaccoonO365 kits based on the wallets that RaccoonO365 Defendants provided to me. Based on my experience, it is likely that RaccoonO365 Defendants utilize other wallets in connection with the sale of the RaccoonO365 kits. From the cryptocurrency that I was able to trace, plus the average subscription costs for the products, I estimate that

approximately 100-200 subscriptions are tied to the \$100,000. The subscriptions are not single use, and even with 100-200 subscriptions (which I believe to be an underestimate of the total subscriptions), RaccoonO365 Defendants can send hundreds of millions of phishing emails per year.

24. After I purchased the RaccoonO365- phishing kits and the requisite cover and phishing domains, I followed the instructions RaccoonO365 Defendants provided to connect the domains to the infrastructure. *See Declaration of Jason Lyons in Support of Ex Parte Application ¶¶ 37-45.* I then performed a test phishing attack to “phish” a Microsoft account that was specifically created for this investigation. This allowed me to observe how the phishing kit operated.

25. Not only did the test purchases allow me to trace the financial transactions and uncover operational details, it provided Microsoft with information about how the kits work, how they can be used by cybercriminals, and how stolen credentials are delivered.

**c. Attempted Test Buy of AI Powered Tool**

26. Within the RaccoonO365 Telegram channel, Defendants have also advertised AI MailCheck, an AI-powered tool that is still in development and has not been released yet. *See Figure 15.* Based on the advertisement, I believe that AI MailCheck will deploy AI to verify and optimize phishing targets. Based on my experience, this demonstrates that RaccoonO365 Defendants have the technical sophistication to evolve and improve their phishing kits to meet customer demand and why these kits are so dangerous to Plaintiffs and the public. I attempted to purchase this product and requested information about when it would be ready. I was told that the code was ready, however RaccoonO365 Defendants were still determining business and marketing strategy. *See Figure 16.*



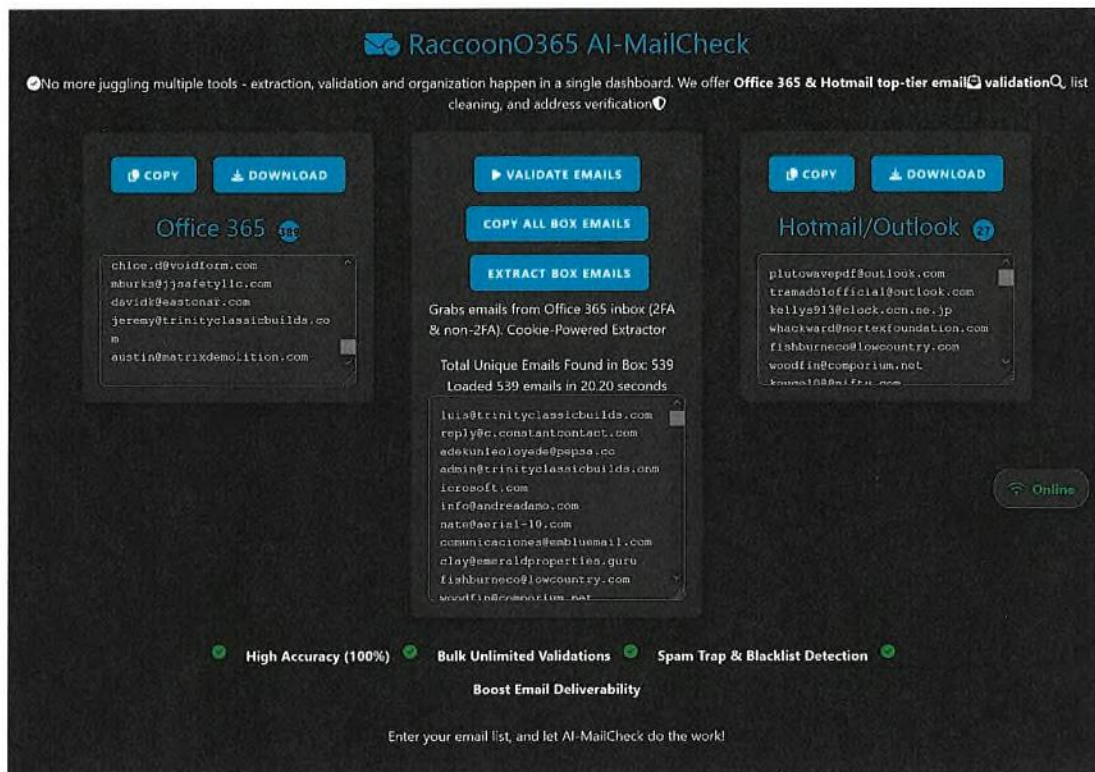


Figure 15 – Screenshot of RaccoonO365’s Advertisement of Future AI-Powered Kit



Figure 26 – DCU Investigator Communication with RaccoonO365 Defendants Regarding AI-Powered Tool

I declare under penalty of perjury under the laws of the United States that the forgoing is true and correct to the best of my knowledge.

Executed August 25, 2025 in New York, New York.



---

Nick Monaco  
Principal Investigator, Digital Crimes Unit  
Microsoft Corporation

# EXHIBIT 1

# Nick Monaco

## Employment

Principal Investigator

*Microsoft Digital Crimes Unit (DCU)*. Feb 2025-present.

China Research Lead and Director of Technology

*Microsoft Threat Analysis Center (MTAC)*. Aug 2022-Feb 2025. Built and maintained MTAC's technical stack, led research on cross-Strait threats. Represented MTAC with public-facing research and speaking engagements.

Chief Innovation Officer and Director of China Research. *Miburo Solutions*. Built and led Miburo's technology development and China research. These efforts led in part to Microsoft's acquisition of the company in August 2022. Jan 2021-Aug 2022

Research Director. *Digital Intelligence Lab at Institute for the Future*. Directing public-facing research on disinformation and digital rights. July 2019 – Dec 2020

Disinformation and Intelligence Analyst. *Graphika*. Jan 2018 – June 2019

Researcher. *Google Jigsaw*. Nov 2016 — Oct 2017

## Education

Master's of Science in Computational Linguistics. *University of Washington*. Seattle, WA. Sept. 2014 – June 2016

International Chinese Language Program (ICLP). *National Taiwan University*. Sept. 2012-Dec. 2013.

Bachelor of Arts in French and Bachelor of Arts in German. 2007-2012. *University of Wisconsin-Madison*. Madison, WI. GPA: 3.98/4.00

Eight-week Summer Intensive Language programs for German/Chinese. *Middlebury College*. 2008/2011

## Technical education

**SANS SEC504: Offensive Hacking Techniques** Completed March 2024.

**SANS SEC593: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals.** Completed May 2025.

## Skills

**Certifications:** GIAC Machine Learning Engineer (GMLE)

**Programming Languages:** Python, KQL, Java.

**Web Scraping/Data Collection:** extensive familiarity with web APIs, Selenium, Python requests and BeautifulSoup.

**Natural Languages:** Native English, fluent Mandarin Chinese, fluent French, fluent German, advanced Italian.

**Fellowships:** Carnegie Endowment for International Peace Partnership for Countering Influence Operations (PCIO) Guild Member, Oxford Internet Institute research affiliate, Institute for the Future research affiliate



## Selected Press

Microsoft Threat Intelligence Podcast (2024, Oct.). *Gingham Typhoon's Cyber Expansion Into the South Pacific*.  
Sanger, D., and Myers S. (2022, Sept.) *China Sows Disinformation About Hawaii Fires Using New Techniques*. The New York Times.  
Alba, D. (2021, Dec.). *Pro-China group continues to spread misinformation, researchers say*. The New York Times.  
Silverman, C. (2020, Mar.). *Chinese Trolls Are Spreading Coronavirus Disinformation In Taiwan*. BuzzFeed.  
Samuels, E. and Akhtar, M. (2019, Nov.). *Are 'bots' manipulating the 2020 conversation? Here's what's changed since 2016*. The Washington Post.  
Zhong, R., Myers S., and Wu. J (2019, Sept.). *How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters*. The New York Times.  
Good, C. (2019, June). *Gab's Islamophobic content draws from YouTube, Twitter, study finds*. CNN.  
Monaco, N. (2019, March). Computational Propaganda with Nick Monaco. *Carnegie Council Audio Podcast*.  
Monaco, N. (2018, Oct.). Midterm Election Special. *Breach Podcast*.  
Riley, M., Etter, L., and Pradhan, B. (2018, March). *A Global Guide to State-Sponsored Trolling*. Bloomberg.  
Woolley, S. and Monaco, N. (2017, Oct.). Segment on Buying Bots Online and the 2016 Presidential Election. *NBC Nightly News*.  
Monaco, N. (2017, Aug.). Long-form interview on Bots and Disinformation. The Open Mind, PBS.

## Selected Publications

MTAC East Asia Team (2024, April.). *China tests US voter fault lines and ramps AI content to boost its geopolitical interests*. Microsoft.  
MTAC East Asia Team (2023, Sept.). *Digital threats from East Asia increase in breadth and effectiveness*. Microsoft.  
Monaco, N. and Woolley, S. (2022, July). Bots. *Polity Press*.  
Monaco, N. and Eide, C. (2022, Apr.) How China is Selling its Muslim Genocide to the Arab World. *National Endowment for Democracy Power 3.0*.  
Agsten, C., Turner, L., and Monaco, N. (2022, Mar.) Chinese State Media Rehashes U.S. Biolab Conspiracy Theories, This Time with a Ukraine Angle. *Miburo Solutions Substack*.  
Monaco, N. (2022, Feb.). 2+2=5: Signatures from Chinese COVID-19 WeChat Petition to the WHO Show Signs of Manipulation. *Miburo Solutions Substack*.  
Yang, J. and Monaco, N. (2022, Jan.). Why the US Must Take China's Disinformation Operations Seriously. *The Diplomat*.  
Monaco, N. (2022, Dec.). Spamouflage Survives: The Series. *Miburo Solutions Substack*.  
Monaco, N., Smith, M., and Studdart, A. (2020, Aug.). Detecting Digital Fingerprints: Tracing Chinese Disinformation in Taiwan. *Digital Intelligence Lab at Institute for the Future, Graphika and the International Republican Institute (IRI)*.  
Monaco, N., Minnehan, S. and Joseff, K. (2020, Aug.). The Hyperconnected World of 2030-2040. *Institute for the Future*.  
Woolley, S. and Monaco, N. (2020, July). Amplify the Party, Suppress the Opposition: Social Media, Bots, and Electoral Fraud. *Georgetown Law Technology Review*. Issue 4.2. *Georgetown Law*.  
Monaco, N. and Arnaudo, D. (2020, May). Data Analytics for Social Media Monitoring. *National Democratic Institute (NDI)*.  
Monaco, N. (2020, Mar.) No Rest for the Sick: Coronavirus Disinformation from Chinese Users Targets Taiwan. *DigIntel Blog*.  
Monaco, N. (2019, Nov.). #DemDebates Data: Hashtag Hijacking, Antivax Disinfo, Cyborgs and Godmen. *DigIntel Blog*.  
Monaco, N. (2019, Sept.) Welcome to the Party: A Data Analysis of Chinese Information Operations. *DigIntel Blog*.  
Monaco, N. and Woolley, S. (2019, Sept.). Natural Language Processing and Global Development: A Future-Focused Primer. *USAID and Duke University, Convening Brief: Digital Tools and the Future of International Development*.  
Pakzad, R., Woolley, S. and Monaco, N. (2019, June). Incubating Hate: Islamophobia and Gab. *German Marshall Fund (GMF)*.  
Kumleben, M. and Monaco, N. (2019, May). Can the Center Hold? Moderate Republicans as Disinformation Targets in 2018. *Digital Intelligence Lab at Institute for the Future*.  
Monaco, N. and Nyst, C (2019, April). *Patriotic Trolling: A Survey of State-Sponsored Trolling Worldwide*, Chapter in: *Media and Mass Atrocity: The Rwanda Genocide and Beyond*. CIGI Press.

- Monaco, N. (2019, Jan.). Troll up your Sleeves: Using Research to uncover State-Sponsored Harassment Online. *NED Power 3.0 Blog*.
- Monaco, N. (2018, Nov.). *Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy*, Chapter in: *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press.
- Monaco, N. and Nyst, C. (2018, Sept.). State-Sponsored Trolling How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns. *Digital Intelligence Lab at Institute for the Future*.
- Monaco, N. (2018, May). Vorsicht - Die Digitalisierung ermöglicht neue Dimensionen an Überwachung und Desinformation. Sie kann damit zu einer Gefahr für die Demokratie werden. *Schweizer Monat*.
- Monaco, N. (2018, April). What makes some people more susceptible to Disinformation? *NDI DemocracyWorks Blog*.
- Monaco, N. and Woolley, S. (2017, Sept.). Tech companies automate autocratic media in China around the world. *Tech Crunch*.
- Monaco, N. & Woolley, S. (2017, Nov.). Reactions and Regulation in the Age of Computational Propaganda. *The Ripon Forum*.

### **Selected Invited Talks and Conferences**

- Monaco, N. (2024, Jan). *China's Digital Influence as Power*. Hoover History Lab Conference: Global Futures II "The Changing Nature of Power". Stanford.
- Monaco, N. (2023, March). Series of Talks on Civil Society Resilience in the Age of Generative AI and Disinformation. *Stanford Digital Tech Camp*.
- Monaco, N., Turner, L. and Hinkins, N. (2022, April). Xinjiang: A Wonderful Land? China's Xinjiang Disinformation in the Indo-Pacific and Beyond. *US Department of State Global Engagement Center, Quad Counter-Disinformation Working Group*.
- Monaco, N. and Turner, L. (2022, April). When Three People Say Tiger: Chinese Propaganda and Disinformation. *National War College*.
- Monaco, N. and Arnaudo, D. (2021, Sept.). Series of 3 Workshops on Data Gathering and Online Investigation Techniques for African Civil Society. *Info/tegrity Africa*. NDI.
- Monaco, N. (2021, April). Tools and Techniques for Online Investigation. *Asia+ disinformation project*. Doublethink Lab and Innovation for Change.
- Monaco, N. (2021, February). Briefing on Chinese Disinformation in Taiwan's January 2020 Presidential Election. United States Department of State Global Engagement Center (GEC) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)
- Monaco, N. (2020, Aug.). Crouching Liar, Hidden Dragon: Chinese Disinformation in Taiwan. *Symposium on Chinese Information Operations*. Facebook Taiwan and DoubleThink Lab.
- Monaco, N. (2020, June). Basic Data Collection and Analysis Techniques. *Data Analytics for Social Media Monitoring*. National Democratic Institute (NDI).
- Monaco, N. (2020, May). Basic Open-Source Intelligence Techniques. *Disinformation During a Global Pandemic: How to Identify and Expose Malign Influence*. International Republican Institute (IRI).
- Monaco, N. (2020, Feb.). Talk on DigIntel's Research on Disinformation in Taiwan's January 2020 Election. *CSIS China Power Project - Event on PRC Interference in Taiwan's Election*. Washington, D.C.: Center for Strategic and International Studies.
- Monaco, N. (2020, Feb.). Amplify the Party, Suppress the Opposition: Social Media, Bots, and Electoral Fraud. *Georgetown Law Election Integrity Symposium*. Washington, D.C.: Georgetown University.
- Monaco, N. (2020, Feb.) Series of talks on Info Ops, Election Integrity and Disinformation and Cross-Strait Relations. *Stanford GDPI/INCL AI/Tech Bootcamp*. Palo Alto, CA: Stanford.
- Monaco, N (2019, Nov.). Best Practices for Protecting Journalists from Weaponized Hacking, Trolling and Disinformation. *Senior Foreign Editors Circle*. New York, NY: Associated Press.
- Monaco, N (2019, Nov.). Chinese Information Operations. *China in the World 2019*. Taipei, Taiwan: Doublethink Lab and National Endowment for Democracy.
- Monaco, N (2019, Sept.). Chinese Information Operations and Election Integrity in Taiwan. *GTI-Prospect Young Scholars Exchange Program*. Taipei, Taiwan: Global Taiwan Institute and Prospect Foundation.
- Monaco, N (2019, April). Election Integrity: A Comparative Analysis of Nigeria and Macedonia. *Emerging Trends in Social Media*. April 2019. Riga, Latvia: NATO StratCom.

- Monaco, N. (2017, Dec.). Patriotic Trolling: State-Sponsored Trolling Worldwide and in Rwanda. *Media and Mass Atrocity: The Rwanda Genocide and Beyond*. Ottawa, Canada: Carleton University.
- Monaco, N. (2017, Nov.). How Bots and Trolls Disseminate Disinformation in the Philippines and Worldwide. *Truth, Trust, and Democracy in the Age of Selfies, Trolls, and Bots*. Manila, Philippines: Rappler.
- Monaco, N. (2017, Nov.). Computational Propaganda: Challenges and Solutions. *ParlAmericas 14th Plenary Assembly*. Medellín, Colombia: ParlAmericas.
- Monaco, N. (2017, Sept.). The State of Computational Propaganda in Cross-Strait Relations. *The Corrosion of Democracy under China's Global Influence*. Arlington, Virginia, USA: Taiwan Foundation for Democracy.