

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

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

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**

COMPLAINT

Plaintiffs Microsoft Corporation (“Microsoft”) and Health-ISAC, Inc. (“Health-ISAC”), by their attorneys, bring this action against Joshua Ogundipe and John Does 1-4 (collectively “RaccoonO365 Defendants”), who manufacture and sell illegal “phishing” kits, deceptively branded as “RaccoonO365”¹ designed to steal sensitive information, and perpetrate business email compromise, ransomware, and financial fraud against Microsoft customers, Health-ISAC member organizations, and the public. Plaintiffs assert claims based on (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (3) Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d); (4) The Electronic Communications Privacy Act, 18 U.S.C. § 2701; (5) False Designation

¹ One of the enterprise products that Microsoft offers is a software suite known as “Office 365,” which is often abbreviated to “O365.” By using “O365” in connection with the Raccoon phishing kits, the threat actors falsely associate their kits with the O365 product and Microsoft brand.

of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (6) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (7) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (8) common law trespass to chattels; (9) conversion; and (10) unjust enrichment.

Plaintiffs allege as follows:

NATURE OF THE ACTION

1. American companies and individuals are besieged daily by cybercriminals seeking to infiltrate or disrupt the vital technologies necessary to maintain their confidential information, operate their businesses, and communicate both internally and to the public. These cybercriminals target reputable organizations to steal and then leverage or sell their confidential information to commit further cybercrimes.

2. This action involves the relentless and persistent phishing attacks conducted and facilitated by a foreign cybercrime organization designated as “RaccoonO365 Defendants,” against Microsoft and its customers, Health-ISAC and its member organizations, and the public, seeking to steal personal and business information for use in perpetrating additional cybercrimes.

3. One of the most pernicious forms of cybercrime is known as “phishing,” which entails luring online victims to open weaponized emails and attachments by tricking them to believe the emails come from a trusted and legitimate source.² RaccoonO365 Defendants manufacture, sell, and facilitate the deployment of pre-packaged phishing kits that enable other cybercriminals to launch phishing attacks with relative ease.

² The estimated financial impact of phishing in 2024 is over \$3.5 billion US. Microsoft, *Microsoft Digital Defense Report 2024*, at p. 34, available at <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf> (Oct. 2024) (“2024 MDDR”).

4. The RaccoonO365 Defendants sell these phishing kits to other cybercriminals, who use these kits to tailor their attacks to particular industries using specialized messages and “subject” lines as bait. A cybercriminal can purchase the phishing kit that best serves its criminal objective, including selecting which companies’ products and systems it wishes to infiltrate and the lure it wants to use. RaccoonO365 Defendants have targeted Microsoft customers and Health-ISAC member organizations with subject lines indicating urgent activity regarding tax and healthcare documents to trigger an immediate response from the victims. Indeed, Health-ISAC members are the subject of ongoing phishing attacks that have led to severe disruptions in patient care in the past.

5. RaccoonO365’s business model of selling phishing kits and services for use by other cybercriminals is also referred to as “Phishing-as-a-Service” or “PhaaS.” These phishing kits include email templates, fake website templates, domain registration services, and customer support features designed to evade detection and lead victims to believe they are dealing with legitimate products. The kits are essentially “how to” or “do it yourself” manuals for cybercriminals to develop and execute attacks on email systems through phishing campaigns, regardless of technical sophistication or capability. The RaccoonO365 Defendants’ phishing operation provides the gateway and know-how for cyber criminals to attack Microsoft customers, including Health-ISAC member organizations, and steal their personal and confidential business information.

6. Together with the purchasers and users of the RaccoonO365 phishing kits, Defendants Joshua Ogundipe and the John Does are involved in the development, creation, and sale of the phishing kits and have collectively formed a criminal racketeering enterprise that works

in tandem to carry out cyberattacks against Microsoft, its customers, Health-ISAC and its member organizations, and the public.

7. These RaccoonO365 phishing kits are particularly destructive as they facilitate “adversary in the middle” (“AiTM”) attacks whereby the attacker is allowed into the victim’s system (through affirmative actions by the victim, such as clicking a link and providing credentials) with the ability to intercept communications and deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved.

8. Microsoft, without disclosing its identity, recently conducted four separate “test buys” of RaccoonO365 phishing kits. Microsoft purchased the kits complete with instructions on how to target Microsoft customers, avoid detection, and become part of RaccoonO365 Defendants’ vast phishing infrastructure. In doing so, Microsoft observed and confirmed the ease and impact of deploying a RaccoonO365 phishing kit. These test buys also permitted Microsoft to track the cryptocurrency transactions of the RaccoonO365 Defendants, confirming the scope of RaccoonO365 Defendants’ phishing activities.

9. Through these test buys and Microsoft’s ongoing investigation, Microsoft determined that RaccoonO365 Defendants have established and operate an infrastructure of websites, domains, and computers, which they use to target their victims. The identity of the website domains used by RaccoonO365 Defendants to support their phishing operation are set forth at **Appendix A**. The domains set forth in **Appendix A** include both the domains that the sellers of the RaccoonO365 kits use to support the administrative panel³³ and the domains that are

³³ RaccoonO365 Defendants offer customers an “administrative panel,” which functions as a consumer dashboard to track recipients of phishing emails, track whether a phishing attack has

independently acquired by the customer/threat actors and then connected into the RaccoonO365 infrastructure. *See infra* ¶ 53. This aggregating of domains to launch attacks against Microsoft customers constitutes a racketeering enterprise.

10. To carry out their criminal racketeering enterprise, the RaccoonO365 Defendants illegally use Microsoft's trademarks and logos. Microsoft has spent considerable time and resources developing goodwill and its reputation as a trusted brand, and owns the trademarks associated with the software and services it provides. The RaccoonO365 Defendants have conspired to and have illegally adopted the Microsoft name and logo to carry out phishing activities. They deceive users by sending phishing emails that use Microsoft trademarks on the login screens that users are directed to once they interact with the links or documents in the phishing email. Because a victim sees the Microsoft logo, it believes that the login page is protected by Microsoft's security measures. In reality, the login pages fraudulently use Microsoft's logos and branding and are actually controlled by the RaccoonO365 Defendants, allowing them to steal the credential information from the login in page.

11. The Raccoon 0365 Defendants operate in a fashion similar to another threat actor known as Fake ONNX. The Fake ONNX Defendants also sold do-it-yourself phishing kits and operated as a PhaaS. In November 2024, Microsoft filed a lawsuit in the Eastern District of Virginia and obtained injunctive relief effectively crippling Fake ONNX's cybercriminal operations. *See Microsoft Corporation and LF Projects LLC v. Abanoub Nady and John Does 1-4*, Civil Action No. 1:24-cv-2013-RDA (E.D. VA. Nov. 12, 2024).

been successful, track stolen credentials, and measure other metrics that Customer can use to assess the success of their cybercriminal activity. Ogundipe and the John Doe Defendants responsible for the administration of the phishing kits, manage this dashboard using domains that Microsoft has been able to track back to Ogundipe. To avoid detection, Ogundipe has periodically updated the domain that the panel is run on.

12. In the wake of Microsoft's successful takedown of the Fake ONNX Defendants' infrastructure, the RaccoonO365 Defendants opportunistically sought to fill the void, by developing and marketing their own phishing kits. Based on Microsoft's investigation, the RaccoonO365 phishing attacks first emerged in July 2024, and RaccoonO365 Defendants have steadily expanded their reach, picking up where the Fake ONNX Defendants left off. Microsoft has caught the RaccoonO365 Defendants at an earlier stage than the Fake ONNX cybercriminals.

13. RaccoonO365 Defendants have caused and will continue to cause irreparable injury to Microsoft, its customers, Health-ISAC and its member organizations, and the public. Plaintiffs seek injunctive relief to take down the infrastructure developed and used by the RaccoonO365 Defendants to perpetrate their crimes and other equitable relief and damages against RaccoonO365 Defendants.

PARTIES

14. Microsoft is a corporation duly organized and existing under the laws of the state of Washington, having its headquarters and principal place of business in Redmond, Washington. 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 2008.⁴ 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 MSTIC, Microsoft's threat intelligence center, which is made up of thousands of world-class experts, security

⁴ *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).

researchers, analysts, and threat hunters. MSTIC publishes a threat intelligence blog alerting customers and the public of cybersecurity threats.⁵

15. Plaintiff Health-ISAC is a non-profit corporation duly organized and existing under the laws of the State of Florida, having its headquarters and principal place of business in Ormond Beach, Florida. Health-ISAC is a membership organization comprised of public and private hospitals, ambulatory providers, health insurance payers, pharmaceutical/biotech manufacturers, laboratories, diagnostic, medical device manufacturers, medical schools, medical R&D organizations and other relevant health sector stakeholders. Health-ISAC represents the interests of its healthcare industry members in combating and defending against cyber threats that pose risk and loss to the industry.

16. Upon information and belief, Defendant Joshua Ogundipe is an individual residing in Nigeria who helped create the RaccoonO365-branded phishing kits and controls the RaccoonO365 Defendants' technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, Health-ISAC and its members, and the public.

17. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 1 provides administrative support and assists in the marketing, advertising, and sale of the RaccoonO365 phishing kits in furtherance of effectuating harm to Microsoft, its customers, Health-ISAC and its members,, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 1 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

⁵ See Microsoft, *Threat Intelligence Blog*, available at <https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/> (last accessed Oct. 10, 2024).

18. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 2 provides technical support for the RaccoonO365 Defendants' technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, Health-ISAC and its members, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 2 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

19. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 3 is a cybercriminal, who purchased the RaccoonO365-branded phishing kit, registered a new phishing domain, and incorporated that phishing domain into the RaccoonO365 Defendants' technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, Health-ISAC and its members, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 3 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

20. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 4 is a cybercriminal, who purchased the RaccoonO365-branded phishing kit, registered a new phishing domain, and incorporated that phishing domain into the RaccoonO365 Defendants' technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, Health-ISAC and its members, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 4 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

21. Set forth in **Appendix A** are the identities of and contact information for third-party domain registries that control the domains used by the RaccoonO365 Defendants.

22. Plaintiffs are informed, believe, and thereupon allege that Defendants Joshua Ogundipe and John Does 1-4 jointly own, rent, lease, or otherwise have dominion over the

technical infrastructure, including the domains identified in **Appendix A**, and through this technical infrastructure, control and operate the phishing operation by selling, distributing, implementing, and using the RaccoonO365-branded phishing kits. Plaintiffs will endeavor to amend this Complaint to allege the Doe Defendants' true names and capacities when and if ascertained. Plaintiff will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

23. Plaintiffs are informed, believe, and thereupon allege that the actions and omissions alleged herein undertaken by Defendants Joshua Ogundipe and John Does 1-4 were authorized, controlled, and/or directed, by RaccoonO365 Defendants for which each Defendant is liable. Each Defendant aided and abetted the actions of RaccoonO365 Defendants and benefited from those actions and omissions, in whole or in part. Each Defendant acted as the agent of each of the remaining RaccoonO365 Defendants and acted within the course and scope of such agency and with the permission and consent of other RaccoonO365 Defendants.

24. Third party VeriSign Global Registry Services is the domain name registry that oversees the registration of all domain names ending in ".com" and ".net" and is located at 12061 Bluemont Way, Reston, Virginia 20190. As set forth in **Appendix A**, the RaccoonO365 Defendants use ".com" and ".net" domains in connection with their cybercriminal operation.

25. Third party Public Interest Registry is the domain name registry that oversees the registration of all domain names ending in ".org" and is located at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, Virginia 20190. As set forth in **Appendix A**, the RaccoonO365 Defendants use ".org" domains in connection with their cybercriminal operation.

JURISDICTION AND VENUE

26. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of RaccoonO365 Defendants' violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), the Racketeer Influenced and Corrupt Organizations Act (RICO) (18 U.S.C. § 1962(d)), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125). Pursuant to 28 U.S.C. § 1367, the Court has supplemental jurisdiction over the common law claims of trespass to chattels, conversion, and unjust enrichment claims.

27. The Court has personal jurisdiction over RaccoonO365 Defendants because they engage in conduct availing themselves of the privilege of conducting business in the State of New York, and utilize instrumentalities located in the State of New York and the Southern District of New York to carry out acts alleged herein. Specifically, as shown in **Figures 1-2**, *infra*, RaccoonO365 Defendants direct a significant amount of their cybercriminal activity to New York organizations and individuals.

28. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims has occurred in this judicial district, including that a substantial part of the property that is the subject of Plaintiffs' claims is situated in this judicial district, and because a substantial part of the harm caused by RaccoonO365 Defendants has occurred in this judicial district. RaccoonO365 Defendants engage in conduct availing themselves of the privilege of conducting business in the State of New York, and utilize instrumentalities located in the State of New York and the Southern District of New York to carry out acts alleged herein. **Figure 1** is a heatmap generated through DCU's investigation, showing the location of cybercriminal activity that DCU has attributed to

RaccoonO365 Defendants. As shown in the heatmap, a significant portion of this activity is directed at New York City-based organizations and individuals. **Figure 2** shows that, by volume of attacks, New York City leads the nation in targeted cities. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because RaccoonO365 Defendants are subject to personal jurisdiction in this judicial district.

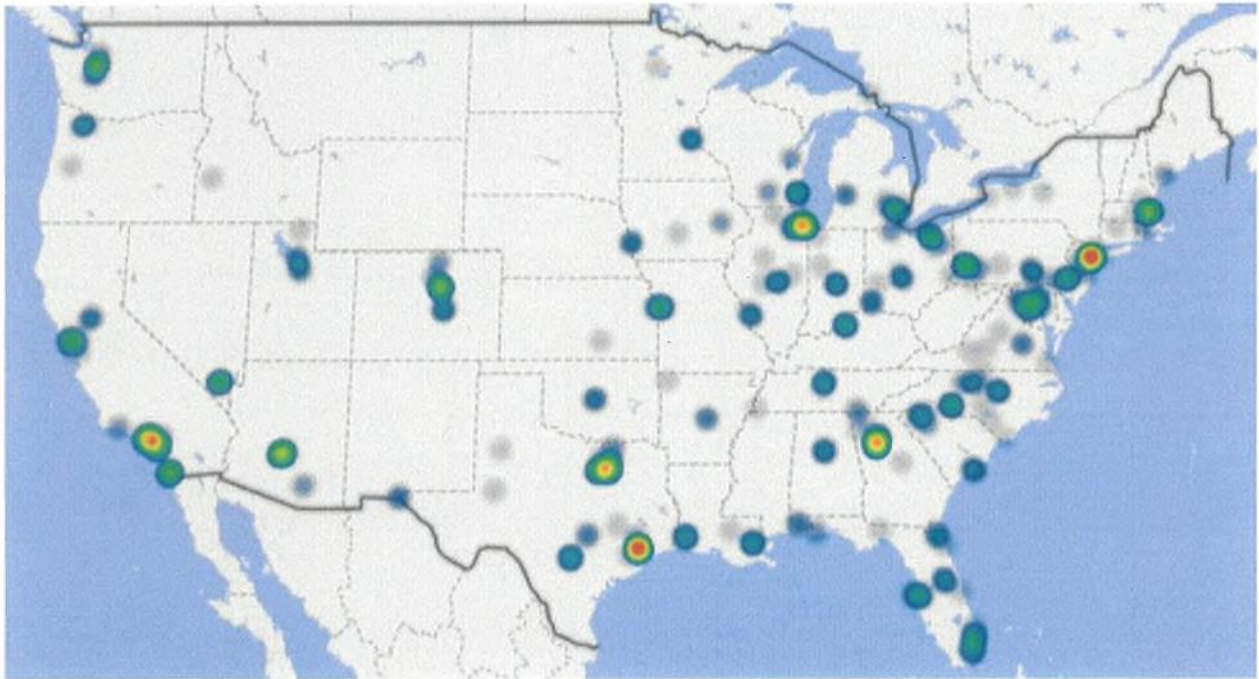


FIGURE 1

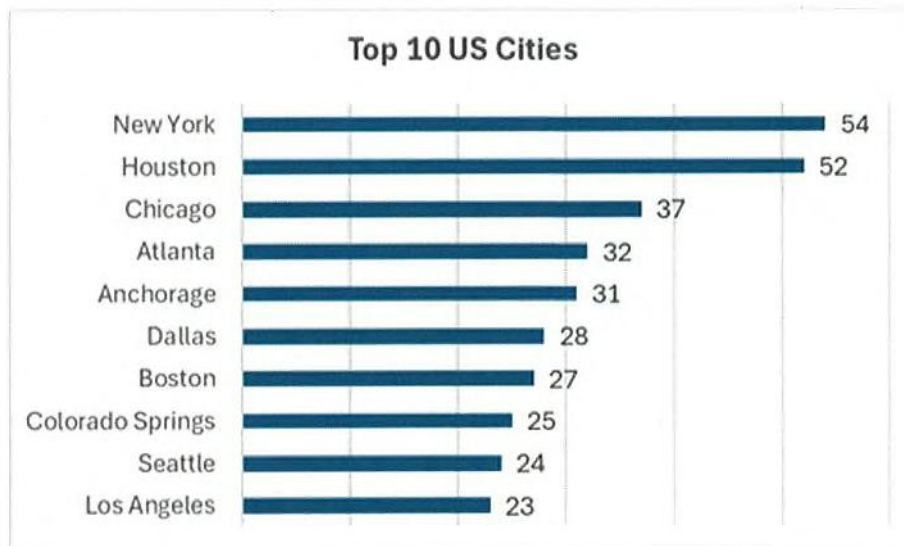


FIGURE 2

FACTUAL BACKGROUND

I. Microsoft's Services and Reputation

29. Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software programs and hardware systems to individuals, businesses and governments. Microsoft is a provider of the Windows® computer operating system, and a variety of other software and services including Microsoft 365®, Office 365®, Outlook®, and Azure®.⁶ Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Azure®. Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint.

30. Health-ISAC is an industry organization that represents approximately 1,000 member organizations both in the United States and globally including hospitals, medical devices manufacturers, pharmaceutical manufacturers, insurers, and health IT organizations. It was established in 2010 to promote public trust by advancing the global health sector's cyber and

⁶ Microsoft 365 and Office 365 are product families of productivity software, collaboration and cloud-based services owned by Microsoft. Microsoft 365 and Office 365 include Microsoft Office, which is a bundle of productivity applications that contains, among other things: a word processor (Word), a spreadsheet program (Excel), a presentation program (PowerPoint), and an email client (Outlook). Microsoft Azure, or just Azure, is the cloud computing platform developed by Microsoft. It offers management, access and development of applications and services to individuals, companies, and governments through its global infrastructure.

physical security protection and resilience as well as enabling the ability to prepare for and respond to cyber and physical threats and vulnerabilities. Health-ISAC's activities include sharing timely, actionable and relevant information with its members, including threat intelligence, involving indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors.

31. Phishing attacks continue to be a major cybersecurity concern for Health-ISAC members and the broader health sector, with significant financial and operational consequences. Phishing schemes are a dominant attack vector in the healthcare sector, and they are involved in a significant percentage of cyberattacks. According to the Health Industry Cybersecurity Practices (HICP) guidelines, phishing simulations conducted in healthcare organizations often reveal click rates between 10% and 30% for employees who fall for phishing emails during tests. HICP noted that healthcare employees are particularly vulnerable to phishing due to the high volume of emails they receive daily and the urgency often associated with their work. This makes them more likely to click on malicious links or attachments. The average downtime for a healthcare company successfully attacked by a cybercriminal is 19 days—during which time patient care can be severely impacted through canceled surgeries, diverted ambulances, and compromised medical records. The average cost of ransomware in the healthcare sector is staggering, reflecting both the financial and operational toll these attacks impose, for example, an attack that involves a ransom demand, can cost approximately \$ 4 million dollars.

II. The RaccoonO365 Defendants

32. RaccoonO365 Defendants are cybercriminals that manufacture and sell RaccoonO365-branded phishing kits and also provide PhaaS to other cybercriminals, who then launch phishing attacks against a multitude of organizations across various industries. RaccoonO365 Defendants first emerged in July 2024. Defendants' use of Microsoft's O365 mark

and other Microsoft trademarks identified above in connection with their products and branding is false, deceptive and unauthorized.

33. The phishing operation is carried out by Defendants Joshua Ogundipe and John Does 1-4. Microsoft was able to identify Ogundipe by using account information from his Microsoft accounts, developmental paths and tooling associated with these accounts and combining this information with open-source intelligence.

III. RaccoonO365's Cybercrime Modus Operandi

34. Much like how companies develop and sell all-in-one do-it-yourself kits to normal customers for personal projects, RaccoonO365 Defendants develop phishing kits for cybercriminals to purchase and use for their cybercrime operations. These cybercriminals become part of the RaccoonO365 Defendants' operation when they, in turn, deploy the RaccoonO365-branded phishing kits to conduct AiTM activities⁷ by positioning themselves between communications directed to and from Microsoft customers. **Figure 3** depicts how cybercriminals become RaccoonO365 Defendants as they collaborate to engage in phishing attacks against a victim using the AiTM model.

⁷ The RaccoonO365-branded phishing kit allows cyber criminals to infiltrate the systems of Microsoft customers undetected and collect the usernames and passwords of the users of the infiltrated network. This is known as AiTM, which is a form of cyberattack where the malicious actor intercepts communications between two parties without their knowledge. It is particularly common for AiTM attacks to leverage PhaaS platforms given the high volume of phishing emails that these phishing kits make possible. This enables these criminals to then enter the system using these purloined credentials and remain undetected. Microsoft has identified AiTM attacks as one of the Top 5 PhaaS models by volume. 2024 MDDR at 34-35.

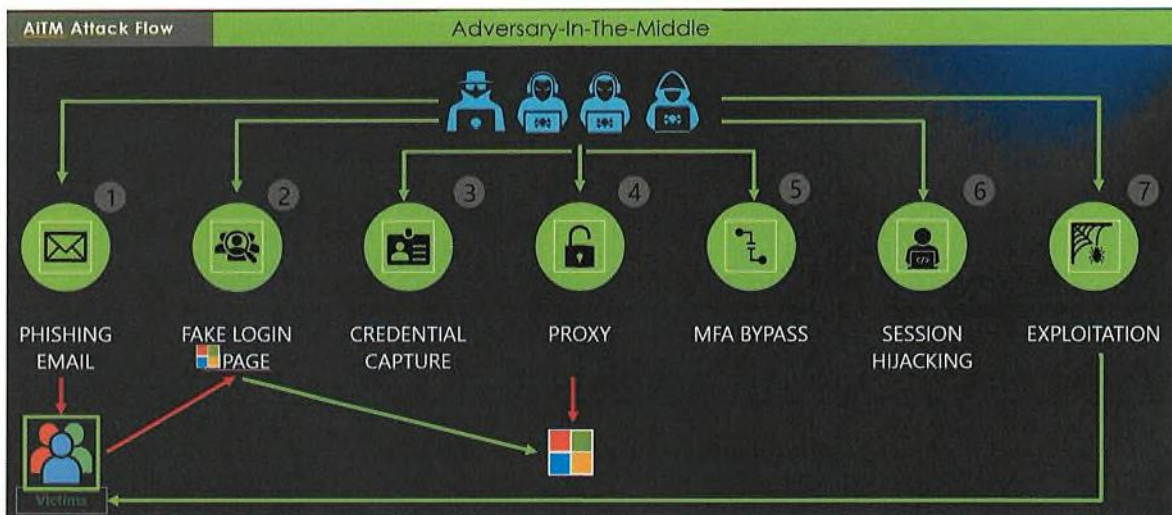


FIGURE 3⁸

35. Phishing is the fraudulent practice of sending emails or other messages purporting to be from legitimate senders to induce recipients to reveal personal information, such as passwords or other credentials. It is a form of social engineering and a scam where the recipient-victim is convinced to interact with the correspondence (referred to as the “lure”). RaccoonO365 Defendants develop and sell RaccoonO365-branded phishing kits that are advertised and promoted as being able to circumvent the security features of Microsoft products, use Microsoft logos, and mimic the appearance of authentic communications to deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. The RaccoonO365 Defendants

⁸ As described in greater detail herein (*see infra* ¶¶ 43-58), an AiTM attack flow follows the following steps:

1. **Phishing Email:** Attacker sends a phishing email to the victim.
2. **Fake Login Page:** Victim clicks the link and is directed to a fake login page.
3. **Credential Capture:** Victim enters credentials on the fake page, which are captured by the attacker.
4. **Proxy to Real Login:** Fake login page proxies credentials to the real login page.
5. **MFA Bypass:** Victim completes MFA, and the session cookie is captured by the attacker.
6. **Session Hijacking:** Attacker uses the session cookie to access the victim’s account.
7. **Exploitation:** Attacker performs actions within the victim’s account.

do not and cannot frontally target Microsoft's security features. Rather, Defendants avoid Microsoft's security features when a phishing recipient clicks on a weaponized link and ushers the attacker into the victim's system right through the front door negating the ability of Microsoft security to repel the attack. The RaccoonO365 Defendants operate similarly to the FAKE ONNX cybercriminal group that was permanently enjoined by the Eastern District of Virginia in November 2024.

36. Like the Fake ONNX cybercriminals, RaccoonO365 Defendants' phishing kits are specifically developed to target Microsoft 365 and Azure users and include two-factor (2FA) authentication⁹ bypass features that allow the attacker to steal system passwords, tokens and Microsoft Authenticator recognition data.¹⁰ These malicious phishing kits support credentials theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud. RaccoonO365 Defendants are able to execute these end-user terminal attacks more readily when they are able to access a victim's Microsoft 365, Office 365, or Azure cloud platform, which serves as gateway to other computer applications, and where these applications are connected by a global Microsoft network infrastructure. These features are the "selling points" of the phishing kits, and RaccoonO365 Defendants advertise the kits' abilities to target Microsoft customers.

37. Once a kit is purchased, cybercriminals can conduct their own phishing attacks using the templates provided in the phishing kits and using domains that the downstream

⁹ Multi-factor authentication (MFA) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism. Two-factor (2FA) authentication is a form of MFA. 2FA relies on a user providing a password as the first factor and a second, different factor (usually either a security token or a biometric factor), such as a fingerprint or facial scan.

¹⁰ Microsoft Authenticator is an application that helps users sign into accounts without using a password, but instead uses a fingerprint, face recognition, or a PIN.

cybercriminal purchases and connects to the overall technical infrastructure. By connecting purchased domains to the infrastructure that is overseen and administered by the RaccoonO365 Defendants, the phishing operation is able to grow and scale and expand its reach. The RaccoonO365 Defendants have built a technical infrastructure of hundreds of website domains that are connected once they have registered the domain. These website domains are identified in **Appendix A** to the Complaint. This action seeks to take down this technical infrastructure, render RaccoonO365 Defendants incapable of continuing their attacks and to transfer ownership and control of these domains to Microsoft. Over the last 15 years, courts have frequently enjoined cybercriminals from attacking Microsoft and its customers, granting the relief Microsoft seeks against the RaccoonO365 Defendants herein.¹¹

38. RaccoonO365 Defendants illegally use Microsoft systems and programs, such as Outlook, Azure, and Microsoft 365 to further enhance the perceived legitimacy of the attack. In doing so, RaccoonO365 Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated, and the trust Microsoft has built with its customers.

a. Development and Sale of RaccoonO365-Branded Phishing Kits

¹¹ See, e.g., *See Microsoft and LF Projects v. Abanoub Nady and John Does 1-4*, 1:24-cv-2013-RDA (E.D. Va. Nov. 13, 2024); *Microsoft and NGO-ISAC v. John Does 1-2*, Case No. 1:24-cv-02719-RC (D.D.C. Sep. 24, 2024), (Contreras, J.); *Microsoft Corporation v. Tu et al.*, Case No. 23-cv-10685 (S.D.N.Y. Dec. 13, 2023) (Engelmayer, J.); *Microsoft, Fortra, and Health ISAC v. John Does 1-16* Case No. 23-cv-2447 (E.D.N.Y. 2023); *Microsoft, FS-ISAC, Health-ISAC v. Denis Malikov and John Does 1-4*, Case No. 1:22-cv-1328-MHC (N.D. Ga. 2022); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Sophos v. John Does 1-2*, Case No. 1:20-cv-00502 (E.D. Va. 2020); *Microsoft v. John Does 1-2*, Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.); *DXC Technology Company v. John Does 1-2*, Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.); *Microsoft and FS-ISAC v. John Does 1-2*, Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.).

39. Much like how an e-commerce business sells its products in online stores for consumers to purchase, RaccoonO365 Defendants sell their RaccoonO365-branded online.

40. The phishing kits are promoted almost exclusively through Telegram Messenger, a cloud-based, cross-platform, instant messaging service. Several Telegram accounts have been established to facilitate communication between cybercriminals and RaccoonO365 Defendants. There are over 800 members in the Telegram channel, each representing a potential or actual purchaser of the RaccoonO365 kit. **See Figure 4.**

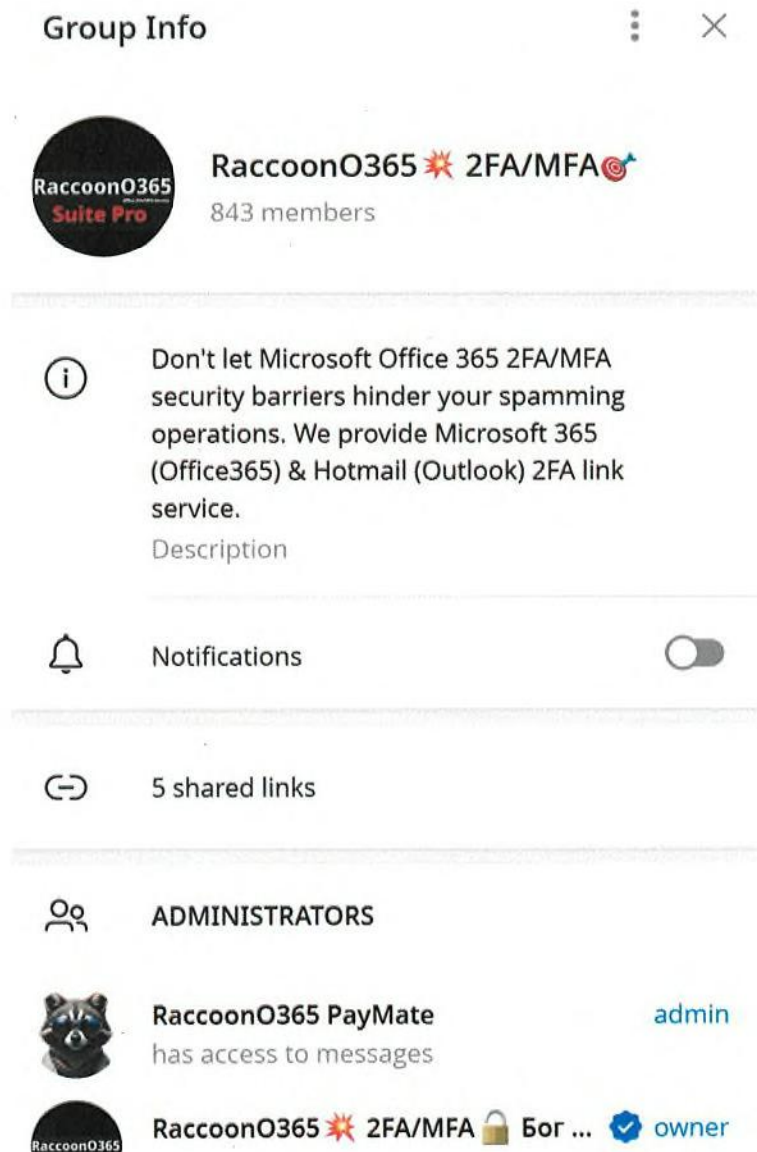


FIGURE 4

41. A successful phishing attack relies on deceiving the victim that the email communication received or a website they are directed to is authentic. To perpetrate this deception, the communication they receive appears to be from familiar contacts or organizations. Victims are directed to click on a link in the malicious email. The phishing websites connected with the link may appear authentic to a victim by using a company name, a well-known product, or some administrative service. Upon closer inspection, the domain name is actually incorrect. For example, if the authentic domain name is www.microsoft.com, a phishing domain may appear to be www.microsft.com or www.mlcrosoft.com, where a letter is missing (missing the “o” in “soft”) or a number is in place of a letter (using “l” instead of “i”). As a result, the phishing domain may easily be misperceived as the authentic domain. When a phishing victim is deceived to visit a website and enter her credentials, RaccoonO365 Defendants lie in wait to collect those credentials to subsequently access the account to further their cybercrime.

42. RaccoonO365 Defendants, including Joshua Ogundipe, design and develop the RaccoonO365-branded phishing kits with features to facilitate the deception. For example, the RaccoonO365 Defendants advertise the “Postman Mass Mailer” and “Links Credential Capture” kits. Postman Mass Mailer is a tool advertised as being able to bypass Microsoft security measures against mass/bulk emailing¹² and deliver phishing emails directly to victims’ inboxes. The Postman Mass Mailer enables users to configure email lists, attachments, subjects, and message

¹² Microsoft implements restrictions that cap the number of emails that can be sent per day. This restriction prevents a user of a Microsoft account from being able to send thousands or tens of thousands of emails per day. Emailing at such a high frequency is often indicative of spam, phishing, or other cyber criminal activity. RaccoonO365 Defendants claim their products bypass this cap. They do not, as Microsoft security features were able to quarantine/embargo the emails that were sent in excess of this cap.

formats. Postman Mass Mailer claims that it allows a customer to input up to 9,000 email addresses at one time. Despite RaccoonO365 Defendants' claims, Microsoft security features have been able to successfully quarantine emails in excess of the cap. Postman Mass Mailer can also be used to automate the email sending process. For a cybercriminal involved in a phishing campaign the advertised ability to send an unrestricted number of emails per day (particularly if the cybercriminal can leverage an automated process) means that there is a higher likelihood of a successful phish or infiltration.

43. The Links Credential Capture is a subscription-based service leveraging an adversary-in-the-middle (AiTM) to intercept the transmission of a victim's two-factor authentication (2FA) code and grab and steal the victim's credentials. This technique presents a Microsoft-themed authentication page to the victim, tricking them into believing that they are entering their Microsoft credentials for a legitimate Microsoft login page.

b. DCU Purchases RaccoonO365 Products

44. Between March and August 2025, Microsoft anonymously purchased four separate phishing kits from RaccoonO365 Defendants. In March 2025, DCU conducted a test buy, where a DCU investigator anonymously purchased the RaccoonO365-branded "Postman Mass Mailer" phishing kit using cryptocurrency. In April, June, and August 2025, DCU conducted three separate test buys of the RaccoonO365-branded Links Credential Capture kit.¹³ Together, these test buys allowed DCU investigators to observe first-hand how RaccoonO365 Defendants operate their telegram store, the information a purchaser is provided, and the instructions given by RaccoonO365 Defendants to connect the domains into the technical infrastructure. Additionally,

¹³ Microsoft purchased a year-long subscription to Postman Mass Mailer. Because the Links Credential Capture kit's subscription is shorter in duration, Microsoft conducted multiple test purchases to observe whether and how RaccoonO365 Defendants updated this kit.

the test buys allowed DCU to gain insight regarding the cryptocurrency wallets used by RaccoonO365 Defendants, including identification of new cryptocurrency wallets.¹⁴

45. As part of this test buy, the DCU investigator began communicating with RaccoonO365 Defendants on Telegram and expressed interest in purchasing both the Links and Postman Mailer offering. *See Figures 5 and 6.* After he expressed interest, the DCU investigator received payment information and successfully purchased a phishing kit. Once he purchased the phishing kit, RaccoonO365 Defendants provided the DCU investigator with instructions on how to connect his pre-purchased domains into the technical infrastructure. Once connected, DCU was able to collect telemetry which has been used to identify key attributes of the RaccoonO365 Defendants' phishing operation.

¹⁴ Through DCU's investigation regarding the cryptocurrency wallets, it has determined that RaccoonO365 has sold approximately \$100,000 worth of phishing kit subscriptions in less than a year's time. This is significant for two reasons. First, DCU has been able to determine that RaccoonO365 has sold nearly 200,000 subscriptions, which demonstrates the growth of the RaccoonO365 Defendants' criminal organization. Second, when purchasing a subscription, the phishing kit is not limited to a single use—rather the cybercriminal can use the kit repeatedly during the subscription period. This means that the existence of 200,000 subscriptions means potentially millions of opportunities to phish and to escalate to other cybercrimes. This is what makes these kits so dangerous: it is low cost, but a highly effective method, and a cybercriminal has all the tools to cause millions in damages simply by spending a few hundred dollars on the subscription for the phishing kit.

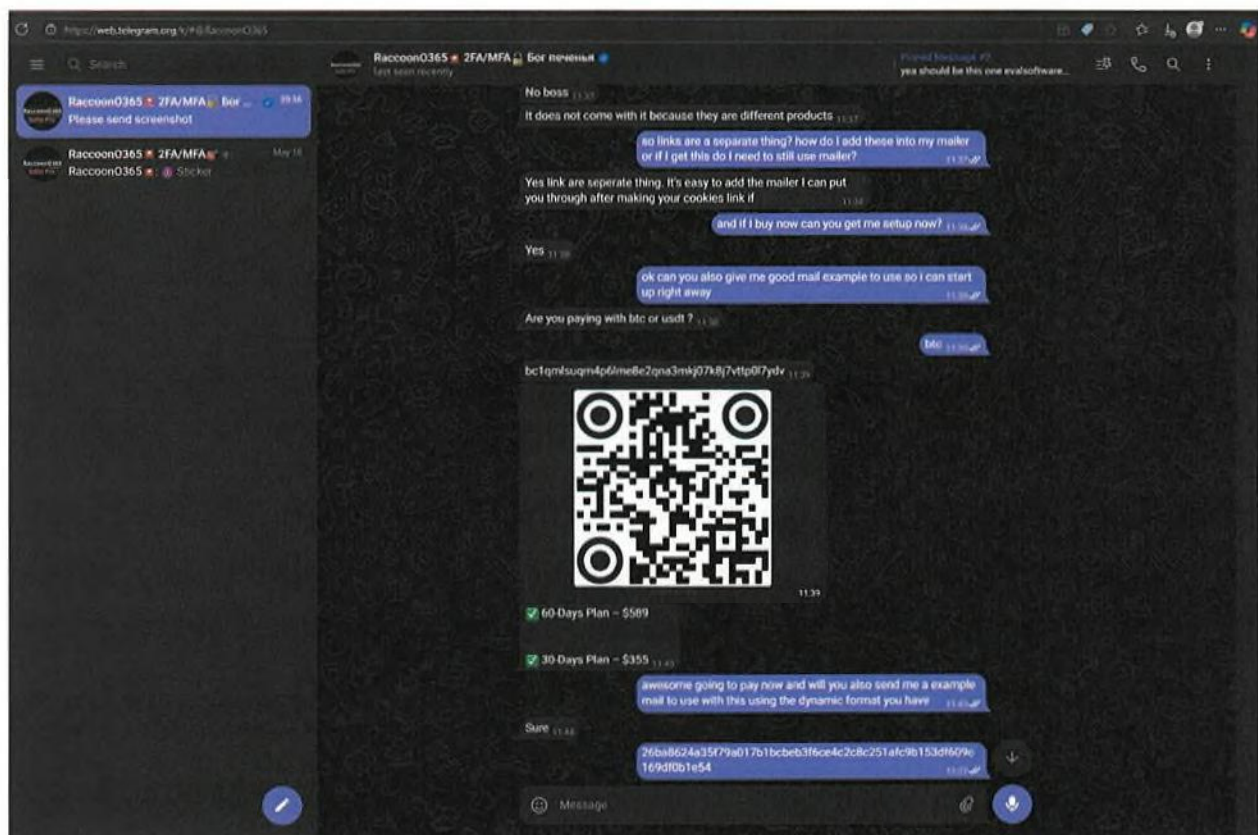


FIGURE 5 – Links Credential Capture Test Buy (Communication with Raccoon0365)

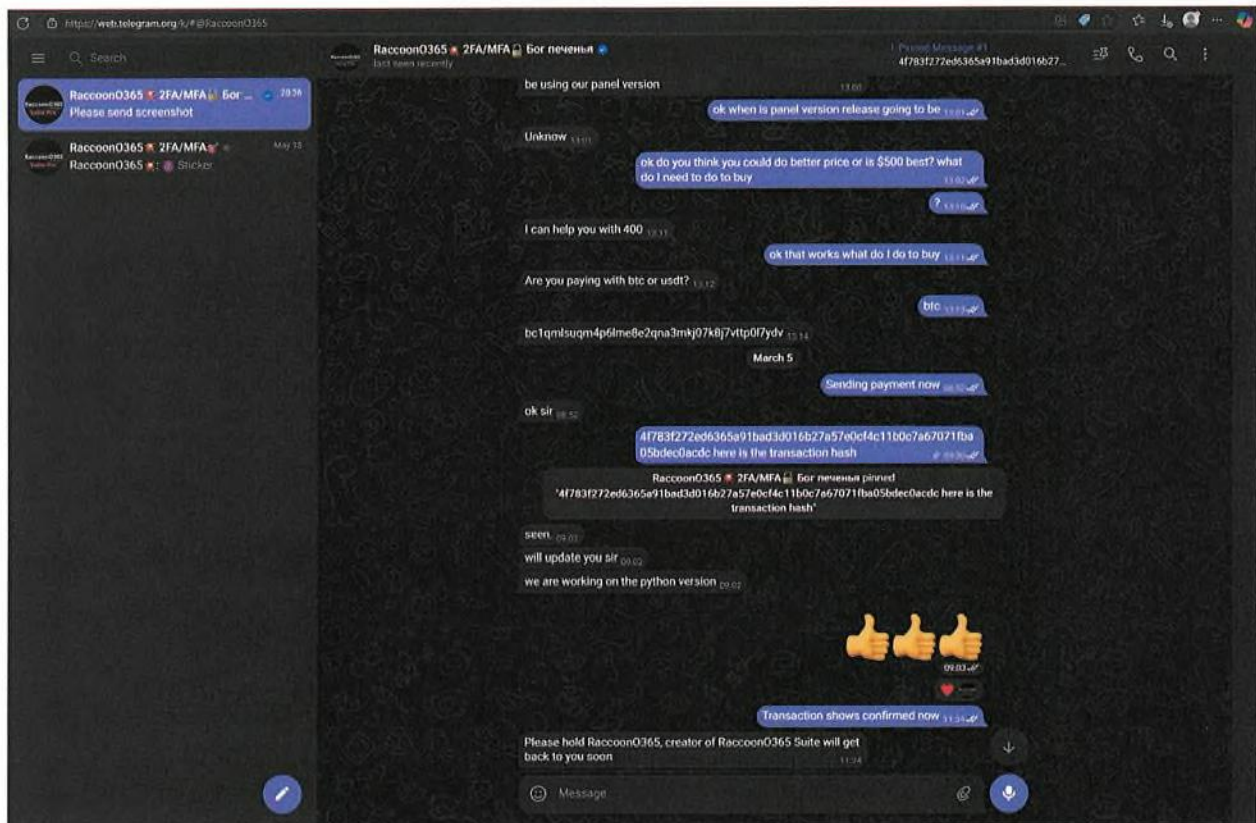


FIGURE 6 – Postman Mailer Test Buy (Communication with Raccoon0365)

46. In addition to Raccoon0365 Defendants purposefully selling their malicious products for use by cybercriminals, they take steps to ensure their products' repeated use. Raccoon0365 Defendants offer various subscription plans at different pricing tiers including "Standard," "Pro," or "Pro Extended" options. See **Figure 7**. By adopting a subscription model, Raccoon0365 encourages repeat, long-term use of the phishing kits. The Raccoon0365 Defendants accept payment via cryptocurrency, specifically via Bitcoin and USDT (a cryptocurrency that is tied to the United States Dollar). Additionally, as shown in **Figure 8**, Raccoon0365 Defendants also offer custom licensing and a support feature. Plaintiffs are informed, believe, and thereupon allege that the "custom licensing" feature, which would allow for the purchase of a kit that allows for more personalization would be attractive to more

sophisticated cybercriminals who may be looking for a customized phishing kit beyond the basic offering.

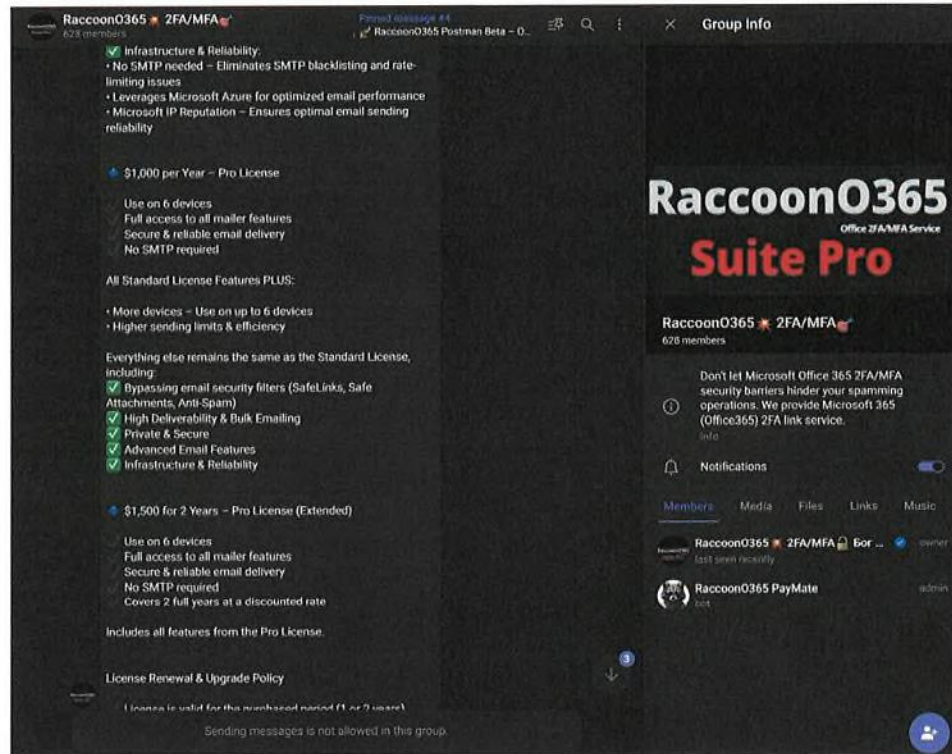


FIGURE 7

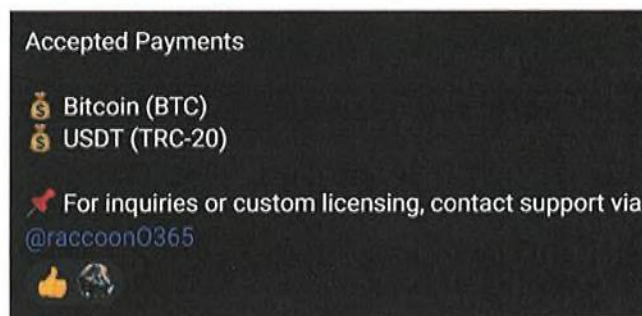


FIGURE 8

c. RaccoonO365 Advertise Future AI-Powered Offerings

47. RaccoonO365 Defendants have also previewed RaccoonO365 AI MailCheck, an AI-powered tool that is still in development and has not been released yet. See **Figure 9** and **Figure 10**. Microsoft has not been able to test this offering, but based on the description provided

by RaccoonO365, Plaintiffs are informed and believe, and on that basis allege, that AI Mail Check will deploy AI to verify and optimize phishing targets. 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.

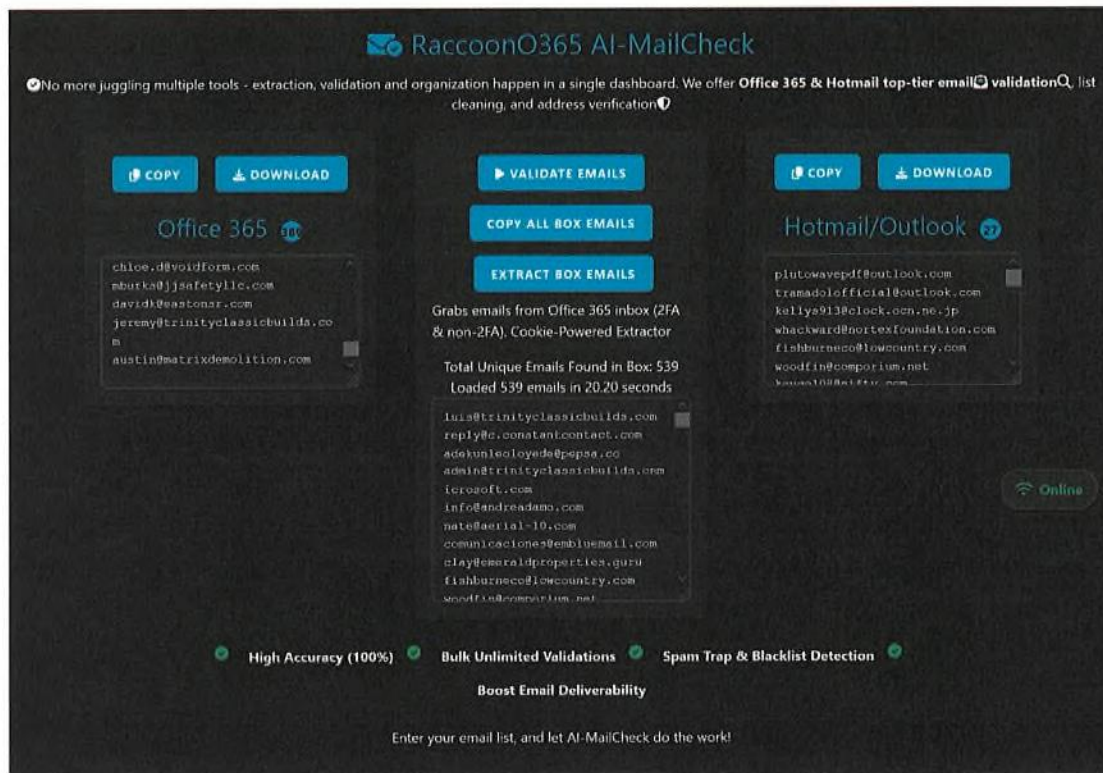


FIGURE 9 – Screenshot of RaccoonO365’s Advertisement of Future AI-Powered Kit

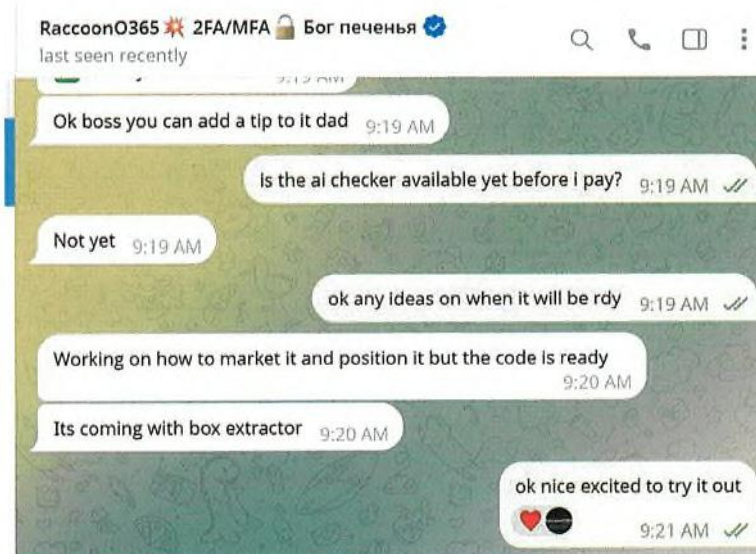


FIGURE 10 – DCU Investigator Communication with RaccoonO365 Defendants Regarding AI-Powered Tool

IV. RaccoonO365 Defendants' Attack Methodology

a. Activation of RaccoonO365-Branded Phishing Kits and Malicious Domains

48. Once a cybercriminal purchases the RaccoonO365-branded phishing kit it must follow several steps¹⁵ to activate the phishing kit and incorporate a phishing domain into the operation controlled by RaccoonO365 Defendants: (i) cybercriminals must purchase domains to be used for the phishing operation and (ii) the cybercriminals' phishing domains must be connected to the phishing operation, which then becomes part of the entire technical infrastructure controlled by RaccoonO365 Defendants. This process for the "Links Credential Capture" tool is described in **Figure 11**.

¹⁵ Cybercriminal customers are John Doe 3-4 once they have purchased a RaccoonO365-branded phishing kit from Defendants.

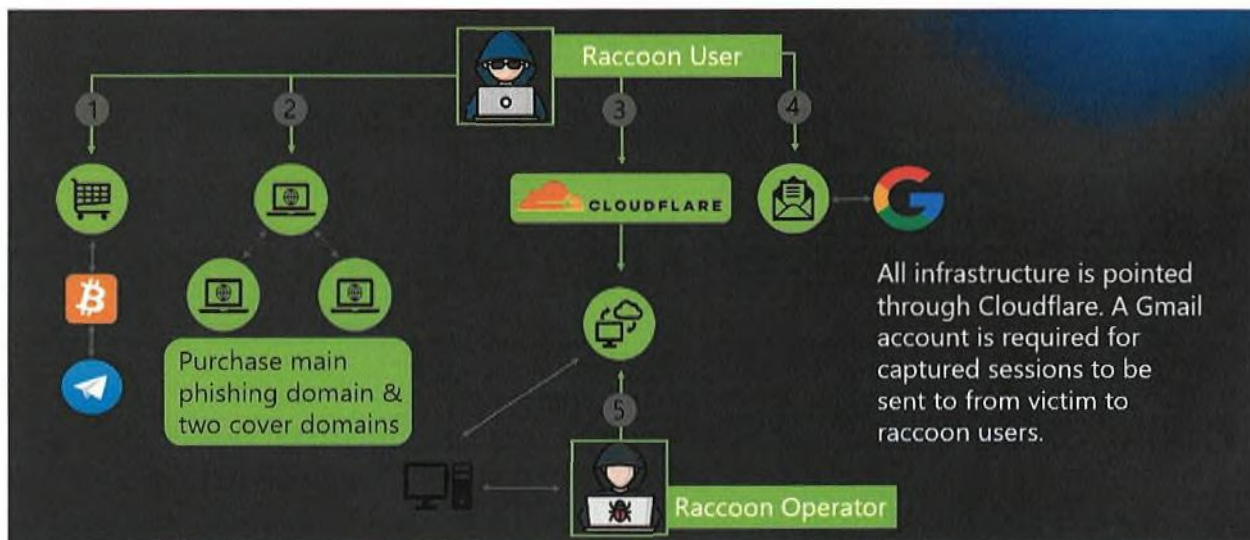


FIGURE 11

b. Purchasing A Domain

49. Users of the RaccoonO365 kit (John Doe Defendants 3 and 4) purchase domains and connect those domains to the infrastructure. Cybercriminals purchase domains from a number of domain registrars (e.g., GoDaddy) who are responsible for the registration of website domain names and assigning Internet Protocol addresses (“IP address”) to those domains.¹⁶ These cybercriminals then “bring their own domain” to the phishing operation controlled by RaccoonO365 Defendants.¹⁷

50. The domains would appear to victims, at a glance, as legitimate—the phished website appears to be branded for specific victims. For example, it would look like a login page for the victim’s employer or a tax service that the victim uses, using fake branding to continue the victim’s interaction with the domains. When the victim logs in, the impersonation of Microsoft’s

¹⁶ An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network. Computers use IP addresses to communicate with each other both over the internet as well as on other networks.

¹⁷ Requiring customers to bring their own domain further obfuscates the criminal activity as tracking of the domains and phishing activity attributable to a particular kit is made more difficult. See 2024 MDDR at p. 46.

brands also adds legitimacy. The domains identified in **Appendix A** appear to be connected to Microsoft and its products, but are subtly misspelled versions of a word, also known as typosquatting. An example of this would be misspelling a name by one letter so that the victim does not catch the difference: using “5” instead of “s” or “nn” instead of “m.” These examples demonstrate RaccoonO365 Defendants’ deliberate effort to lure their victims into a false sense of security and deceive them into providing information that subsequently allows RaccoonO365 Defendants to further their criminal activities.

c. Using Legitimate Infrastructure to Evade Detection and Delay Takedowns

51. The RaccoonO365 customers provide the domains to RaccoonO365 Defendants who direct each of the domains to the Cloudflare infrastructure to further evade detection. Cloudflare is a company that provides a variety of legitimate network services and security features to protect websites from various online cyberthreats. The Cloudflare infrastructure hosts the phishing site and powers the redirection of the cover domains. The RaccoonO365 Defendants misuse Cloudflare services, unbeknownst to Cloudflare, to launder their domains as legitimate. The RaccoonO365 administrators (Ogundipe or John Doe Defendants 1 and 2) request that the user purchase two “cover” domains and a main phishing domain, which are then connected through Defendants’ network. The cover domains are used to protect the main phishing domain from reports and detection.

52. By using Cloudflare’s services, RaccoonO365 Defendants can obscure the real location of their phishing sites by employing and misusing ordinary security measures to make it harder for automated security scanning systems to detect and block their phishing websites. This misuse makes their phishing operations more successful by protecting them from being easily

discovered and shut down. Some of Cloudflare's services include IP proxying¹⁸ and a CAPTCHA¹⁹ service to authenticate that a website link is legitimately clicked by a human.

(a) *IP proxying.* Cloudflare provides an IP proxy feature for account holders, which acts like a middleman to protect the privacy of domain owners. An IP proxy allows legitimate, honest users to have an intermediary in place to protect the privacy of the domain by shielding it from public view. The RaccoonO365 Defendants have exploited this proxy feature to conceal their "home address" (their real IP address). For example, if law enforcement is trying to locate the actual "home address" of RaccoonO365 Defendants' domains, that address is hidden by IP proxying and the only "address" they will obtain is Cloudflare's "business address." This allows RaccoonO365 Defendants to hide their location and prevent their domains from being taken down by law enforcement.

(b) *CAPTCHA.* CAPTCHAs help websites confirm that a user interacting with the website is a human and not a bot. CAPTCHAs are designed to protect normal consumers. In this instance, RaccoonO365 Defendants use a CAPTCHA feature to prevent email security programs that would deploy automated programs (bots) to check if an email has malicious content or links to malicious websites. This allows the RaccoonO365 Defendants to prevent "police robots" (security tools on victim computers) to determine if their domains are engaging in anything illegal (like functioning as a phishing website). Here, RaccoonO365 Defendants use CAPTCHA to block security bots and prevent them from checking a website link in an email address to see if

¹⁸ IP proxying is where a proxy server acts as an intermediary between the user and the web server. Proxy servers use a different IP address on behalf of the user, concealing the user's real address from web servers.

¹⁹ CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) has been widely used as a means of protection against bots. It is a type of challenge – response test used to determine whether the user trying to access a website is human in order to deter bot attacks and spam.

it is malicious. By eliminating the probability of being detected, RaccoonO365 Defendants are better able to deliver phishing emails to their victims without interference.

d. Connecting to the RaccoonO365 Defendants' Phishing Operation

53. Once the cybercriminals complete the domain's registration of the "cover" domain, the next step is to connect the purchased domains with the existing RaccoonO365 infrastructure. The cybercriminals provide their purchased domains to the RaccoonO365 Defendants so that the domains can be pointed to Cloudflare. During the test buys, RaccoonO365 Defendants provided the investigator with a Cloudflare nameserver that the investigator could use to update their Cloudflare account to point the domains toward the existing infrastructure. See **Figure 12**. At this point, all domains are pointed towards the Cloudflare Domain Name System²⁰ that is owned by the RaccoonO365 Defendants. Because Defendant Ogundipe owns this Cloudflare infrastructure, he validates the "cover" domain locally on his machine to ensure full functionality.

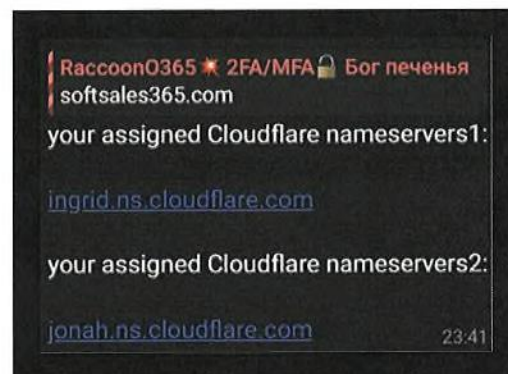


FIGURE 12

e. RaccoonO365 Defendants' Attack Chain

²⁰ Domain Name System, or "DNS" is often referred to as the "phonebook of the Internet," it translates the domain into the numerical IP address that is used to connect computers to websites on the Internet.

54. Once the technical infrastructure is established, the next phase is the phishing attack deployed by RaccoonO365 Defendants. A phishing email is sent to a victim that prompts the victim to click on a link connected to the malicious domain.

55. These phishing emails use, without authorization, Microsoft's logos and format to lull the victim into believing the website is legitimate. Once a victim clicks on the link, they are directed to an ostensibly legitimate Microsoft login page that asks for their credentials—this is the “cover” domain. The cover domain conducts a check (via Cloudflare services) to counteract any security tools that the victim has employed, and a line of code is run to prompt the victim to enable features (such as cookies) to ensure RaccoonO365 Defendants have access to as much victim information as possible. After the security check, the URL that the victim clicked on is redirected to the main phishing page. A line of code is also run at this point to ensure that that standard security features are turned off so that RaccoonO365 can conduct its cybercriminal activity without detection. Once all the security measures have been disabled or circumvented, the victim is presented with a login page with Microsoft branding. When the victim enters their login credentials (their real credentials for their Microsoft account), they will be directed to verify their password and complete the 2FA process. This process is shown in **Figure 13**. At this stage, the RaccoonO365 Defendants have completed the goal of the phishing—credential theft—by using the AiTM methodology described above.

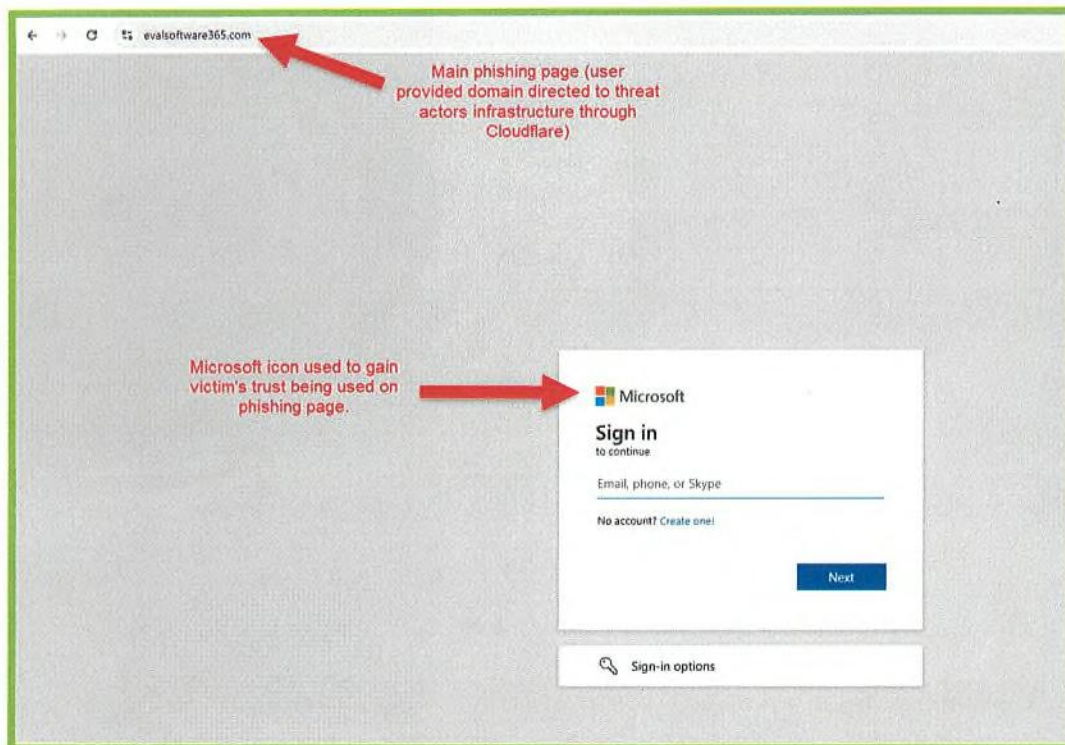




Figure 13

56. Once the victim enters their authentication details, receives the 2FA token, and enters the token into RaccoonO365 Defendants' fraudulent login page, their credentials and 2FA tokens are captured. **Figure 14** is an example of a page designed to capture the 2FA token. **Figures 15** and **16** are examples of RaccoonO365 successfully capturing credentials and the 2FA/MFA token.

The screenshot shows a Microsoft login interface. At the top is the Microsoft logo. Below it is a blurred grey bar. The main heading is "Enter code". A tip icon (a square with "TIP") is followed by the text "Enter the code displayed in the authenticator app on your mobile device". Below this is a text input field with the placeholder text "Code" and a cursor icon. Under the input field is a link that says "More information". At the bottom right are two buttons: a grey "Cancel" button and a blue "Verify" button.







FIGURE 14 – Screenshot of login page designed to capture the 2FA token

 **Sign-in Data Shared!** 🎉 A Microsoft Office 365 user has successfully shared their Microsoft sign-in data with you! 🎉

Note : We have some great news! Please note that the extracted cookies will only expire if the 'Log Out' button is clicked. If you stay signed in without clicking the 'Log Out', the cookies will remain active until they reach their expiration date.

Stay productive with RaccoonO365 2FA/MFA Microsoft Office 365 parasite link. No stress. We're here to help you succeed.

Microsoft Office 365 Credentials:

User: 
User: 
User: 3
Password: 7!
user_id:
Ip: 2a02:
City: 
Region: 
Country: US
Zip: 45368
Timezone: America/New_York
Victim Account sign in page link: login.microsoftonline.com
More IP Details: <https://whatismyipaddress.com/ip/2a02:6ea0:d213:1793::11>
User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:133.0)
Gecko/20100101 Firefox/133.0

RaccoonO365 2FA/MFA tool is capable of obtaining valid Microsoft Office 365 cookies. Experience the extraordinary! This isn't just your average Microsoft Office 365 tool kit – it's a masterpiece meticulously created by RaccoonO365 2FA/MFA Network with passion and precision!

Copyright © 2025 RaccoonO365. All rights reserved.
RaccoonO365 2FA/MFA Cookies Service 2025-04-28 18:40:36

FIGURE 15 – Captured Victim Credential

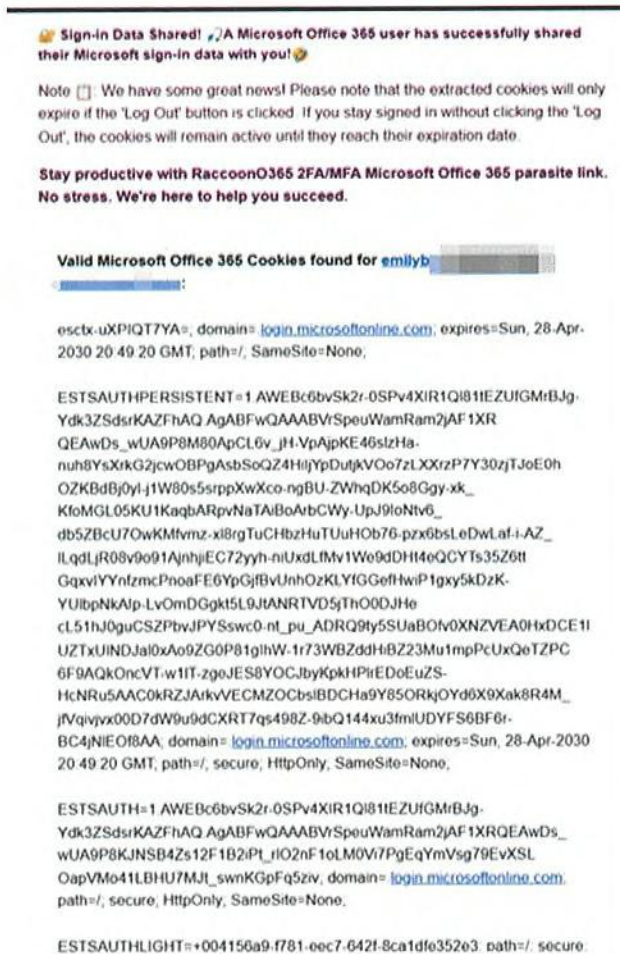


FIGURE 16 – Captured MFA/Cookie Session

57. This verification process convinces the victim that RaccoonO365 Defendants' malicious website is legitimate. RaccoonO365 Defendants subsequently exploit this access to their victim's devices to perpetrate further cybercrime such as ransomware, business email compromise, and financial fraud.

58. The Postman Mailer tool can be used in connection with the Links tool to allow the user/purchaser of the RaccoonO365 kit to scale operations and increase the number of phishing lure emails they can send. The user can utilize this kit to input a large number of email addresses. While this tool is not malicious *per se*, it is advertised in connection with the Links tool to send large volumes of emails into a user's inbox via a single tool using compromised Microsoft 365

accounts using Microsoft Azure infrastructure. When used in connection with Links, RaccoonO365 Defendants advertise that users get more value from their kits because they are able to substantially increase the number of targets they can attack and the frequency at which they attack. In reality, Defendants are not able to exceed the caps, but are able to automate the process, by making it easy for the cybercriminal to add recipients, add an attachment, and update the subject line or message content. Because the Postman Mailer automates the sending process, the threat actor does not have to oversee the process. **Figure 17** depicts the operational flow for Postman Mailer.

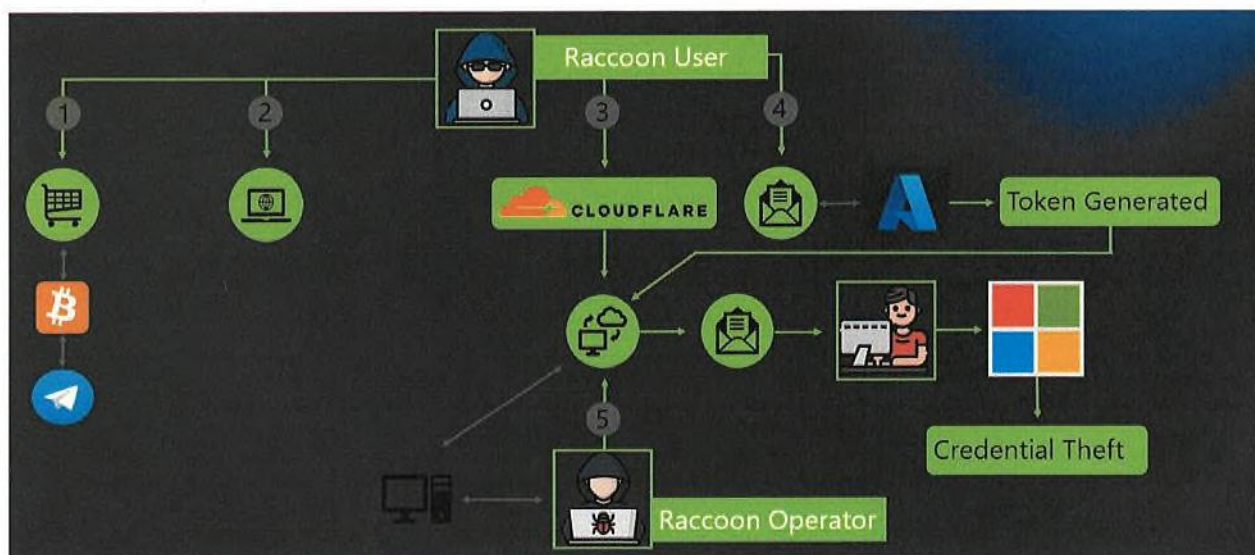


FIGURE 17

V. RaccoonO365 Defendants' Victimology

a. RaccoonO365 Targets Users During Tax Season to Obtain Sensitive Financial Information

59. RaccoonO365 Defendants have targeted victims during tax season and designed phishing emails to look like legitimate communications regarding tax-related documents. During February 2025, RaccoonO365 Defendants were responsible for sending tax-themed phishing emails to over 2,300 organizations, mostly in the United States in the engineering, IT, and

consulting sectors. The emails appeared to be from trusted sources (a result of RaccoonO365 kits allowing Defendants to customize the phishing email to ensure a higher success rate) had no text in the body of the email but contained a PDF attachment that once opened presented a QR code and instructions for the recipient to scan the QR code to access the document. When scanned, the QR code directed the victim to a hyperlink associated with a RaccoonO365 domain: `shareddocumentso365cloudauthstorage[.]com`.²¹

60. In one instance, the RaccoonO365 Defendants sent an email with the subject “Employee Tax Refund Report” that included an attachment labelled “TaxRefundExport.” When the victim opened the pdf file, she was taken to a document instructing her to open and review a purported tax document. The pdf displayed a QR code and encouraged the victim to scan the QR code to begin the review process. As described above, scanning the QR code redirects the victim to a login page controlled by RaccoonO365 Defendants. See **Figure 18** and **Figure 19**.

²¹ Microsoft Threat Intelligence, *Threat Actors Leverage Tax Season to Deploy Tax-Themed Phishing Campaigns*, available at <https://www.microsoft.com/en-us/security/blog/2025/04/03/threat-actors-leverage-tax-season-to-deploy-tax-themed-phishing-campaigns/?msockid=24c40619b2e66c29157512a7b3e56dc4> (Apr. 2013).

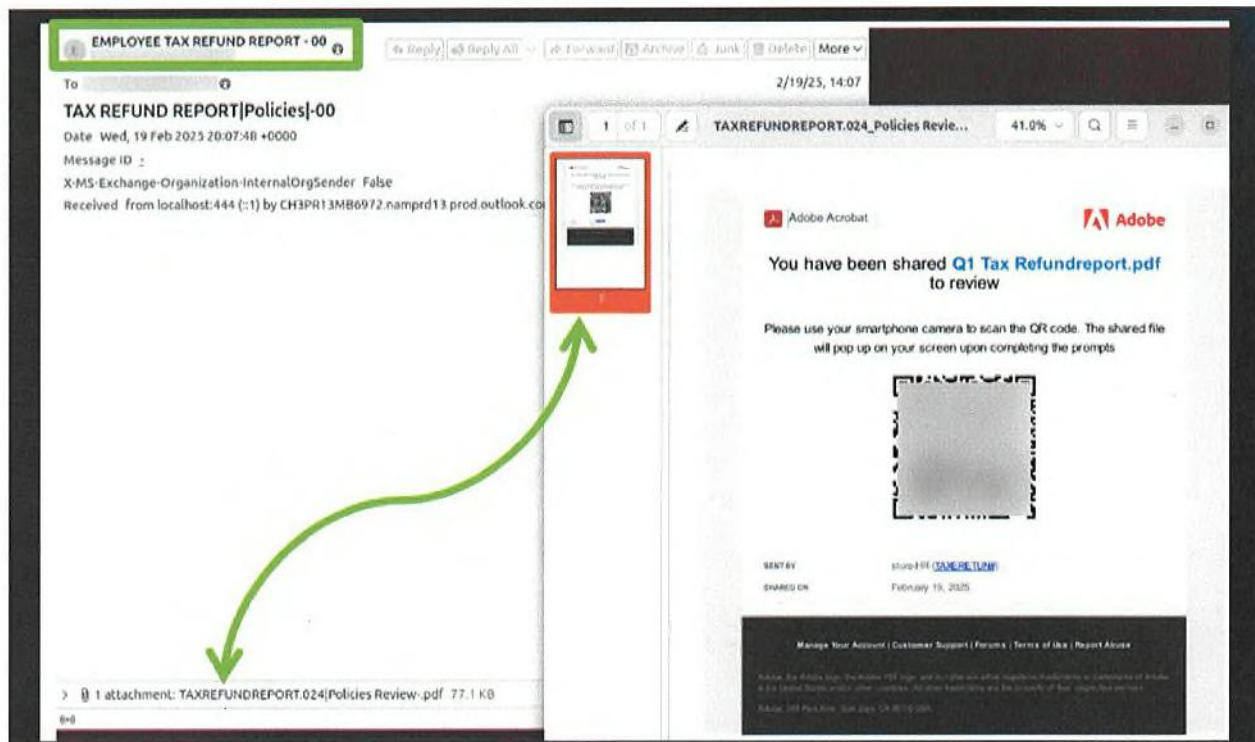


FIGURE 18



FIGURE 19

b. RaccoonO356 Defendants Target the Healthcare Industry

61. RaccoonO365 Defendants have also targeted victims at healthcare companies, luring the victim to open the email and attachment and then interact with the QR code in the attachment. In these instances, the subject line and attachments discuss “incoming payments,” “review and approval,” and “payment confirmation.” *See Figures 20-23.*

Incoming Payment advice-BG_EDG765023485344100192450019_1822_760 (Api*GHfu)



You don't often get email from background@trifid.com. Learn why this is important.

External Email: This is an external email. Please take care when clicking links or opening attachments. When in doubt, contact your IT Department.

FIGURE 20



This is a private share from Api. It will expire on 18/10.

scan the QR Code to Access document on your phone



Attention:

Open your smart phone camera
Scan the QR code on this pdf
Click the pop up yellow redirect link
Review & Sign Document
Click save
Done

FIGURE 21



FIGURE 22

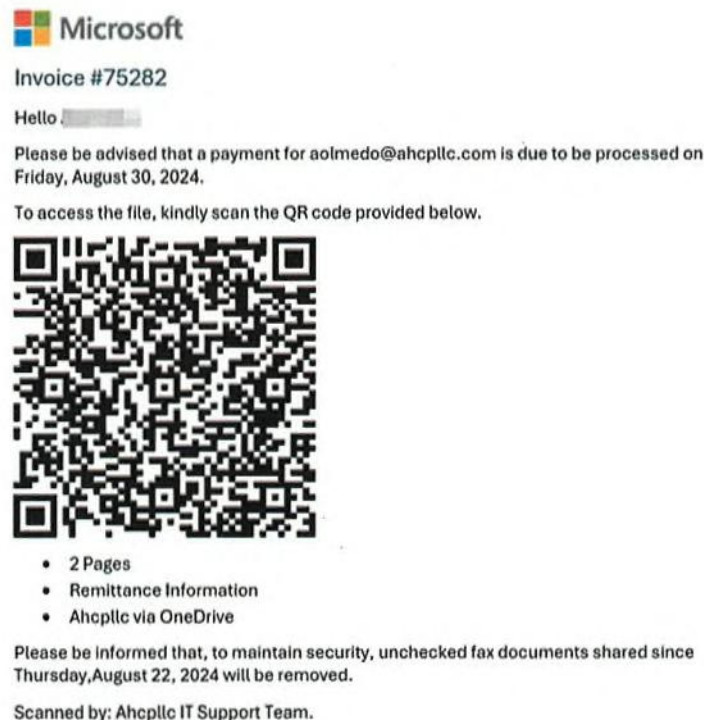


FIGURE 23

62. In recent months, Health-ISAC member organizations have been routinely subject to phishing attacks that are traceable to the RaccoonO365 phishing kits. Health-ISAC has been able to confirm that phishing emails directed at its members have been opened and the recipients interacted with the phishing email and links or documents attached to the phishing email. A successful phish—*i.e.*, the recipient opens the phishing email—is a precursor to other, more

serious cybercrime. When a cybercriminal gains access to computer systems as a result of capturing credentials from a phish, the cybercriminal's next step is to use its control over the system to launch a malware or ransomware attack.

63. For Health-ISAC member organizations such malware or ransomware attacks are devastating and costly. Accordingly, given the end game of cybercriminals who engage in phishing, the fact that RaccoonO365 has been able to successfully phish within the healthcare industry, means it is a question of when they will escalate to malware and ransomware attacks, not if.²²

a. RaccoonO365 Jointly Leverage the Racketeering Enterprise to Commit Cybercrime

64. Defendants Joshua Ogundipe and John Does 1-4 constitute a group of criminals engaged in a common course of conduct, as part of an ongoing organization and functioning as a continuing unit (hereinafter the "Racketeering Enterprise").

65. The Racketeering Enterprise causes significant harm to Microsoft, its customers, Health-ISAC and its member organizations, and the public. The RaccoonO365 Defendants cooperate and collude in the sale, distribution, deployment, or use of the phishing kits, the control of the phishing operation, the importing of domains for use in the phishing operation, the provision of technical support to cybercriminals, the multi-tier subscription of phishing operation services,

²² Fake ONNX Defendants had been marketing and selling their phishing kits for several years before Microsoft successfully took down the infrastructure. During this time, Fake ONNX Defendants escalated conduct and transitioned from phishing campaigns and business email compromise to full-scale control of computer systems and launched malware and ransomware attacks. Here, with RaccoonO365, Microsoft discovered the operation at an earlier stage. Microsoft is in a position to stop RaccoonO365 Defendants *before* they successfully launch ransomware and malware attacks on the public.

circumvention of technical security measures to gain access to victim computers and information, and the unauthorized use and dissemination of Plaintiffs' intellectual property.

66. The relationships among RaccoonO365 Defendants allow them to collectively pursue the criminal purpose of the Racketeering Enterprise. As **Chart 1** below demonstrates, Joshua Ogundipe and John Does 1-4 each have specialized roles in the Racketeering Enterprise, on which the success and furtherance of the Racketeering Enterprise is entirely dependent. Namely, the RaccoonO365 Defendants leverage each other's work to: (i) create, distribute, and operate the phishing technical infrastructure, (ii) sell, distribute, and use RaccoonO365-branded phishing kits, (iii) steal credentials from victims, and (iv) gain access to victim computers to further additional criminal activities like financial fraud, business email compromise, and deploying ransomware. The RaccoonO365 Defendants' ongoing association with one another and reliance on each other's contributions, allows the Racketeering Enterprise to function as a continuing unit and within a lucrative operational structure.

RACCOONO365 DEFENDANTS	FUNCTION
Joshua Ogundipe	Develops the RaccoonO365-branded phishing kit and controls the RaccoonO365 Defendants' criminal phishing organization and the technical infrastructure.
John Doe 1	Controls the RaccoonO365 Defendants' criminal phishing organization and the technical infrastructure.
John Doe 2	Provides technical support for the RaccoonO365 Defendants' criminal phishing organization and the technical infrastructure.
John Does 3-4	Customers of RaccoonO365 kits, who register a new phishing domain, purchase an RaccoonO365-branded phishing kit, and incorporate the new phishing domain into the RaccoonO365 Defendants' criminal phishing organization and the technical infrastructure. Plaintiffs are informed, believe, and thereupon allege that based on the number of users in the RaccoonO365 Telegram channel, there could be hundreds of individuals who have purchased a RaccoonO365 kit.

Chart 1. RaccoonO365 Defendants' Division of Labor.

67. Plaintiffs are informed, believe, and thereupon allege that Defendants Ogundipe and John Does 1-2, the creators, sellers, and distributors of the RaccoonO365-branded phishing kits, work together with the cybercriminals, who purchase and use the phishing kits, and leverage the technical infrastructure to engage in phishing attacks.

68. Plaintiffs are informed, believe, and thereupon allege that Defendants John Does 3-4 are cybercriminals who register new domains for the purpose of using them in the phishing operation and incorporating the domains into the RaccoonO365 Defendants' criminal phishing organization and the technical infrastructure. This allows the prolific expansion of the RaccoonO365 Defendants' phishing operation, which leads to the increase of downstream criminal activities including financial fraud, business email compromise, and ransomware attacks. This level of continuous and coordinated activity allows for the success of the operation.

69. The Racketeering Enterprise has continuously and effectively carried out its purpose of developing and operating a global technical infrastructure that facilitates phishing attacks that lead to credentials theft, allowing for the unauthorized access to a victim's email account, or potentially, a victim's Microsoft 365 or Azure platform, thereby granting access to a broader range of program applications in a victim's computer.

70. The relationship between the RaccoonO365 Defendants is proven by: (i) development and repeated sale of the RaccoonO365-branded phishing kit, (ii) the subsequent development and operation of the technical infrastructure to proliferate the phishing operation and leveraging of the infrastructure to facilitate further criminal activities, and (iii) RaccoonO365 Defendants' respective and interrelated roles in the sale, operation of, and profiting from the

RaccoonO365-branded phishing kits in furtherance of RaccoonO365 Defendants' common financial interests.

71. Plaintiffs are informed, believe, and thereupon allege that RaccoonO365 Defendants have conspired to, and have, knowingly with intent to defraud, facilitated phishing attacks against victims to steal credentials and gain unauthorized access to a victim's computer and have impersonated Microsoft and lured victims to divulge login credentials to non-public personal accounts. These acts are continuing and will continue unless and until this Court grants Plaintiff's request for a temporary restraining order.

72. As set forth in detail herein, RaccoonO365 Defendants have used the technical infrastructure to steal, intercept, and obtain credentials and other device access information from countless individuals, including 2FA authentication tokens.

73. Plaintiffs are informed, believe, and thereupon allege that RaccoonO365 Defendants have also conspired to, and have knowingly and with intent to defraud, possessed and do possess, thousands of unauthorized access devices (e.g., credentials, 2FA codes, and cookies) fraudulently obtained as described herein.

74. Each of the foregoing illegal acts perpetrated by the RaccoonO365 Defendants were conducted using interstate ACH and/or interstate and/or foreign wires as described herein and therefore affected interstate and/or foreign commerce.

VI. Harm to Microsoft and Microsoft's Customers

75. Through research and investigation, Microsoft has determined that RaccoonO365 Defendants used the domains identified in **Appendix A** in their technical infrastructure and have actively and affirmatively targeted Microsoft customers in the United States. The RaccoonO365 Defendants sometimes disguise their technical infrastructure by incorporating into the names of

their technical domains the names and trademarks of some well-known companies and organizations, including Microsoft.

76. For example, as seen in **Appendix A**, RaccoonO365 Defendants have registered website domains that contain Microsoft's brands and trademarks as disguises, including microsoft-securedocuments[.]com, microsoft365docssuite[.]com, and office365clouddrive[.]com. Because these are the webpages that a victim is redirected to when they interact with a phishing email, a domain that contains Microsoft's branding will further trick the victim into believing that the login page is legitimate and that Microsoft has endorsed the email. RaccoonO365 Defendants rely on the Microsoft brand and trademark to perpetrate their phishing and malware attacks by leveraging and misusing the trust Microsoft has obtained from its customers.

77. Microsoft determined that RaccoonO365 Defendants also cause great harm to the company and its customers through the unauthorized access of Microsoft enterprise platforms, which serves as a cloud platform that grants access to a victim's other computer applications and information. When the RaccoonO365 Defendants access the Microsoft enterprise platforms, they move through other computer applications and can facilitate additional criminal activities like ransomware, financial fraud, and business email compromise.

78. RaccoonO365 Defendants irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill. RaccoonO365 Defendants' misuse of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links that they believe are associated with and owned by Microsoft. Because RaccoonO365 Defendants impersonate Microsoft platforms and logins, victims will believe that they are protected. When the victim realizes that they have been attacked, they will believe that Microsoft is responsible for

or complicit in the attack and customers may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

79. Microsoft has invested considerable resources in developing high-quality products and services, including significant resources to combat RaccoonO365 Defendants and other cybersecurity threats. Microsoft spent at least \$250,000 and 750 hours investigating and remediating RaccoonO365 Defendants' activities, including engaging teams across the country. Through the development of flagship products used by millions of customers, Microsoft has thereby cultivated significant customer goodwill and globally recognized trademarks. Trademark registrations for marks infringed by RaccoonO365 Defendants are attached as **Appendix B**.

80. A phishing attack where customers blame Microsoft involves a risk that customers may move from Microsoft's products and services because of the RaccoonO365 Defendants and their activities. For customers who leave, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks. This causes injury to Microsoft.

VII. Harm to Health-ISAC and its Member Organizations

81. Health-ISAC has invested considerable resources in developing high-quality products and services, including significant resources to combat RaccoonO365 Defendants and other cybersecurity threats. Health-ISAC Microsoft spent at least \$12,000 investigating and remediating RaccoonO365 Defendants' activities.

82. Health-ISAC has identified at least 25 healthcare companies, including 9 organizations who are members of Health-ISAC organizations that have been hit by RaccoonO365 phishing kits. Health-ISAC has been able to confirm that phishing emails directed at its members have been opened and the recipients interacted with the phishing email and links or documents

attached to the phishing email. For example, two entities received phishing emails attributable to RaccoonO365, but the organizations successfully blocked delivery of the emails to the recipient. In two other instances, the RaccoonO365 phishing email was delivered and opened by the recipient, who then attempted to click the malicious links contained in the phishing email. The organization successfully blocked access to the RaccoonO365-controlled website. RaccoonO365 phishing emails were delivered and opened by the recipients of five other member organizations. The recipients clicked on the RaccoonO365-controlled links and entered their credentials into the RaccoonO365-controlled website. The Health-ISAC member organizations detected this activity and were able to successfully reset the credentials before further malicious activity could occur.

83. Additionally, Health-ISAC members had internal staff that fell victim to RaccoonO365 phishing emails by providing their username / password credentials on RaccoonO365-controlled websites. Those organizations detected the incidents and responded appropriately by resetting each individual victim employee's credentials.

84. The Health-ISAC members' receipt of RaccoonO365 phishing emails is a precursor to subsequent cybercriminal activity. Once the cybercriminal has successfully intruded into the system (such as when a Health-ISAC member organization's employee interacts with the link contained in the phishing email), it is not a question of if there will be subsequent attacks, it is a question of when.

85. When hospitals are attacked by ransomware, critical IT systems become unavailable and hospital services begin to decline rapidly, causing devastating consequences, including:

- Ambulances forced to divert from hospitals;
- Delays in providing emergency patient services, delays or cancellation of

providing treatments for cancer patients, delays in receiving lab results, delays in scheduling appointments;

- Hospitals forced to cancel elective procedures;
- Electronic Health Record systems being taken offline, which prevent hospitals, doctors, and providers from accessing any portion of the patient's electronic file;
- Malware and ransomware attacks that have crippled IT systems and have led to the breach of sensitive health information; and
- Financial losses, including ransom payments to cybercriminals, legal fees, and regulatory fines.

COUNT I

Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030

(Microsoft; Health-ISAC)

86. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 85 above.

87. RaccoonO365 Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and through the use of stolen credentials, and knowingly caused the transmission of a program, information, code, and commands, resulting in damage to the protected computers, the software residing thereon, of Microsoft, and Health-ISAC.

88. RaccoonO365 Defendants' conduct involved interstate and/or foreign communications.

89. RaccoonO365 Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least \$5,000. Specifically, Microsoft has incurred damage in excess of \$650,000. The same harm has caused Health-ISAC damage in excess of \$12,000.

90. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

91. As a direct result of RaccoonO365 Defendants' actions, Microsoft and Health-ISAC have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

COUNT II

Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962

(Microsoft; Health-ISAC)

92. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 91 above.

93. Beginning in August 2024 and continuing up through the filing of this Complaint, RaccoonO365 Defendants Joshua Ogundipe and John Does 1-2 were and are associated in fact with the Racketeering Enterprise and have conducted its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. At various dates thereafter and continuing through the filing of this Complaint, RaccoonO365 Defendants John Does 3-4 also became associated in fact with the Racketeering Enterprise and have conducted their affairs through a pattern of racketeering activity that affects interstate and foreign commerce.

94. RaccoonO365 Defendants conduct their affairs through a pattern of racketeering activity affecting interstate and foreign commerce involving thousands of predicate acts of fraud including violations of (i) the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

95. RaccoonO365 Defendants manufacture malicious phishing kits and operate a global technical infrastructure that supports credentials theft, information exfiltration, and subsequent end-user terminal attacks including business email compromise, ransomware, and financial fraud.

96. RaccoonO365 Defendants, as members of the Racketeering Enterprise, share the common purpose of developing and operating a malicious technical infrastructure that proliferates phishing attacks through the sale, distribution, deployment, and use of the RaccoonO365-branded phishing kits.

97. RaccoonO365 Defendants have knowingly and with intent to defraud, possessed, and do possess, thousands of unauthorized access devices, including specifically credentials, 2FA tokens, and cookies, fraudulently obtained as described above, in violation of 18 U.S.C. § 1029.

98. RaccoonO365 Defendants have knowingly and with intent to proliferate phishing kits used to steal, intercept and obtain credential information through access devices (including credentials, 2FA tokens, and cookies) defrauded Microsoft customers by sending emails impersonating Microsoft and its customers in order to lure victims to unknowingly providing login credentials to RaccoonO365 Defendants, in violation of 18 U.S.C. § 1343. RaccoonO365 Defendants have captured login credentials from victims within the healthcare industry with the intent to defraud, itself a predicate offense for a RICO action.

99. Plaintiffs have been and continue to be directly injured by RaccoonO365 Defendants' conduct. But for the alleged pattern of racketeering activity, Plaintiffs would not have incurred harm.

100. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT III

Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. § 1962(d)

(Microsoft; Health-ISAC)

101. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 100 above.

102. Beginning in or before August 2024 and continuing up through the filing of this Complaint, RaccoonO365 Defendants, Joshua Ogundipe and John Does 1-4, conspired to associate in fact with the Racketeering Enterprise and conduct its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. RaccoonO365 Defendants further conspired to engage in an unlawful pattern of racketeering activity involving thousands of predicate acts of violations of (i) the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

103. The members of the Racketeering Enterprise conspired for the common purpose of developing malicious phishing kits and operating a global technical infrastructure that supports credential theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud.

104. Plaintiffs have been and continue to be directly injured by RaccoonO365 Defendants' conduct. But for the alleged conspiracy to conduct a pattern of racketeering activity, Plaintiffs would not have incurred damages. Specifically, Microsoft has incurred over \$650,000 in damages as a direct result of RaccoonO365 Defendants' racketeering activity. Health-ISAC has incurred over \$12,000 in damages as a direct result of the same activity.

105. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT IV

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

(Microsoft; Health-ISAC)

106. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 105 above.

107. Microsoft's Windows operating system software and Microsoft's customers' computers running such software are facilities through which electronic communication services are provided to users and customers.

108. RaccoonO365 Defendants knowingly and intentionally accessed the Windows operating system and Health-ISAC members' network infrastructure and associated software, services, and computers upon which this software and services run without authorization or in excess of any authorization granted by Microsoft, including through the use of stolen credentials. RaccoonO365 Defendants relentlessly attack Health-ISAC members through phishing campaigns and have knowingly and intentionally accessed the networks of Health-ISAC member organizations.

109. Through this unauthorized access, RaccoonO365 Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users.

110. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

111. As a direct result of RaccoonO365 Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

COUNT V

False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a)

(Microsoft)

112. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 111 above.

113. Microsoft's trademarks are distinctive marks that are associated with Microsoft, and exclusively identify Microsoft's businesses, products, and services.

114. RaccoonO365 Defendants make unauthorized use of Microsoft's trademarks. By doing so, RaccoonO365 Defendants create false designations of origin as to tainted Microsoft's products and projects that are likely to cause confusion, mistake, or deception.

115. Because of their wrongful conduct, RaccoonO365 Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

116. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

117. As a direct result of RaccoonO365 Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

COUNT VI

Trademark Infringement Under the Lanham Act, 15 U.S.C. § 1114 *et seq.*

(Microsoft)

118. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 117 above.

119. RaccoonO365 Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Azure®, among other trademarks. By doing so, RaccoonO365 Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system and software. As a result of their wrongful conduct, RaccoonO365 Defendants are liable to Microsoft for violations of the Lanham Act.

120. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

121. As a direct result of RaccoonO365 Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

122. RaccoonO365 Defendants' wrongful and unauthorized use of Plaintiff's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

COUNT VII

Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c)

(Microsoft)

123. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 122 above.

124. Microsoft's trademarks are famous marks that are associated with Microsoft, and exclusively identify its businesses, products, and services.

125. RaccoonO365 Defendants make unauthorized use of Plaintiff's trademarks. By doing so, RaccoonO365 Defendants are likely to cause dilution by tarnishment of Plaintiff's trademarks.

126. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

127. As a direct result of RaccoonO365 Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

COUNT VIII

Common Law Trespass to Chattels

(Microsoft; Health-ISAC)

128. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 127 above.

129. RaccoonO365 Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

130. RaccoonO365 Defendants have, without authority, used a computer or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers, including when RaccoonO365 Defendants uses stolen credentials to access the account, spy on the account's content, and steal other sensitive information.

131. RaccoonO365 Defendants' actions in offering the phishing kits result in unauthorized access through the use of stolen credentials to Microsoft's Windows operating

system and the computers on which such programs run, and result in unauthorized intrusion into those computers and theft of information, account credentials, and funds.

132. RaccoonO365 Defendants' actions in offering the phishing kits result in unauthorized access to Health-ISAC and its member organizations' email accounts and other non-public resources, and result in an unauthorized intrusion into those computers and theft of information and account credentials for the purpose of extracting sensitive information.

133. RaccoonO365 Defendants intentionally caused this conduct, and this conduct was unlawful and unauthorized.

134. RaccoonO365 Defendants' actions have caused injury to Microsoft and Health-ISAC and have interfered with the possessory interests of Microsoft over its software.

135. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

136. As a direct result of RaccoonO365 Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

COUNT IX

Conversion

(Microsoft; Health-ISAC)

137. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 136 above.

138. Microsoft owns all right, title, and interest in its Windows software and the Microsoft 365, Outlook, and Azure software and services. Microsoft licenses its software to end-users. RaccoonO365 Defendants have interfered with, unlawfully and without authorization, and

dispossessed Microsoft of control over its Windows software and its Outlook, OneDrive, and Microsoft 365 software and services. RaccoonO365 Defendants have also deprived Health-ISAC's member organizations of control over their network infrastructure, as RaccoonO365 has been able to use the ill-gotten sensitive information they received through their phishing operation to infiltrate the systems belonging to Health-ISAC's member organizations.

139. Defendants interfered with and converted computers running Windows operating systems and deprived Microsoft and its customers of possession and use of their property and systems.

140. RaccoonO365 Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

141. RaccoonO365 Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

142. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of RaccoonO365 Defendants' ill-gotten profits.

143. As a direct result of RaccoonO365 Defendants' actions, Plaintiffs suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

COUNT X

Unjust Enrichment

(Microsoft; Health-ISAC)

144. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 143 above.

145. The acts of RaccoonO365 Defendants complained of herein constitute unjust enrichment of the RaccoonO365 Defendants at Plaintiff's expense, in violation of the common law.

146. RaccoonO365 Defendants used, without authorization or license, software belonging to Plaintiffs to facilitate unlawful conduct inuring to the benefit of RaccoonO365 Defendants.

147. RaccoonO365 Defendants profited unjustly from their unauthorized and unlicensed use of Plaintiff's intellectual property.

148. Plaintiffs are informed, believe, and thereupon allege that RaccoonO365 Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property and Health-ISACs members stolen information.

149. Retention by the RaccoonO365 Defendants of the profits they derived from their malfeasance would be inequitable and unjust.

150. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of RaccoonO365 Defendants' ill-gotten profits.

151. As a direct result of RaccoonO365 Defendants' actions, Plaintiffs suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless RaccoonO365 Defendants' actions are enjoined.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court enter judgment in their favor and against Defendants, as follows::

1. Awarding judgment in favor of Plaintiffs and against Defendants, for Plaintiffs' actual damages from RaccoonO365 Defendants' activity complained of herein and for any injuries complained of herein, including but not limited to interest and costs, in an amount to be proven at trial. .

2. Declaring that RaccoonO365 Defendants' conduct has been willful, and that RaccoonO365 Defendants have acted with fraud, malice, and oppression.

3. Issuing a temporary restraining order and preliminary and permanent injunction enjoining RaccoonO365 Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injuries complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activities complained of herein or from causing any of the injuries complained of herein.

4. Issuing a preliminary and permanent injunction giving Microsoft control over the domains used by RaccoonO365 Defendants to cause injury and enjoining RaccoonO365 Defendants from using such instrumentalities.

5. Entering judgment disgorging RaccoonO365 Defendants' profits.

6. Entering judgment awarding enhanced, exemplary, and special damages, in an amount to be proved at trial.

7. Entering judgment awarding attorneys' fees and costs, and

8. Awarding such other relief that the Court deems just and proper.


DEMAND FOR JURY TRIAL

Plaintiffs respectfully request a trial by jury on all issues so triable in accordance with Fed.

R. Civ. P. 38.

Dated: August 26, 2025

CROWELL & MORING LLP

By: 
Gary A. Stahl

Two Manhattan West
375 Ninth Avenue
New York, NY 10001
Telephone: (212) 223-4000
Fax: (212) 223-4134
gstahl@crowell.com

Jeffrey L. Poston (*pro hac vice* forthcoming)
Brentnie Brown (*pro hac vice* forthcoming)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
T: 202-624-2500
F: 202-628-5116
JPoston@crowell.com
BrBrown@crowell.com

Amanda (Anna) Z. Saber (*pro hac vice* forthcoming)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
T: 415-986-2800
F: 415-986-2827
ASaber@crowell.com

*Attorneys for Plaintiffs Microsoft Corporation and Health-
ISAC*
