

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

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

Plaintiffs,

v.

Joshua Ogundipe,

and

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

Defendants.

Civil Action No.

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

**DECLARATION OF JASON B. LYONS IN SUPPORT OF PLAINTIFFS' *EX PARTE*
APPLICATION FOR TEMPORARY RESTRAINING ORDER**

I, Jason B. Lyons, declare as follows:

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

2. Microsoft 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®, Outlook®, and Azure®.

Microsoft has invested substantial resources in developing high quality products and services. 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, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous worldwide symbols that are well-recognized within its channels of trade. To protect this goodwill, reputation, and strong branding, Microsoft has registered trademarks for the following products and services: Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Azure®, among other trademarks. The registrations for these trademarks are attached to the Complaint as **Appendix B**.

3. 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 2008.¹ One of DCU's responsibilities is to investigate cybersecurity threats and identify and attribute attacks, like it has done here with the RaccoonO365 Defendants. DCU also collaborates with the Microsoft Threat Intelligence Center (MSTIC), which is made up of thousands world-class experts, security researchers, analysts, and threat hunters. MSTIC regularly publishes threat intelligence blogs alerting customers and the public of cybersecurity threats.²

¹ *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).

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

4. In my role at Microsoft as part of DCU, I assess technological security threats to Microsoft and the effect of such threats on Microsoft's business and customers. Among my responsibilities is protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of malware and participate in court-authorized countermeasures to neutralize and disrupt malware. For example, I have personally investigated and assisted in the court-authorized takedown of several families of malware or botnets while at Microsoft, including the malware families and botnets known as Ramnit, ZeroAccess, Dorkbot, and Necurs.

5. Before joining Microsoft, I worked for Xerox as the Manager of Xerox's Incident Response Team. I also worked for Affiliated Computer Services ("ACS") prior to Xerox's acquisition of ACS. While at ACS, I provided in court testimony in connection with a temporary restraining order application concerning misappropriation of ACS's intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

6. My declaration concerns the investigation into a foreign-cybercriminal organization comprised of Joshua Ogundipe and a series of unknown individuals—John Does 1-4—who are collectively known as "RaccoonO365 Defendants." I have investigated the structure and function of RaccoonO365 Defendants' criminal organization, which I discuss in this declaration. I have also investigated and addressed RaccoonO365 Defendants' victim targeting methodology, attack techniques, and the tools used to execute their cybercriminal attacks. My

declaration also addresses the impact and harm that RaccoonO365 Defendants cause Microsoft, its customers, including Health-ISAC and its member organizations, and the public, and the continuation of this irreparable harm if the RaccoonO365 Defendants are permitted to carry out their cybercriminal activity. Finally, my declaration explains what I believe to be the most effective way of disrupting RaccoonO365 Defendants' illegal activity.

CYBERCRIME AT ISSUE: PHISHING-AS-A-SERVICE

7. 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 manufacture, sell, and facilitate the deployment of pre-packaged sets of tools ("phishing kits") that enable other cybercriminals to launch phishing attacks with relative ease. These RaccoonO365-branded phishing kits 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 do not and cannot frontally target Microsoft's security features. Rather, when a phishing recipient clicks on a weaponized link, he effectively ushers the attacker right through the front door of the victim's system negating the ability of Microsoft security to repel the attack.

8. Phishing is particularly pernicious because once the victim interacts with the lure and unknowingly provides their credentials to a cybercriminal, that cybercriminal has unfettered

access, with which it can launch devastating ransomware and malware attacks. In 2024 alone the estimated financial impact of phishing attacks was more than \$3.5 billion.

9. I, along with other Microsoft investigators, investigate cybercrime campaigns like phishing-as-a-service (“PhaaS”) that are perpetrated by threat actors targeting Microsoft and its customers. In this role, I have investigated RaccoonO365’s PhaaS campaign.

10. As an experienced cybercriminal investigator, I am familiar with phishing. The intent of phishing typically includes stealing someone’s account credentials, authorization tokens or causing the victim to reveal personal information (such as credit card numbers, bank information, or passwords) or sensitive business information for use in perpetrating additional cybercrimes.

11. The Phishing-as-a-Service or PhaaS kits are essentially “how to” manuals to assist RaccoonO365 Defendants’ cybercriminal customers in developing and executing attacks on email systems through phishing campaigns. Cybercriminals can buy the phishing kit that best serves their criminal objective, including selecting which companies they want to target (here, targeting Microsoft’s enterprise customers). This declaration specifically concerns the phishing kits that are designed to lead victims to believe they are dealing with legitimate Microsoft products and therefore can be used to target Microsoft customers.

12. The RaccoonO365 Defendants operate in a similar fashion to another threat actor known as Fake ONNX. Fake ONNX 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 against the Fake ONNX Defendants 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). I was personally

involved in the investigation and takedown of the Fake ONNX cybercriminal operation. In connection with Microsoft's Application for a Temporary Restraining Order, I testified in Court regarding my investigation and the scope of Fake ONNX's operation.

13. 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 right where the Fake ONNX Defendants left off.

14. These phishing kits are particularly problematic as they facilitate "adversary-in-the-middle" ("AiTM") attacks whereby the attacker establishes a permanent presence in a victim's system with the ability to intercept communications.

15. PhaaS lowers the barrier to entry for cybercrime from a technical skillset perspective, by allowing even novices to launch effective phishing attacks. PhaaS also offers anonymity to the attackers as the service provider (the developer of the RaccoonO365-branded kits) handles the technical aspects of the phishing campaigns and advertises these support services as a selling point. Additionally, PhaaS lowers the barrier to entry from a financial perspective as cybercriminals no longer need to expend significant financial resources to develop and scale their infrastructure. This model has proven lucrative, as it enables widespread phishing activities. The ease of use and availability of these services makes it an attractive option for potential cybercriminals. The RaccoonO365 Defendants' "phishing operation" provides the gateway and know-how for would-be cybercriminals to attack Microsoft customers and steal their personal and confidential business information. For more seasoned cybercriminals, PhaaS kits, such as the

RaccoonO365 kit, allows for low-cost scaling of a small-scale cyber operations into a larger, more widespread operation.

THE RACCOONO365 DEFENDANTS

16. RaccoonO365 Defendants are cybercriminals that manufacture and sell RaccoonO365³, phishing kits and also provide PhaaS to other cybercriminals. Other downstream cybercriminals purchase the RaccoonO365-branded phishing kits from the RaccoonO365 Defendants and launch phishing attacks against many organizations across various industries.

17. DCU investigated the RaccoonO365 Defendants and identified Joshua Ogundipe as an individual involved in the criminal organization. DCU investigators identified a shared video on the RaccoonO365 telegram page demonstrating a new phishing technique and phishing domains being offered by RaccoonO365. DCU investigators then combined open-source intelligence (OSINT) with Microsoft internal telemetry which revealed an email address belonging to joshuaogundipe38@gmail.com. The investigation of this email address revealed the account name “Joshua Ogundipe,” who is believed to reside in Nigeria. Additionally, DCU investigators were able to identify developmental paths and tooling associated with RaccoonO365 which led to connecting the name to a LinkedIn account Joshua-ogundipe-292688261 and a Gmail account profile picture, showing Joshua Ogundipe’s picture and country of residence. **See Figure 1.** Additionally, as described in the Declaration of Nick Monaco that has been concurrently filed, Microsoft has been able to connect Ogundipe’s cryptocurrency wallets to Nigerian crypto exchanges.

³ Given that O365 is a shorthand name given to Microsoft Outlook 365 products, I am informed and believe that the phishing kit name was intentionally selected to demonstrate to customers that the RaccoonO365 phishing kits are designed to target Microsoft’s customers.



Figure 1

18. To support this phishing operation, RaccoonO365 Defendants have established and operated a vast network of domains (also known as web addresses), which are used to identify a website and allow users on the internet to access a particular website. RaccoonO365 Defendants include the domains in their phishing emails and encourage the victims to click on the malicious domains where they are redirected to a RaccoonO365-controlled webpage and then unknowingly provide their credentials to Defendants. The identity of the website domains used by RaccoonO365 Defendants to support their phishing operation are set forth at **Appendix A** to this Complaint and constitute RaccoonO365 Defendants' technical infrastructure. Microsoft has identified 338 domains associated with Raccoon0365.

19. The remaining identities of the RaccoonO365 cybercriminal organization are unknown or uncertain because Defendants take great measures to hide their identity. Even still, I have been able to identify specific functions or responsibilities of these individuals who collectively carry out RaccoonO365's cybercrime operation.

20. Based on my investigation, I am informed and believe that John Doe 1 controls the RaccoonO365 Defendants criminal phishing organization and the technical infrastructure.

21. Based on my investigation, I am informed and believe that John Doe 2 provides technical and administrative support for the RaccoonO365 Defendants' criminal phishing

organization and the technical infrastructure, including facilitating the sale and promotion of the RaccoonO365-branded phishing kits.

22. Based on my investigation, I am informed and believe that John Doe 3 and John Doe 4 are cybercriminals who purchased the RaccoonO365-branded phishing kit, registered a new phishing domain, and incorporated that phishing domain into the RaccoonO365 Defendants' criminal phishing organization and the technical infrastructure. Given that the Telegram channel used by RaccoonO365 Defendants has over 800 members (*see infra* ¶ 33, Figure 3)—each of whom could be an actual or potential customer—I estimate that John Does 3 and 4 represent hundreds of purchasers and users of the RaccoonO365 kits.

23. The RaccoonO365 Defendants each have specialized roles within the cybercriminal organization. Each RaccoonO365 Defendant cooperates and colludes in the sale, distribution, deployment 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 cybercriminal customers, the multi-tier subscription of phishing operation services, circumvention of technical security measures to gain access to victim computers and information, and the unauthorized use and dissemination of Microsoft's intellectual property. Their ongoing association with one another and reliance on each other's specialized role and contribution allows the RaccoonO365 Defendants to function as a single unit within a unitary operational structure. Based on my investigation, I have concluded that this allows the RaccoonO365 Defendants to scale their operation and increase the profitability of their criminal activity. Because the creator, sellers, and distributors of the RaccoonO365-branded phishing kits work collectively with the cybercriminal customers, they are able to expand the scope and reach of the RaccoonO365 Defendants' phishing operation.

RACCOONO365 DEFENDANTS' MODUS OPERANDI: PHISHING

24. RaccoonO365 Defendants develop phishing kits for their cybercriminal customers to purchase and use for the customers' cybercrime operations. These customers who purchase the all-in-one, do-it-yourself kits become part of the RaccoonO365 Defendants' criminal operation when they, in turn, use and deploy the RaccoonO365-branding phishing kits to conduct their own cybercrimes directed at Microsoft and its customers. The RaccoonO365-branded phishing kits allow the cybercriminal customer to infiltrate the systems of Microsoft customers undetected and steal credentials belonging to users of the infiltrated network, through deceit or tricking the victims. The cybercriminal customers then use these stolen credentials to access and infiltrate the victim's network. The cybercriminal customers take on what is known as an AiTM role, whereby the cybercriminal customer positions itself between communications directed to and from Microsoft customers. **Figure 2** demonstrates how cybercriminal customers become part of the RaccoonO365 Defendants criminal organization as they buy the phishing kit, deploy the kit, and engage in phishing attacks (in collaboration with other, existing RaccoonO365 Defendants) against a victim.

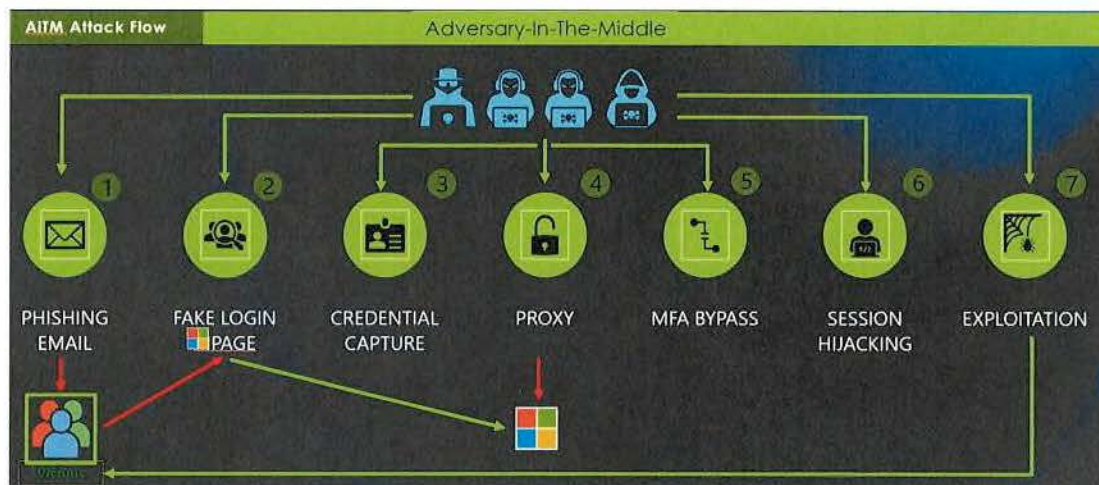


Figure 2

25. A successful phishing attack relies on a victim being convinced that the email communication received or a website they are directed to is authentic. This is made possible when the communication they receive appears to be from familiar contacts or organizations (even when the communication *is not* actually from a known contact or organization). This is done by creating an email address designed to look *similar* to a legitimate email address, for example using “5” instead of “s” or “nn” instead of “m.” Similarly, when a victim is tricked into clicking on a RaccoonO365-controlled domain, they will be deceived into believing that the domain is benign, if the domain name appears to refer to a company name or its well-known products. 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 (the “o” in “soft”) or a number is in place of a letter (here the number “1” in place of the letter “i”). This is a practice known as either a “homoglyph” domain or “typosquatting.” As a result, the phishing domain may easily be perceived as the authentic domain. For example, loginmicrosoftonlineservices.com and microsoft-securedocuments.com, which are identified in **Appendix A** references Microsoft, its well-known products and services, and employ the tactic described above of typosquatting.

26. When a phishing victim is deceived to visit a website to enter their credentials, RaccoonO365 Defendants lie in wait to collect those credentials in order to subsequently access their accounts to further their cybercrime.

RACCOONO365 DEFENDANTS ATTACK CHAIN

Step 1: Development and Sale of RaccoonO365 -Branded Phishing Kits

27. The phishing kits designed, developed, and sold by the RaccoonO365 Defendants are specifically intended to allow customers a do-it-yourself toolkit to phish Microsoft customers and use the ill-gotten credentials to infiltrate Microsoft systems. Specifically, these kits are

customized using Microsoft logos, to 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.

28. RaccoonO365 Defendants' phishing kits are specifically developed to target Microsoft 365, Office 365, or Azure⁴ users, and include two-factor (2FA) authentication⁵ bypass features for the Microsoft Authenticator⁶ application and Microsoft Office, specifically the Outlook application. 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 can 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 break into Microsoft systems.

⁴ Microsoft 365 and Office 365 are product families of productivity software, collaboration and cloud-based services owned by Microsoft. Microsoft 365 and Office 365 includes 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. These products facilitate the electronic communications of Microsoft's customers.

⁵ 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.

⁶ 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.

29. Based on my investigation, I have become aware of two products that RaccoonO365 sell and promote: the Postman Mass Mailer and Links Credential Capture kits.⁷ Postman Mass Mailer is advertised as a tool designed to bypass Microsoft security measures against mass/bulk emailing⁸ and deliver phishing emails directly to victims' inboxes. The Postman Mass Mailer enables users to configure email lists, attachments, subjects, and message formats. Mass Mailer also claims that it permits users to evade Microsoft's technology, limiting the number of emails that can be sent from an address in a single day. This is false as the Raccoon 0365 Defendants cannot evade these limits contrary to their advertising.

30. 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.

31. I also am aware that RaccoonO365 has advertised AI MailCheck, an AI-powered tool, as a new all-in-one lead extraction engine designed to automate the process of harvesting and sorting email leads directly from compromised Office 365 inbox sessions. The tool uses active session cookies to extract emails from 2FA and non-2FA accounts, with a built-in verifier that checks the validity and responsiveness of harvested emails. Extracted leads are automatically sorted and segmented by type, including Office 365 Business, Hotmail, Okta, GoDaddy, and

⁷ As described in the concurrently filed Monaco Declaration, DCU was able conduct test buys for both the Postman Mass Mailer and Links Credential Capture kits. Monaco Decl. ¶¶ 6, 7, 19, 12, 13, 15, 20.


⁸ 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 emails per day; emailing at such a high frequency is often indicative of spam, phishing, or other cybercriminal activity.



ADFS. All harvested leads are centrally managed within a dashboard for efficient export and targeting. DCU attempted to do a test buy of this product but was informed by RaccoonO365 that the product had not yet been released. *See Monaco Decl.* ¶ 26.

32. The ability to use the phishing kit to trick Microsoft customers to hand over their credentials allowing infiltration into Microsoft's systems is a "selling point" of the RaccoonO365-branded phishing kits. Cybercriminal customers purchase these RaccoonO365-branded kits because they are advertised as possessing the ability to infiltrate Microsoft systems and the significant security protocols that Microsoft implements to protect against cyberattacks.


33. The RaccoonO365-branded phishing kits are promoted through Telegram Messenger, a secure, cloud-based messaging platform. It is known for its end-to-end encryption. RaccoonO365 Defendants have set up Telegram accounts and "channels" (a thread that allows the admin of the channel to post information to a larger audience) to facilitate private communications between the RaccoonO365 Defendants and potential customers interested in purchasing the phishing kits. **See Figure 3** for screenshots of the Telegram channel used by the **RaccoonO365 Defendants**.

Group Info




RaccoonO365  2FA/MFA 


843 members




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


Description




Notifications 



5 shared links




ADMINISTRATORS





RaccoonO365 PayMate

has access to messages

admin



RaccoonO365  2FA/MFA  For ...

owner

Figure 3

34. The RaccoonO365 Defendants do not just sell their phishing kit for one time use. The RaccoonO365 Defendants offer a subscription plan at different pricing tiers to gain access to the phishing kits – offering a “Standard,” “Pro,” or “Pro Extended” option See **Figure 4**. By adopting a year-long subscription model, RaccoonO365 encourages repeat, ongoing, longtime use of the phishing kits. Additionally, as shown in **Figure 4**, RaccoonO365 Defendants also

15

offer custom licensing and a support feature, which would be attractive to more sophisticated cybercriminals who may be looking for a customized phishing kit beyond the basic offering.

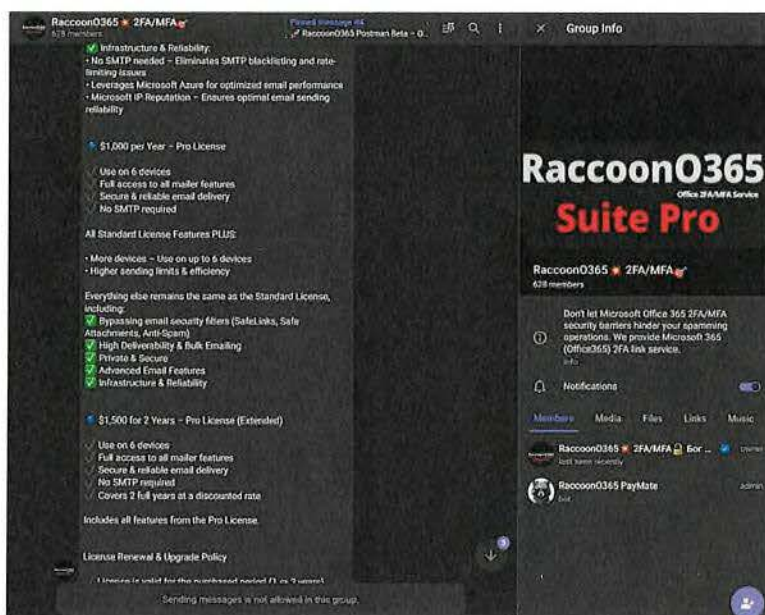


Figure 4

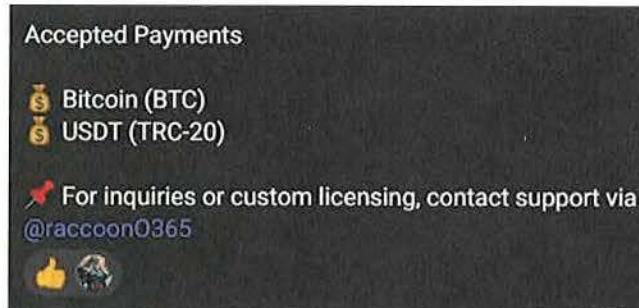


Figure 5

35. RaccoonO365 Defendants also offer an administrative panel which functions as a customer dashboard. Customers can use this dashboard to track recipients of phishing emails, track whether a phishing attack has 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 (John Does 1 and 2), manage this dashboard using domains that Microsoft has been able to track back to Ogundipe.

To avoid detection, Ogundipe has periodically updated the domain on which the panel is operated.

Figure 6 is an image of the login page that a customer can use to access the admin panel.

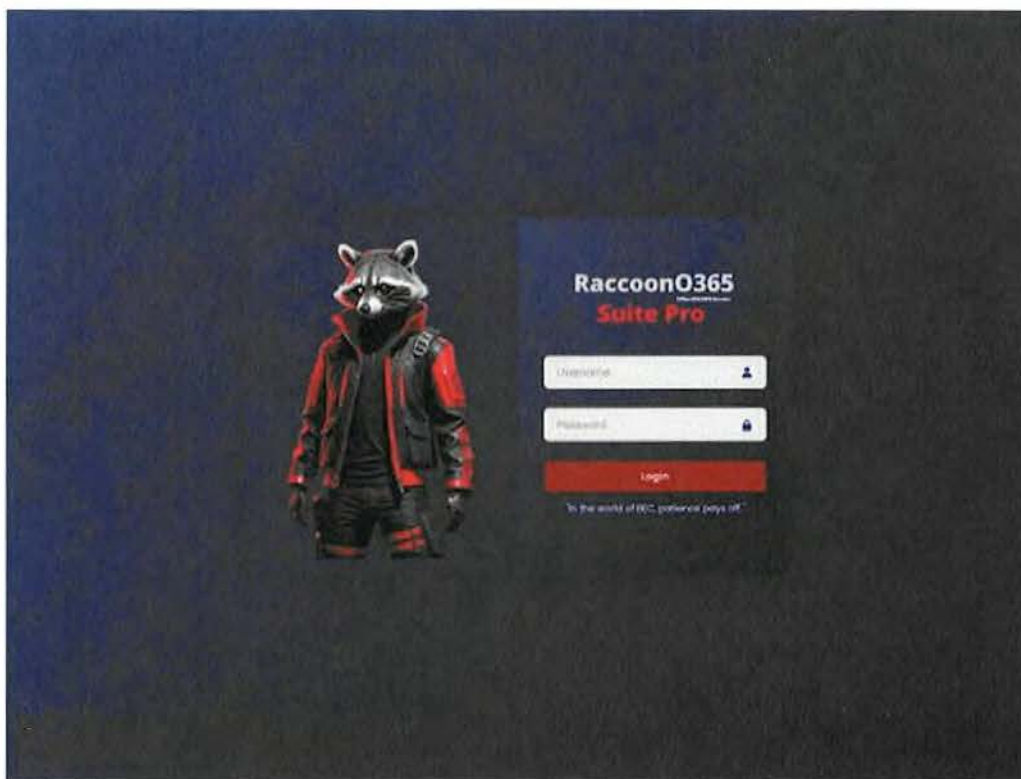


Figure 6 – LOGIN SCREEN FOR CUSTOMER DASHBOARD

36. The RaccoonO365 Defendants accept payment via cryptocurrency, specifically via Bitcoin (BTC) and Tether (USDT, a cryptocurrency tied to the United States Dollar). By using cryptocurrency, RaccoonO365 Defendants incorporate an added layer of protection given that tracing cryptocurrency transactions is much more difficult.

Step Two: Activation of RaccoonO365-Branded Phishing Kits and Malicious Domains

37. Once the RaccoonO365 Defendants sell the RaccoonO365 -branded phishing kit to a cybercriminal customer,⁹ the customer must take several steps to activate the phishing kit and

⁹ Cybercriminal customers are John Doe 3-4 once they have purchased an RaccoonO365-branded phishing kit from Defendants.

incorporate the malicious domain into the RaccoonO365 Defendants technical infrastructure. First, the cybercriminal must purchase a domain to be used for the phishing operation. Second, the cybercriminal must provide RaccoonO365 Defendants with the domains and in turn is directed to Cloudflare and uses other Cloudflare services to avoid detection. Third, the cybercriminals' phishing domain must be connected to the phishing operation which then becomes part of the entire technical infrastructure controlled by RaccoonO365 Defendants. Fourth, the cybercriminals must set up a Gmail account that captures the victim's credentials from the phishing domain. This process for the "Links" tool is described in **Figure 7**.

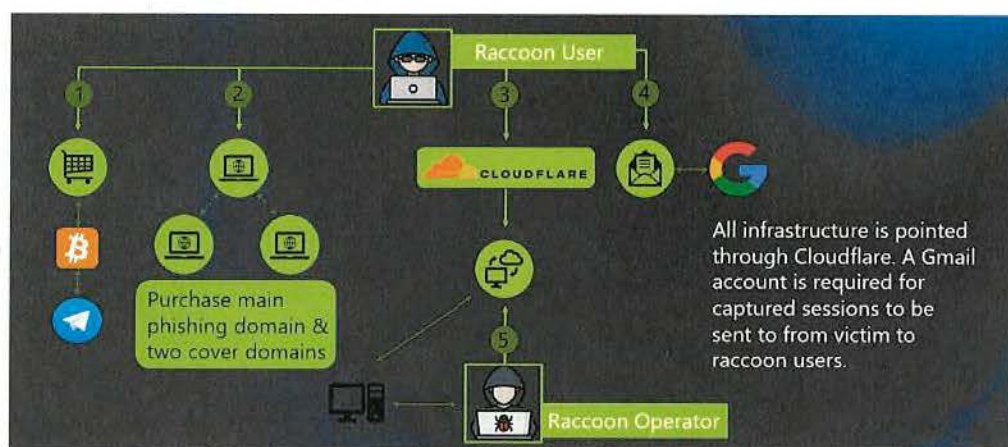


Figure 7

38. The first step is purchasing domains. RaccoonO365 Defendants' cybercriminal customers must purchase a domain from a registrar (a third-party company, like GoDaddy that makes domains available for purchase). The RaccoonO365 Defendants follow a "bring your own domain" model, where each cybercriminal customer is responsible for bringing their own pre-purchased domain to connect into the overarching RaccoonO365 technical infrastructure.

39. As described in Paragraph 25, *supra*, the domains registered are purposefully selected because they appear, at first glance, to be related to Microsoft or its products. But these domains actually contain subtle misspellings — *e.g.*, "verificaton" (with a missing "i") instead of

“verification” (the word correctly spelled), which as I described in Paragraph 25, *supra* is a practice known as using a “homoglyph” domain or “typosquatting.” Because these domains will be used by the cybercriminal customers to carry out phishing attacks, RaccoonO365 Defendants focus on manufacturing “legitimacy” and employing tactics like typosquatting to hide the sinister nature of the malicious domain.

40. The second activation step for the cybercriminal is to resolve the domain to Cloudflare and use other Cloudflare services to avoid detection. The Cloudflare infrastructure proxies the phishing site and powers the redirection of the cover domains. Cloudflare, Inc. (“Cloudflare”) is a company that provides a variety of legitimate network services and security features to protect their users from online cyberthreats and attacks.

41. The RaccoonO365 customers provide the two “cover” domains and main phishing domain to the RaccoonO365 Defendants’ who direct each of the cover domains to the Cloudflare infrastructure to further evade detection.

42. 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 determine the legitimacy of an email. The RaccoonO365 Defendants have hijacked this proxy to conceal their “home address” (their real IP address). This means that the IP address will show a fictitious location, which further allows RaccoonO365 Defendants to evade detection.

43. The RaccoonO365 Defendants misuse these legitimate services offered by Cloudflare to perpetrate their cybercrimes. In my experience, it is common for cybercriminals to misuse an otherwise legitimate software or tool for the purposes of committing cybercrime. This is done intentionally because cybercriminals can simply retool an existing product, which is more

efficient than creating once from scratch. Additionally, the cybercriminal can capitalize on the branding and goodwill associated with the legitimate product because victims will be unaware that they are interacting with a malicious version of a product or service that they would ordinarily consider to be “safe.”

44. By misusing Cloudflare’s services, RaccoonO365 Defendants can obscure the real location of their phishing websites and can employ measures like CAPTCHA to make it harder for automated security scanning systems to detect and block their phishing websites. By preventing scanning, the RaccoonO365 Defendants increase their phishing campaign efficiency: they protect themselves from being discovered which lessens the chance that they are shut down, either by the third-party registrars or law enforcement.

Step Three: Connecting to the RACCOONO365 Defendants’ Phishing Operation

45. After the cybercriminals complete the domain’s registration of the “cover” domain, the next step is to connect the purchased domains with the RaccoonO365 infrastructure. The domains must be connected to the phishing operation which then becomes part of the entire technical infrastructure controlled by RaccoonO365 Defendants. The cybercriminals will then provide the RaccoonO365 Defendants with the domains and are then directed to connect the domains to the Cloudflare infrastructure. After this step, all domains are pointed towards the Cloudflare Domain Name System¹⁰ that is owned by the RaccoonO365 Defendants. Because Ogundipe owns this Cloudflare infrastructure, he validates the “cover” domain locally on his machine to ensure full functionality. **Figure 8** is an example of the cybercriminals domains being pointed towards the Cloudflare Domain Name System.

¹⁰ 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.



Figure 8

Step Four: Phishing Attacks by RaccoonO365

46. The next step involves the RaccoonO365 Defendants deploying the phishing kits and engaging in phishing attacks. The RaccoonO365 Defendants will send phishing emails to victims that prompt the victim to click on a link. The RaccoonO365 kits give their customers the ability to customize the phishing email to promote greater efficacy. For example, as described in Paragraph 47, *infra*, during tax season, the RaccoonO365 Defendants sent emails with subject lines related to tax documents urging immediate attention to avoid adverse tax consequences. These phishing emails were crafted to extract financial information. Likewise, RaccoonO365 Defendants use the kits to send customized phishing emails to companies in the healthcare industry, with the goal of extracting sensitive healthcare information.

47. For example, in one instance, the lure is an email with the subject “Employee Tax Refund Report.” Contained within the lure is an attachment labeled “TaxRefundExport.” See **Figures 9-10**. If a victim opens the pdf file, they are taken to a document that states the victim has tax documents to review. The pdf also displays a QR code and encourages the user to scan the QR code to begin the review process.

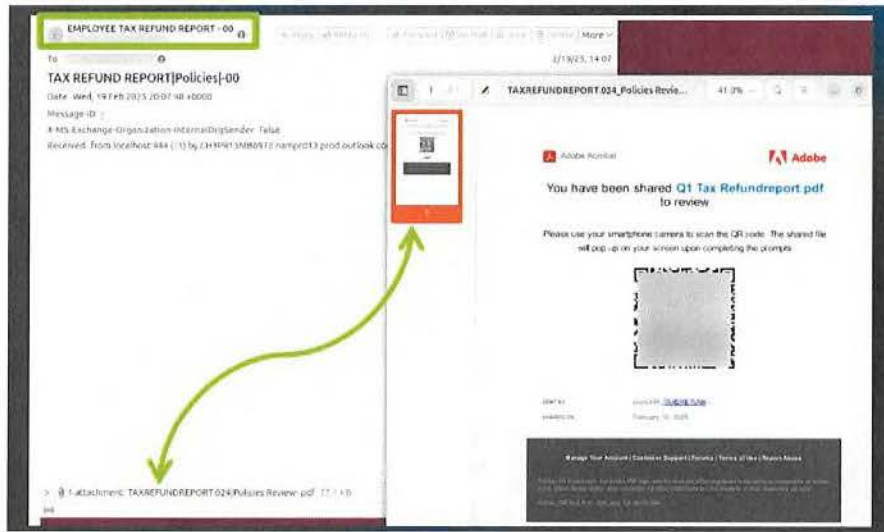


Figure 9



Figure 10

48. In another example, RaccoonO365 Defendants have 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 examples, the subject line and attachments discuss “incoming payments,” “review and approval,” and “payment confirmation.” *See Figures 11-14.*



Figure 11



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 12

[CAUTION: SUSPECT SENDER]



Caution: This message was sent from outside your organization

Alert sender | Block sender

Privacy Notice: This electronic mail message, and any attachments, are confidential and are intended for the exclusive use of the addressee(s) and may contain information that is proprietary and that may be individually identifiable or Protected Health Information under HIPAA. If you are not the intended recipient, please immediately contact the sender by telephone, or by email, and destroy all copies of this message. If you are a regular recipient of our electronic mail, please notify us promptly if you change your email address.

Figure 13



Invoice #75282

Hello [redacted]

Please be advised that a payment for aolmedo@ahcpllc.com is due to be processed on Friday, August 30, 2024.

To access the file, kindly scan the QR code provided below.



- 2 Pages
- Remittance Information
- Ahcpllc via OneDrive

Please be informed that, to maintain security, unchecked fax documents shared since Thursday, August 22, 2024 will be removed.

Scanned by: Ahcpllc IT Support Team.

Figure 14

49. That the kits offer the ability to customize the phishing lures with ease is one reason why these kits are so damaging to Microsoft, its customers, Health-ISAC, its member organizations, and the public. With minimal effort, RaccoonO365 Defendants can customize the phishing lures to target a myriad of victims across various industries, making it easy for RaccoonO365 Defendants to scale their cybercriminal activity and target sensitive-information rich targets.

50. Once a victim clicks on the link or scans the QR code, 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 the 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 **Figures 15-17**. At this stage, the RaccoonO365 Defendants have completed the goal of the phishing—credential theft—by using the AiTM methodology described above. To complete the deception, after the victim provides the credentials to RaccoonO365 Defendants, the victim is then rerouted to a legitimate Microsoft website so that the victim remains unsuspecting that their system has been compromised.



Figure 15



Figure 16

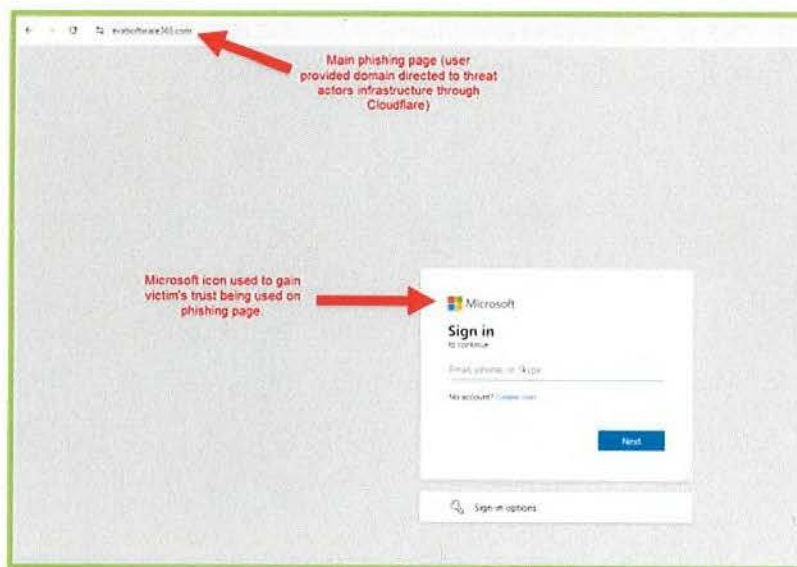


Figure 17

51. 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. A 2FA token is a unique piece of code that contains information about the user's identity and the type of access for which they have authorization. For example, it may be a six-digit code that the user must enter after they have entered their login credentials. Once the victim enters their authentication details, receives the 2FA token, and enters the token into Fake RaccoonO365 Defendants' fraudulent login page, their credentials, and 2FA tokens are captured

by RaccoonO365 Defendants. **Figures 18-20** are examples of RaccoonO365 successfully capturing credentials and the 2FA/MFA token.



Figure 18 – Prompt for 2FA



Figure 19 – Captured Victim Credential



Figure 20 – Captured MFA/Cookie Session

52. This verification then creates the impression that RaccoonO365 Defendants' malicious website is legitimate. At this point, RaccoonO365 Defendants can login to the user's real account and take control of the account, even though RaccoonO365 Defendants did not have authorization to access these accounts.

53. Based on DCU's investigation, 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 automate the process of sending phishing emails by easily selecting the attachment, subject line, and message contents once and then automating for all the other recipients. 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 or Office 365 accounts using Microsoft Azure infrastructure. When used in connection with Links, RaccoonO365 Defendants get more value from their kits because they can amplify the number of targets they can

attack and the frequency at which they attack. Because the Postman Mailer automates the sending process, the threat actor does not have to oversee the process.

54. The attack methodology described in Paragraphs 27-53 of this declaration are depicted in **Figure 21**.

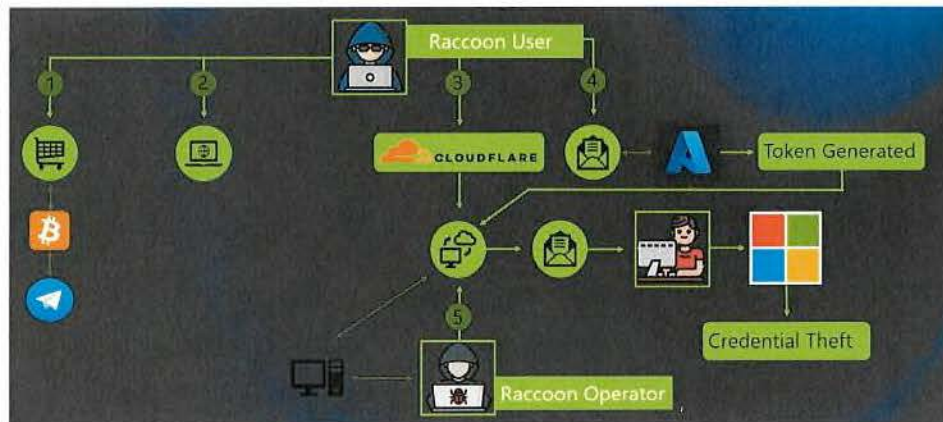


Figure 21

ATTRIBUTION TO THE RACCOONO365 DEFENDANTS

55. Microsoft investigated the online infrastructure used in the RaccoonO365 Defendants' phishing campaign described in this declaration. I determined that Defendants have registered 338 Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. The RaccoonO365 Defendants have registered domains using functioning email addresses by which they communicated with domain registrars to complete the registration process.

56. Cybercriminals, such as the RaccoonO365 Defendants, are known to hide their identities to evade capture by law enforcement and continue their cybercrime.

57. During the investigation, I engaged in the analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Defendants. By identifying these signatures, I determined that the domains identified in **Appendix A** belong to

and are used by the RaccoonO365 Defendants. Specifically, the following indicators were used in my assessment: domain registration patterns, phishing URL patterns and components based on known RaccoonO365 domains, the time period during which the domain was registered, analysis of WHOIS data, indicators from the Microsoft email detonation/protection system, domain resolution patterns, and Open-Source threat detection rules.

58. These features when taken together, provide a high level of confidence that a given domain is a RaccoonO365 domain. Each such domain is manually reviewed in detail by one or more subject matter experts at DCU as necessary to ascertain whether it is, in fact, a RaccoonO365 domain. Based on this analysis, we have identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the RaccoonO365 Defendants. At times, other researchers in the security community independently identify RaccoonO365 domains and associated IP addresses, and these reports may be used to further validate Microsoft's analysis. These high-confidence domains are identified in **Appendix A**.

DEFENDANTS TARGET VICTIMS LOCATED IN NEW YORK

59. The RaccoonO365 Defendants have targeted numerous healthcare organizations and financial institutions. Among the states affected, New York ranks in the top ten, with a significant concentration of victims located in New York City where 54 entities were harmed by RaccoonO365 phishing attacks. New York City has the most attacked organizations of any city in the United States. Based on my investigation, I have generated a heatmap showing the location of cybercriminal activity that DCU has attributed to RaccoonO365 Defendants. *See Figure 22*.

Figure 23 depicts the Top United States cities where RaccoonO365 have attacked Microsoft customers and Health-ISAC member organization.

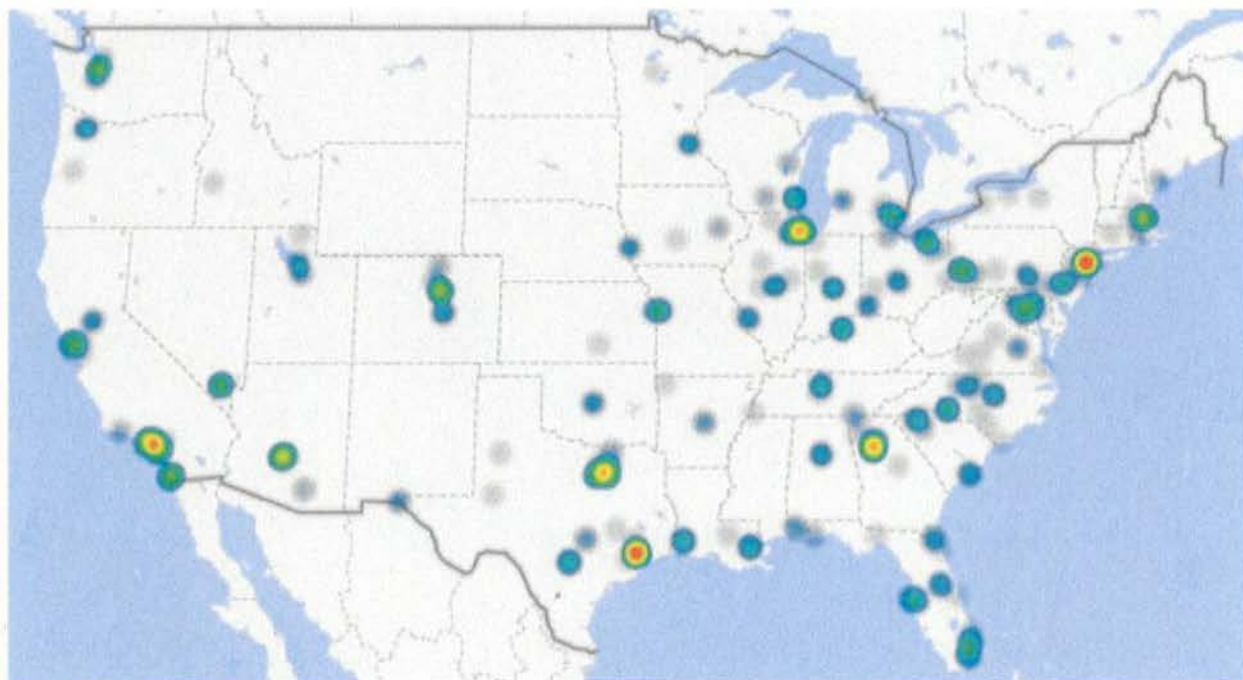


Figure 22



Figure 23

HARM TO MICROSOFT AND ITS CUSTOMERS

60. RaccoonO365 Defendants have targeted Microsoft, its customers, and the public to advance their financially motivated cybercrimes. The RaccoonO365 Defendants have caused and continue to cause irreparable injury to Microsoft, its customers, Health-ISAC, its member organizations, and the public. The RaccoonO365 Defendants' activities irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill.

61. The RaccoonO365 Defendants' criminal acts directly harm Microsoft's reputation and goodwill that it has obtained through its extensive branding efforts.

62. *First*, RaccoonO365-branded phishing kits are customized using Microsoft logos to 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. Thus, each time a phishing kit is sold, it is done with the express purpose of hacking into Microsoft's products and systems that Microsoft has expended significant resources to build and protect.

63. *Second*, RaccoonO365 Defendants leverage Microsoft systems and programs, such as Outlook, Microsoft 365, and Office 365 to further enhance the perceived legitimacy of the attack. Similarly, because the login pages that RaccoonO365 Defendants use include the Microsoft name and logo, the victim will be completely unaware of the threat and believe that the link is to a legitimate Microsoft webpage is trustworthy, when in fact, it is malicious. 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 and that customers have come to expect.

64. *Third*, the domains used by RaccoonO365 are intentionally designed to mimic the name Microsoft and its products. This means that when a victim is phished and is redirected to a

RaccoonO365-controlled domain, the victim will see a domain that on its face looks like a Microsoft domain. The victim will not be suspicious of the domain because of how legitimate it appears. For example, sharepointcloudfilese-storage.com incorporates “SharePoint,” which is Microsoft’s online document management platform. Likewise, office365cloudfiles.com references Office 365, which is the name Microsoft gives to a family of software that includes Word, Excel, PowerPoint, Outlook, and One Note. In each instance, a victim who sees these domains would believe she is visiting a Microsoft website.

65. Customers expect certain quality from Microsoft. When “Microsoft” systems and products are used in connection with cybercrime, customers will mistakenly believe that Microsoft is responsible for the attack. Customers subjected to the negative effects of Defendants’ phishing attacks sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused. There is a great risk that because RaccoonO365 Defendants misuse Microsoft’s branding and trademarks and rely on this misuse to deceive, Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft’s products and services, thereby diluting and tarnishing the value of these trademarks and brands. If a customer leaves Microsoft due to improperly blaming Microsoft for a phishing attack or believes that Microsoft’s systems and products are not secure (because customers are unaware of RaccoonO365 Defendants’ deception), it may be costly or impossible to convince the customer to return to Microsoft. Additionally, because a successful phishing attack can be the precursor to other cybercriminal attacks, an organization that is later subject to a malware or ransomware attack that occurred because the cybercriminal gained network

access through the phishing, may incorrectly blame Microsoft for these attacks.¹¹ In connection with my investigation, I became aware that RaccoonO365 Defendants and their phishing kits pose a significant risk to the financial and healthcare sector. RaccoonO365 Defendants attempts to acquire sensitive financial information through emails that resemble official tax refund documents. An example includes an email titled “Tax Refund Report,” which contains an Adobe attachment requiring a login to access the report. These fraudulent emails are primarily aimed at the healthcare sector, focusing on tax refund themes. In other instances, RaccoonO365 Defendants have targeted healthcare companies, with emails purporting to concern payment details. In total, based on DCU’s investigation, I am aware that RaccoonO365 Defendants have targeted at least 60 companies in the healthcare sector, including 17 organizations that are members of Co-Plaintiff Health-ISAC and at least 75 companies in the financial sector.

66. Microsoft has invested significant resources in excess of \$5,000 to address and attempt to remediate the harm caused by RaccoonO365 Defendants’ crimes. Specifically, Microsoft has spent approximately \$250,000, which represents the time that Microsoft DCU personnel have spent investigating the RaccoonO365 Defendants and their infrastructure.

DISRUPTING RACCOONO365’S ILLEGAL ACTIVITY

67. The most vulnerable point in the Defendants’ operations are technical infrastructure domains used by the RaccoonO365 Defendants to carry out their phishing campaigns. These

¹¹ The Fake ONNX cybercriminals that Microsoft took down last year had been marketing and selling their phishing kits for several years before enjoined. 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, therefore, in a position to stop RaccoonO365 Defendants *before* they successfully launch ransomware and malware attacks on the public.

domains are attached as **Appendix A** to my declaration. These domains have been used in phishing emails directed at users of Microsoft's email services and enterprise platforms.

68. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers and thereby cut off the way the RaccoonO365 Defendants phish and collect sensitive personal and business information from victims. In other words, any time a user clicks on a link in a phishing email and provides their username and password, that information will no longer be captured by RaccoonO365 Defendants because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of the RaccoonO365 Defendants.

69. Redirecting these RaccoonO365 domains will directly disrupt current infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest in protecting customers of other web services companies who have consented to the relief sought in this action.

70. I believe that the most effective way to suspend the injury caused to Microsoft, its customers, including Health-ISAC and the public, is to take the steps described in the Proposed Order. This relief will significantly hinder the RaccoonO365 Defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to RaccoonO365's malicious activities.

71. The RaccoonO365 Defendants' techniques are designed to avoid technical mitigation efforts, eliminating the ability to curb the injury purely through technical means. For example, once domains in the RaccoonO365 Defendants' active infrastructure become known to

the security community, the Defendants abandon that infrastructure and move to new infrastructure that is used to continue Defendants' efforts to compromise accounts of new victims.

72. For this reason, providing notice to the RaccoonO365 Defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the RaccoonO365 Defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward.

73. In my experience RaccoonO365 Defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.


74. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by actors carrying out intrusions such as those in this case but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the internet and took other countermeasures causing the actors to continue their operations and destroying or concealing evidence of their operations.

75. In December 2023, I appeared in this Court in connection with the takedown of a group of Vietnamese threat actors who were engaged in a cybercrime as a service operation against Microsoft. I specifically testified before Judge Paul A. Engelmeyer. In that action we sought an *ex parte* TRO, which Judge Engelmeyer granted. Microsoft subsequently served notice on the threat actors.

76. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active RaccoonO365 infrastructure, is to redirect the domains at issue prior to providing notice to the Defendants.

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

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



Jason B. Lyons
Principal Investigator, Digital Crimes Unit
Microsoft Corporation

EXHIBIT 1

JASON LYONS - RESUME

SUMMARY

Jason Lyons is an experienced investigator specializing in computer investigations. Trained and experienced in hacker methodology/techniques, computer forensics, incident response, electronic discovery, litigation support and network intrusion investigations.

SECURITY CLEARANCE

- Top Secret/SCI-Expired.

CERTIFICATIONS

- Encase Certified Examiner (EnCE) - Guidance Software
- Counterintelligence Special Agent - Department of the Army
- Certified Basic Digital Media Collector - Department of Defense
- Certified Basic Computer Crime Investigator – Department of Defense
- Certified Basic Digital Forensic Examiner – Department of Defense
- State of Texas licensed Private Investigator

TECHNICAL SKILLS

- | | |
|--------------------------------------|--|
| • Network Intrusion Investigations | • EnCase Certified Examiner |
| • Incident Response | • PDA and Cell Phone Seizure and Forensics |
| • Investigative Network Monitoring | • Expert Witness Experience |
| • Investigation Management/Liaison | • Technical/Investigative Report Writing |
| • Computer Media Evidence Collection | |
| • Computer Forensics | |

PROFESSIONAL EXPERIENCE

Microsoft Corporation

2013 – Present

Principal Manager of Investigations, Digital Crimes Unit (DCU)

- Work with public (law enforcement, country certs) and private sectors, and develop international partnerships to support malware disruptions on a global scale.
- Conduct proactive malware investigations to identify critical command control infrastructure and to develop disruption strategy to eliminate or severely cripple cyber-criminal infrastructure.
- Document and identify monetization schemes utilized by cyber-criminals ranging from online advertising fraud, ransomware, and targeted financial fraud.
- Work with the Microsoft legal team to develop new legal strategies to disrupt cyber crime through both civil and criminal proceedings.
- Collect electronic evidence to support global malware disruptions and develop criminal referrals for law enforcement.
- Enhance Microsoft's Cyber Threat Intelligence Program (CTIP) which empowers ISP and country CERTS too identify victims of cybercrime.

- Provide expert court testimony with the support of written declarations describing the threat and impact of malware threats on the Microsoft ecosystems.
- Lead and participate in security community working groups that support cybercrime disruption.
- Work with Microsoft Malware Protection Center (MMPC), and other Anti-Virus vendors, to enhance detection of malware and to assist in the development of disruption strategies.

Affiliated Computer Services, Inc. (ACS)

2005 – 2013

Manager, Digital Forensic and eDiscovery Group

- Manager of a fortune 500 company's digital forensic laboratory/group. Responsible for managing, coordinating, investigating, and reporting on legal, corporate security, human resources, and ethics investigations involving digital media.
- Developed policy and procedures for digital evidence acquisition, storage, examination, processing and production.
- Developed and maintained technical investigative support for ACS inside and outside legal counsel on eDiscovery matters. Experienced in developing and executing large eDiscovery collection plans, preserving data in a forensically sound manner, culling of relevant data, presenting data for review, hosting data for review, and producing relevant data for final production.
- Implemented Access Data's Enterprise and eDiscovery solution.

U.S. Department of the Army

1998 – 2005

Assistant Operations Officer/Counterintelligence Special Agent, 902nd Military Intelligence (MI)

Cyber Counterintelligence Activity (CCA), (2003 – 2005)

- Assisted in managing of all CCA branch operations to include all cyber investigations, special intelligence collection missions, cyber investigator training, and quality assurance of all investigative products.
- Supervised 35 special agents and computer forensic technicians.
- Prepared detailed investigative briefings which include results of investigations and forensic analysis for executive level officers.
- Conducted national level liaisons with federal intelligence and law enforcement agencies on many national security investigations.
- Conducted network intrusion investigations, computer media forensics examinations, counterintelligence/counterterrorism special operations, and network forensic analysis.

Counterintelligence Special Agent / Computer Investigator (2000 – 2003)

- Assistant Supervisory Special Agent (ASSA) of an eight man computer Incident Response Team (IRT) specializing in cyber investigations.
- Accountable for managing, editing and reviewing associated technical and investigative reports pertaining to the IRT's investigations.
- Provided and maintained incident response, computer forensics, evidence handling, and computer media search and seizure training for the members of the IRT.
- While assigned to the IRT, served as lead agent on numerous network intrusion and computer forensic Counterintelligence investigations.

Counterintelligence Special Agent / Liaison Officer, 501st MI Brigade, South Korea (1998-1999)

- Served as liaison officer for a Counterintelligence Resident Office in South Korea.
- Maintained regional-level liaison with foreign government officials to collect strategic information for intelligence reporting.
- Established business partnerships and furthered cooperation between the United States and South Korean investigative/intelligence agencies to accomplish bilateral goals.

EDUCATION

- Graduate from Excelsior College in October 2002, with a Bachelor of Science in Liberal Arts.
- Thirteen hours completed for Master's Degree in Information Technology with University of Maryland University College (UMUC).

TRAINING

- Counterintelligence Agent Course-Department of the Army-1998.
- Counterintelligence Fundamentals Warfare (CIFIW)-Department of the Army-2000.
- Introduction to Computer Search and Seizure-Defense Computer Investigation Training Program (DCITP), Linthicum, MD-2000.
- Introduction to Networks and Computer Hardware (INCH)-DCITP, Linthicum, MD-2000.
- Network Intrusion Analysis Course (NIAC)-DCITP, Linthicum, MD-2001.
- Computer Investigations for Special Agents (CICSA)-Department of the Army-2001.
- Basic Evidence Recovery Techniques (BERT)-DCITP, Linthicum, MD- 2002.
- Basic Forensic Examiner Course (BFE)-DCITP-Linthicum, MD-2002.
- Forensics in a Solaris Environment (FISE)-DCITP-Linthicum, MD-2002.
- SANS-Tracking Hackers/Honey pots-SANS Institute, Dupont Circle, DC-2003.
- Encase Intermediate Analysis and Reporting-Guidance Software, Sterling VA-2004.
- PDA and Cell Phone Seizure and Analysis-Paraben Software, Orlando FL-2005
- Network Monitoring Course (NMC)-DCITP- Linthicum, MD-2005
- Encase Advanced Internet Examinations-Guidance Software, Los Angeles CA-2006
- (FTK) Windows Forensics-AccessData, Dallas TX-2006
- (DNA) Applied Decryption-AccessData, Nashville TN, 2007
- Network Intrusion Course-Guidance Software, Houston, TX, 2010
- SANS-Hacker Techniques, Exploits, and Incident Handling, San Francisco, CA, 2011