IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

Microsoft Corporation, a Washington State Corporation and LF Projects, LLC, a Delaware State Series Limited Liability Company, Plaintiffs, v. Abanoub Nady (also known as MRxC0DER), and John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

COMPLAINT

Plaintiffs Microsoft Corporation ("Microsoft") and LF Projects, LLC ("LF Projects"), by their attorneys, brings this action against Abanoub Nady (also known as MRxC0DER) and John Does 1-4 (collectively "Fake ONNX Defendants" and formerly known as "Caffeine"), who manufacture and sell illegal phishing kits, deceptively branded as "ONNX," designed to steal sensitive information and perpetrate business email compromise, ransomware, and financial fraud against Microsoft customers. 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 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 that they rely on 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 confidential information in order to commit further cybercrimes.

2. This action involves the relentless and persistent phishing attacks conducted and facilitated by a foreign cybercrime organization designated as "Fake ONNX Defendants," against Microsoft and its customers, including LF Projects, seeking to steal personal and business information for use in perpetrating 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.[1] Fake ONNX 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. This 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, customer support features designed to evade detection and lead

[1] 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*").

victims to believe they are dealing with legitimate products. The kits are essentially "how to" manuals for cybercriminals to develop and execute attacks on email systems through phishing campaigns. The Fake ONNX Defendants offer phishing kits designed to target a variety of companies across the technology sector, including Google, DropBox, Rackspace, and Microsoft. A cybercriminal can purchase the phishing kit that best serves their criminal objective, including selecting which companies' products and systems they wish to infiltrate. This action brought by Microsoft and LF Projects focuses on the ONNX-branded phishing kits that are used to target Microsoft's systems, products, and users.

4. These phishing kits are particularly pernicious 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 and affirmatively circumvent the security features of Microsoft products 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.

5. PhaaS lowers the barrier to entry for cybercrime, allowing even novices to launch effective phishing attacks. This model has proven lucrative, as it enables widespread phishing activities without requiring users to possess extensive technical skills. The ease of use and availability of these services make it an attractive option for would-be cybercriminals. The Fake ONNX Defendants' "phishing operation" provides the gateway and know-how for would-be cyber criminals to attack Microsoft customers and steal their personal and confidential business information. Indeed, Microsoft, without disclosing its identity, recently conducted a "test buy" of Fake ONNX Defendants' phishing kit. Microsoft was able to procure the kit complete with

instructions on how to target Microsoft customers, avoid detection, and become part of Fake ONNX Defendants' vast phishing infrastructure.

6. To support this phishing operation, Fake ONNX Defendants have established and operate an infrastructure of websites, domains, and computers on the Internet, which they use to target their victims, compromise the security of their networks, and steal information from them. The identity of the website domains used by Fake ONNX Defendants to support their phishing operation are set forth at **Appendix A** to this Complaint and comprise their technical infrastructure.

7. To carry out their criminal operation, the ONNX Defendants illegally use the trademarks and logos of the Plaintiffs -- Microsoft and LF Projects. LF Projects owns the trademarks for the Open Neural Network Exchange, or "ONNX" (herein referred to as the "ONNX Exchange").[2] ONNX is a well-known ecosystem of technology companies that has spent considerable time and resources building goodwill and a trusted brand. The Fake ONNX Defendants have illegally adopted the "ONNX" name and logo to carry out phishing activities by exploiting the trust associated with the "ONNX" brand. They deceive users by sending phishing emails that appear to come from trusted sources, such as Microsoft, complete with Microsoft's logos and branding. By doing so, Fake ONNX Defendants lure unsuspecting victims into believing the phishing emails and websites linked to in the emails are legitimate. Victims are wrongly induced to enter credential information, which is captured by Fake ONNX Defendants, on websites they control. To make matters worse, these phishing kits include features that bypass technical security measures implemented by Microsoft.

---

[2] For the purposes of this filing, references to "ONNX Exchange" is a reference to Plaintiff LF Projects, LLC. "ONNX Exchange" is used to bring clarity as to the specific harm Fraudulent ONNX Defendants are causing given the confusion in the use of the name "ONNX" and its improper association with the legitimate ONNX Exchange project.

8. Fake ONNX Defendants have caused and continue to cause irreparable injury, to Microsoft, its customers, LF Projects, and the public. Plaintiffs seek injunctive relief to take down the infrastructure developed and used by the ONNX Defendants to perpetrate their crimes and other equitable relief and damages against Fake ONNX Defendants.

PARTIES

9. 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.

10. LF Projects, LLC, is series limited liability company duly organized and existing under the laws of the state of Delaware, having its principal place of business in Wilmington, Delaware.

11. Upon information and belief, Defendant Abanoub Nady (also known as MRxC0DER), is an individual residing in Egypt, who is involved in the creation of the ONNX-branded phishing kits and controls the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, the ONNX Exchange, and the public.

12. Prior to January 2024, Fake ONNX Defendants conducted their criminal operation using the name "Caffeine." In 2024, Fake ONNX was considered to the most prolific phishing kit by volume of attacks, with 16.8 million phishing messages observed since December 2023.

13. Upon information and belief, Defendant John Doe 1 controls the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, the ONNX Exchange, 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**.

14. Upon information and belief, Defendant John Doe 2 provides technical support for the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, the ONNX Exchange, 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**.

15. Upon information and belief, Defendant John Doe 3 is a cybercriminal, who purchased the ONNX-branded phishing kit, registered a new phishing domain, and incorporated that phishing domain into the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, the ONNX Exchange, 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**.

16. Upon information and belief, Defendant John Doe 4 is a cybercriminal, who used an existing phishing domain that is already connected to an ONNX-branded phishing kit, and has been incorporated into the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, the ONNX Exchange, 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**.

17. Third party VeriSign Global Registry Services ("VeriSign") is the domain name registry that oversees the registration of all domain names ending in ".com," ".cc," and ".net" and is located at 12061 Bluemont Way, Reston, Virginia 20190. As set forth in **Appendix A**, the Fake ONNX Defendants use ".com", ".cc," and ".net" domains in connection with their spear phishing

operation. Third-party Registry Services, LLC is the domain name registry that oversees the registration of all domain names ending in ".biz," ".us," and ".vip" and is located at 100 S. Mill Ave, Suite 1600, Tempe, AZ 85281. As set forth in **Appendix A**, the Fake ONNX Defendants use ".biz," ".us," and ".vip" domains in connection with their spear phishing operation. Third-party Identity Digital Limited is the domain name registry that oversees the registration of all domain names ending in ".life," ".live," and ".pro" and is located at 10500 NE 8th Street, Suite 750, Bellevue, WA 98004. As set forth in **Appendix A**, the Fake ONNX Defendants use ".life," ".live," and ".pro" domains in connection with their spear phishing operation. Third-party XYZ.COM LLC is the domain name registry that oversees the registration of all domain names ending in ".lol" and ".xyz" and is located at 2121 E Tropicana Ave, Suite 2, Las Vegas, NV 89119. As set forth in **Appendix A**, the Fake ONNX Defendants use ".lol" and ".xyz" domains in connection with their spear phishing operation. 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, VA 20190. As set forth in **Appendix A**, the Fake ONNX Defendants use ".org" domains in connection with their spear phishing operation.

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

19. Upon information and belief, Abanoub Nady 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 ONNX-branded phishing kits. Plaintiffs will endeavor to amend this complaint to allege the Doe Defendants' true names and capacities when and if ascertained. Plaintiffs will exercise due diligence to determine Doe

Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

20. On information and belief, the actions and omissions alleged herein to have been undertaken by Abanoub Nady and John Does 1-4 were actions that the Fake ONNX Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Fake ONNX Defendants set forth below in that each Defendant had knowledge of those actions and omissions, aided and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Fake ONNX Defendants, and in engaging in the activities hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Fake ONNX Defendants.

JURISDICTION AND VENUE

21. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Fake ONNX 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 Conspiracy to Violate 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). The Court also has subject matter jurisdiction under 28 U.S.C. § 1367 for the trespass to chattels, conversion, and unjust enrichment claims.

22. 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 Fake ONNX Defendants has occurred in this judicial district. Fake ONNX Defendants maintain Internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and utilize instrumentalities located in Virginia and the Eastern District of Virginia to carry out acts alleged herein. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Fake ONNX Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Microsoft Services and Reputation

23. 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®.[3] 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

[3] Microsoft 365 is a product family of productivity software, collaboration and cloud-based services owned by Microsoft. Microsoft 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.

365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, Microsoft Exchange Server®, Teams®, Microsoft Defender®, Windows Vista®, Sway®, and Azure®. Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint.

24. LF Projects is a series limited liability company[4] organized under the laws of Delaware that establishes each "opens source project" as an individual series. LF Projects owns the registered trademarks associated with the open source projects in its series limited liability companies and licenses the marks to each respective series. LF Projects owns the trademarks for both the "ONNX" name and logo. These are linked to an LF Projects project known as the Open Neural Network Exchange, or "ONNX." The ONNX Exchange is an open-source artificial intelligence ecosystem of technology companies and research organizations that establishes open standards for representing machine learning algorithms and software tools to promote innovation and collaboration in the AI sector. The ONNX Exchange licenses the "ONNX" name and mark from LF Projects. A copy of the trademark registration for this trademark is attached as **Appendix C** to this Complaint.

What are the Fake ONNX Defendants?

25. Fake ONNX Defendants are prolific cyber criminals that manufacture and sell ONNX-branded phishing kits and also provide PhaaS to other cybercriminals, who purchase the ONNX-branded phishing kits from the Fake ONNX Defendants and launch phishing attacks against a multitude of organizations across various industries. Fake ONNX Defendants first

[4] A series limited liability company consists of a parent or umbrella LLC, with one of more sub-LLC, known as a "series" that branch off from it. Each series is considered a separate corporate entity, The Manager of a Series LLC has the authority to create the series. *See* Forbes, *What is A Series LLC? Everything You Need To Know*, FORBES ADVISOR, available at https://www.forbes.com/advisor/business/what-is-series-llc/ (Jun. 1, 2024).

emerged in October 2017, under the brand name "bl4ck-tools-net." From 2017 to 2020, Abanoub Nady used various branding in connection with his phishing kits. In 2020, the phishing kit was distributed under the branding "Caffeine," which was used for several years. Subsequently, in 2024, the Defendants transitioned to the brand "ONNX." Defendants' use of the ONNX mark is false, deceptive and unauthorized. **Figure 1** demonstrates a timeline of the various names under which Defendants have advertised, sold, or distributed their phishing kits.

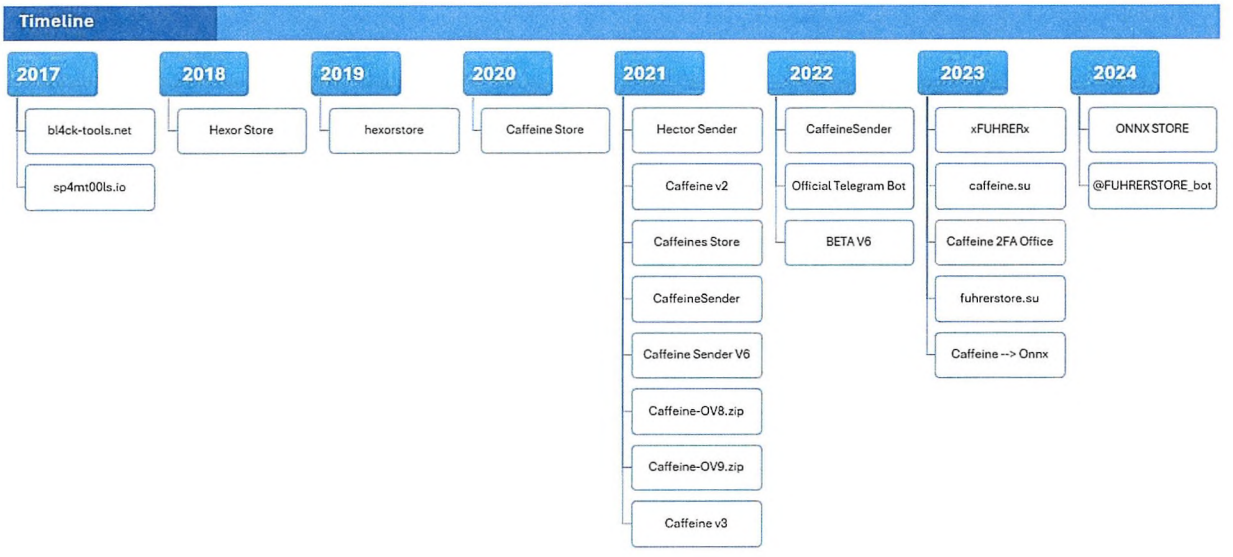


Figure 1

26. The phishing operation is carried out by Abanoub Nady and John Does 1-4.

27. The handle "MRxC0DER" is known as an administrator of the Fake ONNX Defendants' phishing operation. **See Figure 2**. Microsoft was able to attribute the MRxC0DER username to Defendant Abanoub Nady through their investigation into the Fake ONNX Defendants. Moreover, on or around June 2024, security threat researchers published an article

which connected MRxC0DER to be Defendant Abanoub Nady.[5] This third-party, independent publication confirmed Microsoft's attribution.

Figure 2

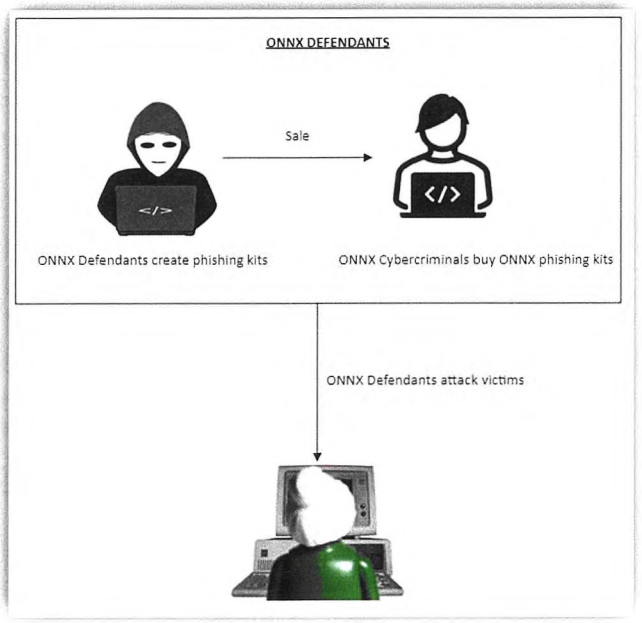
28. In addition to causing significant harm to its phishing victims, Fake ONNX Defendants appear to have also stolen their name and logo from an unrelated and innocent third-party: the ONNX Exchange. **See Figure 3**.

Figure 3

[5] Identity Reveal: The Threat Actor Behind ONNX Store and Caffeine Phishing Kit, https://darkatlas.io/blog/identity-reveal-the-threat-actor-behind-onnx-store-and-caffeine-phishing-kit.

Fake ONNX Defendants' *Modus Operandi*

29. Much like how companies develop and sell all-in-one do-it-yourself kits to normal customers for personal projects, Fake ONNX Defendants develop phishing kits for cybercriminals to purchase and use for their cybercrime operations. These cybercriminals become part of the Fake



ONNX Defendants' operations when they, in turn, deploy the ONNX-branded phishing kits to conduct AiTM activities[6] by positioning themselves between communications directed to and from Microsoft customers. **Figure 4** is a visual depiction of how cybercriminals become Fake ONNX Defendants as they collaborate to engage in phishing attacks against a victim.

Figure 4

[6] The ONNX-branded phishing kit allows cyber criminals to infiltrate the systems of Microsoft customers undetected and collect the user names 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.

30. Phishing is the fraudulent practice of sending emails or other messages purporting to be from legitimate senders in order 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"). Fake ONNX Defendants develop and sell ONNX-branded phishing kits that are customized 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.[7]

31. Fake ONNX Defendants' phishing kits are specifically developed to target Microsoft 365 and Azure users, and include two-factor (2FA) authentication[8] bypass features for the Microsoft Authenticator[9] 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. Fake ONNX Defendants are able to execute these end-user terminal attacks more readily when they are able to access a victim's Microsoft 365 or Azure cloud platform, which serves as gateway to other computer applications, and where these applications are connected by

---

[7] Fake ONNX Defendants customize their phishing kits to infiltrate the systems of particular companies. In addition to having Microsoft-focused phishing kits, Fake ONNX Defendants also sell phishing kits that can attack Google, Dropbox, and Rackspace.

[8] 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.

[9] 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.

a global Microsoft network infrastructure. These features are the "selling points" of the phishing kits, and Fake ONNX Defendants advertises the kits' abilities to break into Microsoft systems.

32. Once a kit is purchased, cybercriminals can conduct their own phishing attacks using the templates provided in the phishing kits and using either the domains that are provided with the kits or the ones that the downstream cybercriminal purchases and connects to the overall technical infrastructure. By connecting purchased domains to the infrastructure that is overseen and administered by the Fake ONNX Defendants, the phishing operation is able to grow and scale. The Fake ONNX Defendants have built a technical infrastructure of hundreds of website domains that are connected together by the steps the Fake ONNX Defendants take once they have registered the domain. These website domains are identified in **Appendix A** to the Complaint. This action seeks to takedown this technical infrastructure to render Fake ONNX Defendants incapable of continuing their attacks and transferring ownership and control of these domains to Microsoft.

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

34. In addition to standard email phishing, Fake ONNX Defendants also engage in QR code phishing or "quishing."[10] This is a relatively new tactic used by cybercriminals. Since last year, Microsoft has observed a significant increase in phishing using QR codes by cybercriminals generally. [11] A quishing attack involves a cybercriminal sending a phishing message containing a

---

[10] FINRA, *FINRA Cyber Alert – ONNX Store Purpotedly Targeting Firms in Quishing Attacks*, available at https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-onnx-store-purportedly-targeting-firms-quishing-attacks (last accessed Oct. 27, 2024).
[11] *See* 2024 *MDDR* at p. 34.

QR code encoded with a URL. The victim is prompted to scan the QR code and then they are redirected to a fake login page, where they are tricked into providing credentials. This demonstrates Fake ONNX Defendants technical sophistication and their ability to adapt to new methodologies of committing cybercrime.

Development and Sale of ONNX-Branded Phishing Kits

35. 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. When 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 if it uses domain names that at a glance to the victim, are familiar, such as 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.m1crosoft.com, where a letter is missing or a number is in place of a letter. As a result, the phishing domain may easily be misperceived as the authentic domain. When a phishing victim is deceived to visit a website to enter their credentials, Fake ONNX Defendants lie in wait to collect those credentials in order to subsequently access their accounts to further their cybercrime.

36. Understanding the critical elements to make a phishing attack a success, Fake ONNX Defendants, including Abanoub Nady (MRxC0DER), design and develop the ONNX-branded phishing kits with features to facilitate the deception. For example, Fake ONNX Defendants' phishing kit, "Office 2FA Cookie Stealer" includes features like auto capture that permit these criminals to intercept the transmission of a victim's two-factor authentication (2FA) code used to confirm a victim's identity, then automatically grabs the victim's credentials. Fake

ONNX Defendants also include in the phishing kit the ability to customize logos and email templates to appear authentic. **See Figure 5**.

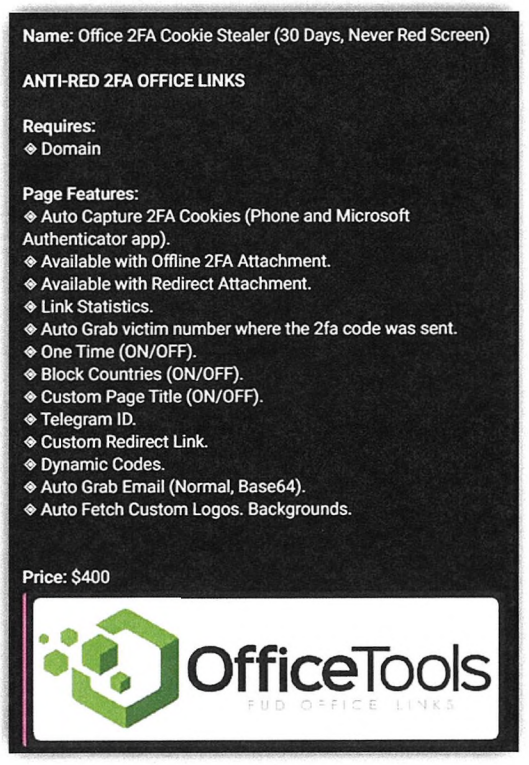


Figure 5

37. Much like how an e-commerce business sells their products in online stores for consumers to purchase, Fake ONNX Defendants sell their ONNX-branded phishing kits at the "ONNX Store" (formerly known as the "Caffeine Store") for cybercriminals to purchase. **See Figure 6**.

Figure 6

38. 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 Fake ONNX Defendants. **See Figures 7-9**. Fake ONNX Defendants also use media platforms such as YouTube to provide guidance on the purchase and implementation of these phishing kits.

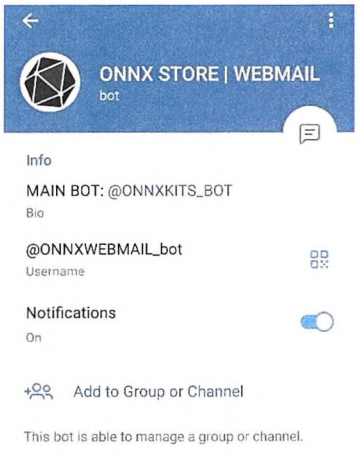


Figure 7

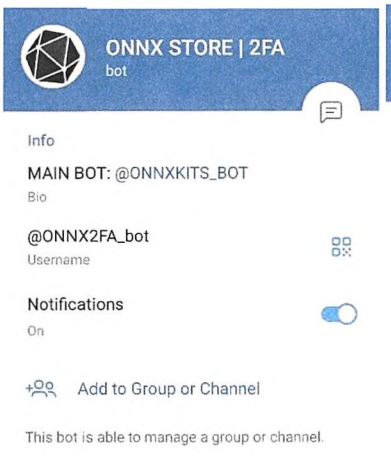


Figure 8

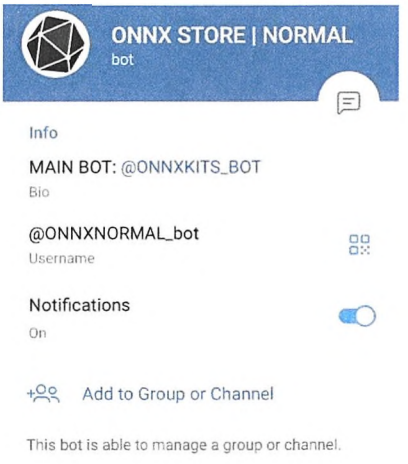


Figure 9

39. Furthermore, Defendant Abanoub Nady, who is known to use the online handle, MRxC0DER, advertises Fake ONNX Defendants' phishing kits on Telegram. **See Figure 10**.

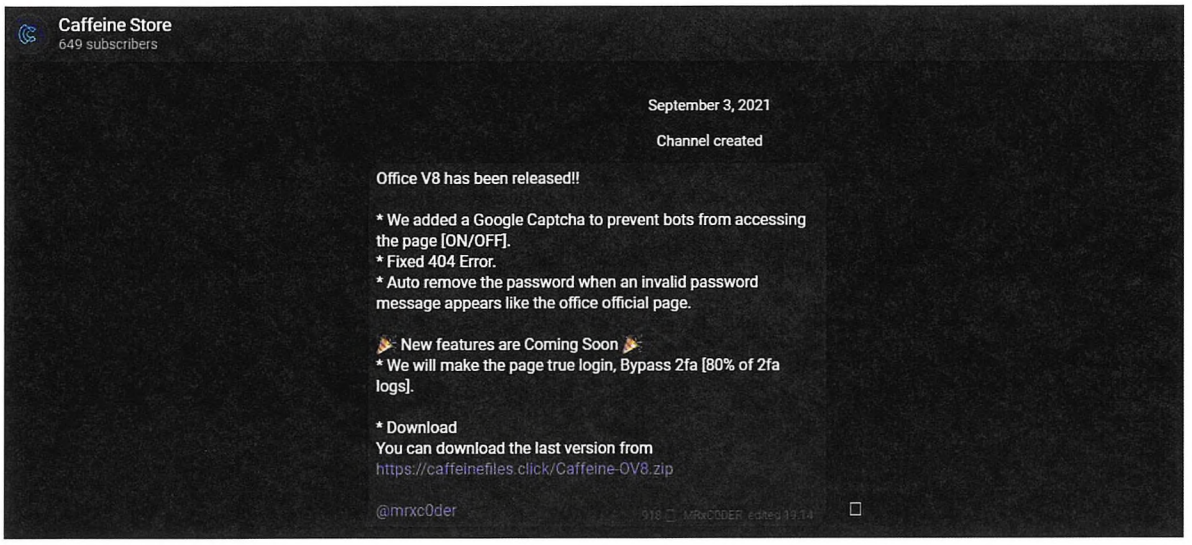


Figure 10

40. In April 2024, DCU conducted a test buy of the ONNX-branded phishing kits, which allowed DCU investigators to observe first-hand how Fake ONNX Defendants operate their telegram store, the information a purchaser is provided, and the instructions given by Fake ONNX Defendants to connect the domains into the technical infrastructure. As part of this test buy, the DCU investigator began communicating with Fake ONNX Defendants on Telegram and expressed interest in purchasing an ONNX-branded phishing kit. He was provided with payment information and successfully purchased a phishing kit. Once he purchased the phishing kit, Fake ONNX 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 Fake ONNX Defendants' phishing operation.

41. In addition to Fake ONNX Defendants purposefully selling their malicious products for use by cybercriminals, they take steps to ensure their products' repeated use. Fake ONNX Defendants offer a subscription plan to gain access to the phishing kits – Basic is 1-month access, Professional is 3-month access, and Enterprise is 6-month access. **See Figure 11**. Fake

ONNX Defendants also provides "Unlimited Support" for the Basic and Professional subscriptions. For those with a more significant cybercriminal need at the Enterprise level, "Unlimited VIP Support" is provided. Furthermore, Fake ONNX Defendants knowingly work to circumvent detection of their phishing operation by highlighting as a feature of their malicious subscription plans, the undetectable nature of their product and for the Enterprise level, the use of an anti-bot[12] application programming interface (API).[13] An anti-bot API is like a security guard at a building who checks if someone entering is a real person or a robot. Fake ONNX Defendants created a phishing kit that "hires a security guard" for their websites to prevent bots from scanning or checking their site and revealing their true identity and purpose. In this instance, Fake ONNX Defendants implement an anti-bot API to block email security programs from determining whether emails from Fake ONNX Defendants contain malicious content or links to malicious websites. This allows the Fake ONNX Defendants to bypass security tools on victim computers.

[12] A bot is a computer program that runs tasks without human intervention.
[13] An API helps two programs or systems talk to each other without the user needing to know how everything works behind the scenes. It is a way for one application to request services or data from another application.

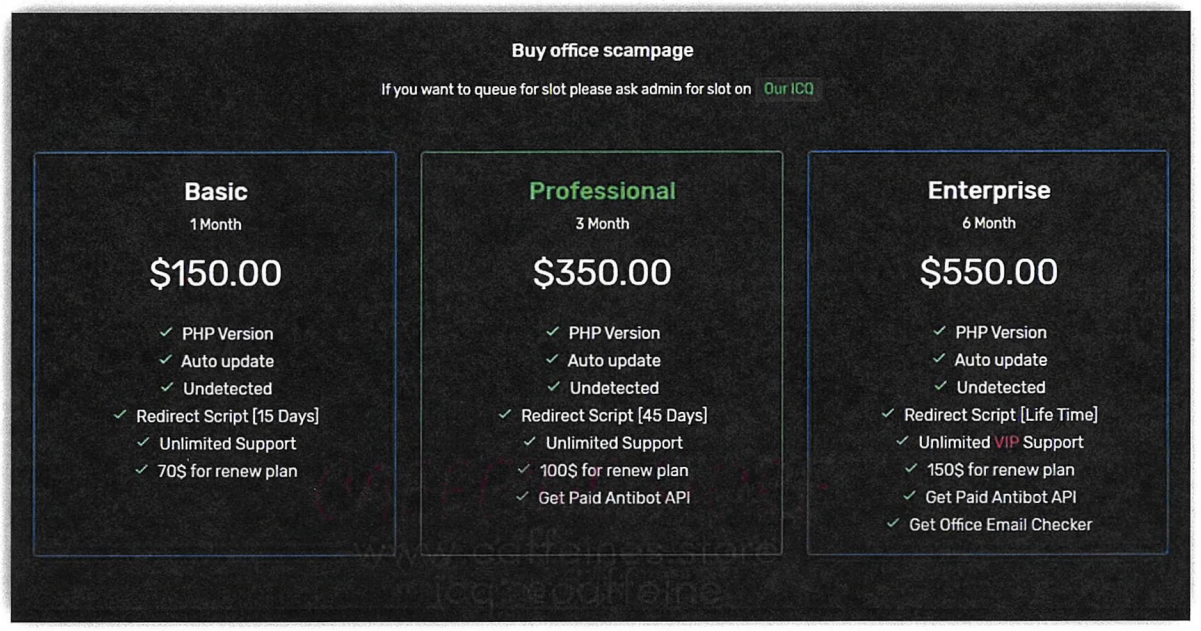


Figure 11

Activation of ONNX-Branded Phishing Kits and Malicious Domains

42. Once Fake ONNX Defendants sell an ONNX-branded phishing kit to cybercriminals,[14] several actions must happen in order to activate the phishing kit and incorporate a phishing domain into the operation controlled by Fake ONNX Defendants: (i) cybercriminals must purchase a domain to be used for the phishing operation, (ii) the cybercriminal must follow the step to resolve the domain to Cloudflare and use other Cloudflare services to further avoid detection, and (iii) the cybercriminals' phishing domain must be connected to the phishing operation which then becomes part of the entire technical infrastructure controlled by Fake ONNX Defendants. This process is described in **Figure 12**.

[14] Cybercriminal customers are John Doe 3-4 once they have purchased an ONNX-branded phishing kit from Fraudulent ONNX Defendants.

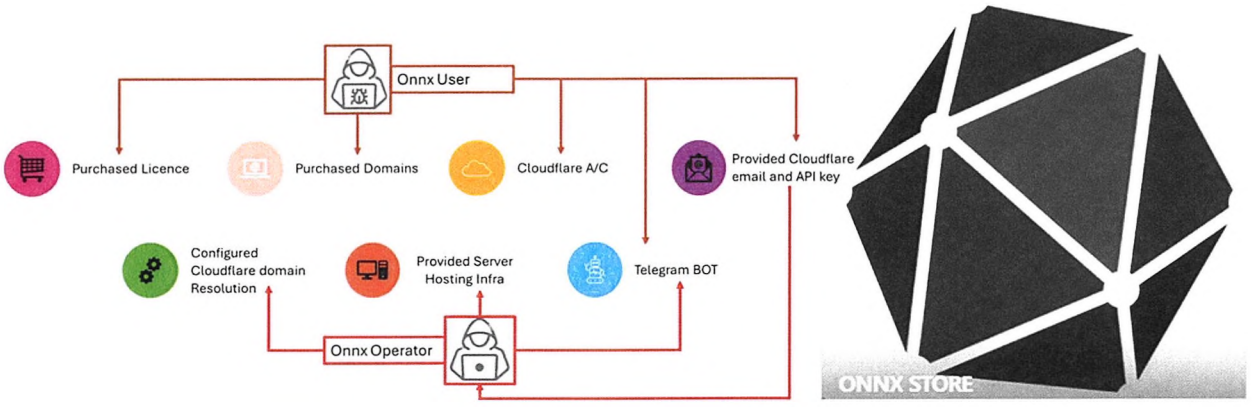


Figure 12

Purchasing a domain.

43. 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.[15] These cybercriminals then "bring their own domain" to the phishing operation controlled by Fake ONNX Defendants.[16]

44. 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) and includes impersonation of Microsoft brands to add legitimacy. **Figure 13** are domains listed in **Appendix A** that are part of Fake ONNX Defendants' phishing operation. Many of these domains 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

[15] 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.

[16] Previous iterations of the ONNX-branded phishing kits did not allow or require purchasers to utilize their own domains. However, in April 2024, purchasers and users of the kits were able to supply and connect their own domains to the criminal infrastructure. This made tracking of the domains and phishing activity attributable to a particular kit more difficult. *See* 2024 *MDDR* at p. 46.

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 Fake ONNX Defendants' deliberate effort to lure their victims into a false sense of security and deceive them into providing information that subsequently allows Fake ONNX Defendants to further their criminal activities.

0365-aut-hentication-service.com	login-outlook-livestreem.com	login-outlook-midstreamauth.com	outlook-live-authworkspace-organizationsigninge39f93meea.com
0365-docs-cument.com	login-outlookonline.com	msonlinemailencryption.com	outlook-live-barcode-workspace.com
0365expirationsonline.com	login-outlookonline-server.com	msonlinemailencryptions.com	outlook-loginsecurity.com
0365mailupdatesystem.com	login-outlook-stream.com	msquarantine.com	outlookoffice365.xyz
0365securedfile.com	login-outlook-streams.com	msquarantine.net	outlook-online-server.com
0ff356veriflogin.com	loginoutloo-verification-officee365.com	mssoftcloudportal.com	outlooksecurityonline.com
0ffice365mailupdatesystem.com	loginsharepoint.net	mssoftcloudportal-shared.com	outlookservers.com
0ffice-esign.com	loginsoutlookmidstreams.com	mstforeks.com	outlook-verify-office.com
0ffice-inboxcomowaokta876543213456789.com	login-stream-outlook.com	msviewing.com	outlook-verifyoffice-security-us.com
24teamssharingfile.com	login-streams-outlook.com	msxchangefiledocs.com	outlorklve.com
2fa-0ffice03protection-65auth.com	login-strems-outlook.com	myoffícesdocusviews.com	pdf-login-outlook.cc
2fa-auth-outlook.com	logínteams.com	myonenoteoutlook.live	portal-outlookredirecting365.com
365invoicespdf.com	logmicrosfocus.info	nmsn-accounts-serveraccess-user-access-onmsn.com	secure-2fa-outlook.com
365protection-stats.com	mailaccountvalidationmicrostmail.com	o365authenticator.com	secure-microservices.com
access-sharepointonline-us.com	mail-office365.com	o365-doc-uments.com	secureoutlookverify.com
access-sharepointonline-usa.net	mauteníicator-365.com	off356reviewdocs.com	securesharepointprotection.xyz
app-office0365voicemail-protection.com	mfa-auth-outlook.com	off356reviewdocu.com	servr-0365-protection.com
app-office03auth-65protection.com	micfst.com	off356reviewsign.com	servr-office365check.com
app-office03auth-65protections.com	miclosoft.us	office.net	servr-office365nauth.com
app-office03auth-65protections.org	mico-soft.com	office356doc.com	sharepiont-docs.com
app-office03voice-65protections.com	micr0s1inediveee.com	office356reviewdoc.com	sharepointauth.com
app-office03voicemail-protection.com	micr0softsharepo1nt.com	office360authclearance.com	sharepoint-datacloud.com
app-office03voicemail-protections.com	microdefenderdesk.com	office360dropboxlivemail.com	sharepointfilesonline.com
app-office06voicemail-protections.com	microdoc-exchange.com	office360dropboxlivemail1.com	sharepoint-investorcloud.com
auth-365protection.com	microdocs-exchange.com	office360livemail.live	sharepoint-investorscloud.com
authkeystreamoutlook.com	microofficensdkdjosdbfihlakndaldnadknaidno.com	office36503.com	sharepointonliine.com
authmicro.com	microofficesoft.com	office365doc.com	sharepointonlinedoc.com
auth-onedriveverificationapp.biz	microscofield.info	office365log.com	sharepointonline-microsoft.com
authorize-l0gin0365.com	microshareviews.com	office365ppshare.com	sharepointproposal.com
auth-outlook.com	microsofttonline.lol	office365reviewdocs.com	sharepointproposal.net
auth-protection365.com	microsofiiti.com	officeauthmicrpdfreciept.com	sharepointproposals.com
auth-protection365office.com	microsoftofficials.org	office-authmlimwdfdolkcxfbtsalhhfdfdorikcxauthdietetoutloe.com	sharepointscloud.com
azureendpoint.com	microsoftstonline.com	officeazure365.com	sharepointsproposal.com
captiveresourcesharepoint.com	microsoft365datacenter.com	officecheckduclud.com	sharepointsproposal.net
cloudmicrosoftoffice365.com	microsoft675.com	office-depots.com	sharepointzip.com
cloudoffice365pro.com	microsoftauthserverboc3online.info	officeducloud.com	sharepointonedrive.com
cloudsharepointauth.com	microsoft-free.live	office-encryptedfile.com	sharpointaccountingpackiic.com
confirm-outlook.com	microsoftpadlet.com	office-file.info	sharpointaccountingpackic.com
connectingteamsfolder.com	microsoftsfilessharing.com	office-hdfdwhichauth620kea79uehg.com	sharpoint-docus.com
countysharepoint.com	microsworksfilemwf.com	office-mailhfnnskworauthdwefmsh.com	shrepointupdates-microsoft.com
docu-ment-0365review.com	micr-sftonline.xyz	office-msxchangesx.com	stream-outlook-login.com
documentmicroffi36work.us	micrsharefileview.com	office-outlook-verify.com	streams-outlook-login.com
doc-ument-o365view.com	micrsharepoint.com	officeredirecting365.com	sway-financegroup.com
docu-ments0365review.com	micrshareview.com	office-redirecting365.com	teams-cloud.com
documents-management365.com	micrst020o3soft.live	office-run.info	tu-office03auth-65protection.com
docu-sharepiont.com	micsoftauthentprocesssignin2proceed.com	office-supportadmin.com	tw-00authoffice-protection365.com
docushare-sharepoint.info	micr-sftolonine.xyz	office-to-pdf-file.us	tw-00-authy-officeprotection365.com
docxservice110365.com	miscftoline.org	office-tw-auth-0365-protection.com	tw-00officeauth-protection365.com
gesa-sharepoint.com	mmicrosmwnsadmin1hmmailoda4mailauth.com	office-voice-recordings.pro	tw-microsoftsharepointauthy-protection.com
ipm-sharepoint.com	mmicrosmwnsadmin1hmmailwfkltservercwnwm4oda4mailauth.com	office-whctklbfqsmxrv.com	tw-office036auth-5protection.com
livelogInmicrosoft.com	mrsft-protecteddocs.com	oficep360.life	tw-office03auth-65protection.com
login0365organizationsigning.com	msdocvieeewlvce.com	onedriveadobesafty.com	tw-office03auth-65protections.com
login036ssolutions.com	msdriveproposal.com	onedrivebusiness.info	tw-office03auth-65protections.net
login-faxplus-outlook.com	msdriveproposal.net	onedrivedocmee.com	tw-office03protection-65auth.com
loginmicrosof0nline.com	msenterprisesignonline.com	onedrive-docsend.com	tw-officeauth-365-protection.com
loginmicrosoftonline.com	msft-encryptedfile.com	onedrive-document.com	uwm-onedrive.com
login-midstream-outlook.com	msft-encryptfile.com	onedrivepdf.com	veri356signing.com
login-midstreams-outlook.us	msnote365.com	onedriveprotected09876543456789087.com	verificationoutlook365s.com
login-ms-outlook.com	msnviewing.com	onedrive-wetransfer.com	verify-2fa-outlook.com
loginoffce.com	msofficesharedfiles.com	oneilgroupsharepoint.com	verify-office-outlook.com
login-office0-365auth.com	msoftsecurity.us	onmsoft.org	verifysecurityoutlook.com
login-office365.org	msoftshare1.com	outbound-corporate-server-officemail-onmsn.com	verify-securityoutlook.com
login-ofice-files.vip	msoftshareonedriive.com	outloko-oficeo365o20.com	verifysharepointfi1es.us
login-ofiice-outlook.com	msoftshareonedrive.com	outlook365-online-login.com	verify-signinoutlexchangeadmin.com
login-online-outlook365.com	msoftstorage.com	outlook-live-authentitciteiwork.com	viewmicroosoft.com
login-outlook365-microsoft.com	msonlineencrypt.com	outlook-live-authentitciteworkspaces.com	vistawindowsvtah.com
login-outlook-filestreamskey.net	msonlineencryption.com	outlook-live-authentitciteworkzones.com	voicemaile0365.com
login-outlook-liveauth.com	msonlineencryptmail.com	outlook-live-authworkspace.com	windowhistorytools.com
login-outlook-livestream.com	msonlineencryptmessage.com	outlook-live-authworkspace-1s903a.com	

Figure 13

Use infrastructure to evade detection and delay takedowns.

45. Fake ONNX Defendants direct cybercriminals to create accounts on Cloudflare, Inc. ("Cloudflare") to evade detection and delay takedowns of the phishing domains. Cloudflare

is a company that provides a variety of legitimate network services and security features to protect websites from various online cyberthreats. Some of Cloudflare's services include IP proxying[17] and a CAPTCHA[18] 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 Fake ONNX Defendants have exploited this proxy feature to conceal their "home address" (their real IP address). So, for example, if law enforcement is trying to locate the actual "home address" of Fake ONNX Defendants' domains, that address is hidden by IP proxying and the only "address" they will obtain is Cloudflare's "business address." This allows Fake ONNX 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, which is an automated program designed to act without human direction to automatically do specific tasks (like access a website). CAPTCHAs are designed to protect normal consumers. In this instance, Fake ONNX 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 Fake ONNX Defendants to prevent "police robots" (security tools on victim computers) to determine if their

---

[17] 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.

[18] 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.

domains are engaging in anything illegal (like functioning as a phishing website). Here, Fake ONNX Defendants use CAPTCHA to keep out security bots in order to prevent them from checking a website link in an email address to see if it is malicious. By eliminating the probability of being detected, Fake ONNX Defendants are able to deliver phishing emails to its victims without interference. **Figure 14** is a depiction of how the Fake ONNX Defendants use CAPTCHA in connection with their cybercriminal activities.

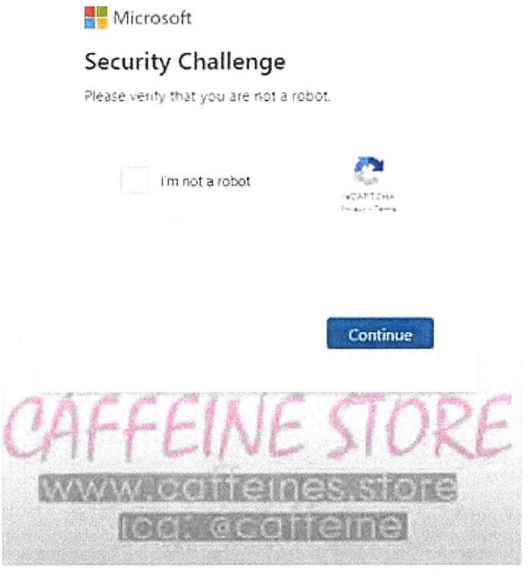


Figure 14

46. By using Cloudflare's services, Fake ONNX Defendants can obscure the real location of their phishing sites and employ measures like CAPTCHA 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 subsequently, shut down.

Connecting to the Fake ONNX Defendants' phishing operation.

47. Once the cybercriminals complete the domain's registration, Cloudflare provides an API key, which is a code used to identify and authenticate an application or user in Cloudflare. This API key also serves as a way to access the cybercriminals' Cloudflare account. The cybercriminals then provide this API key to the Fake ONNX Defendants, who then use the code to access the cybercriminals' Cloudflare account, and administratively connect on the back end, the cybercriminals' domain into the technical infrastructure. This step incorporates the cybercriminals' domain into the technical infrastructure controlled by Fake ONNX Defendants. Cybercriminals also benefit from this action by Fake ONNX Defendants because as an added "security feature," Fake ONNX Defendants have their own IP servers that can also act as another "IP proxy," creating another layer of obfuscation by masking the location of a domain. Rather than being able to find the "home address" (actual IP address) or even a "business address" (Cloudflare's IP address) of a cybercriminals' domain, Fake ONNX Defendants provide a "post office box address" (another IP address that Cloudflare can use) to create even more privacy layers to protect the real IP address associated with cybercriminals' domain. **Figure 15** is a visual depiction of the process.

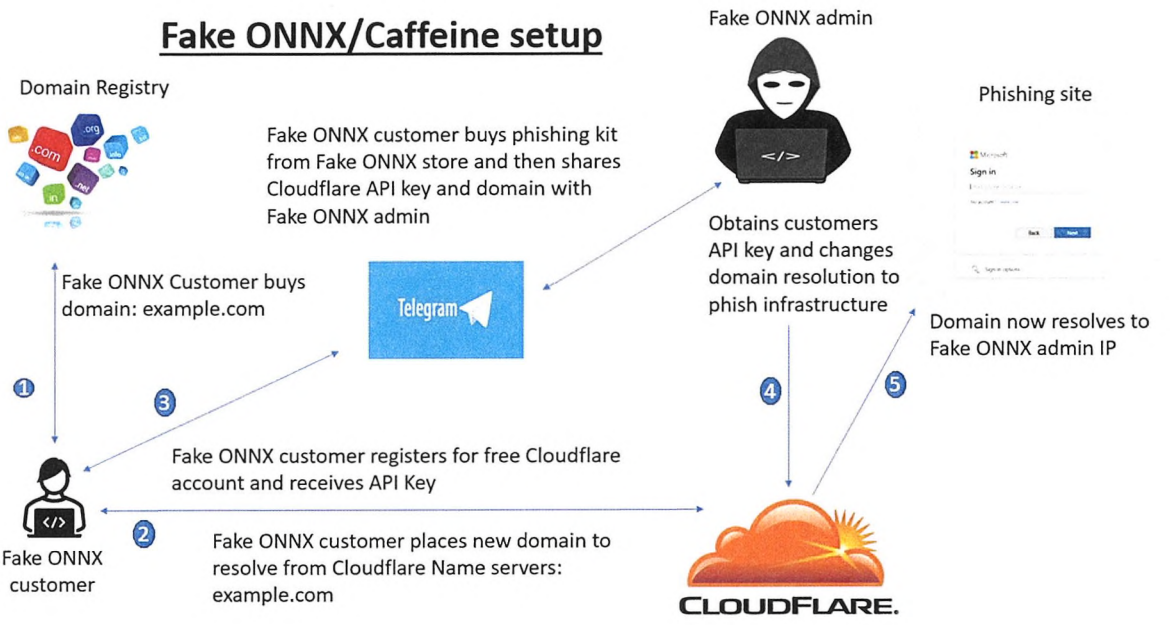


Figure 15

ONNX Attack Chain

48. Once the technical infrastructure is established, the next phase is the phishing attack deployed by Fake ONNX Defendants. Phishing emails are sent to victims that prompts the victim to click on a link connected to the domain brought into the Fake ONNX Defendants' technical infrastructure by the cybercriminals.

49. These phishing emails often use, without authorization, Microsoft's logos and format that would appear to the victim, as a legitimate website. **Figures 16 and 17** are examples of Fake ONNX Defendants' phishing email that fraudulently uses Microsoft's name and logo. "Support Server" as a sender lends additional legitimacy that the email sender has a reason to send such an email but at closer inspection, the email address is not from Microsoft, but rather, an unrelated email address created for the purpose of sending bulk phishing emails.

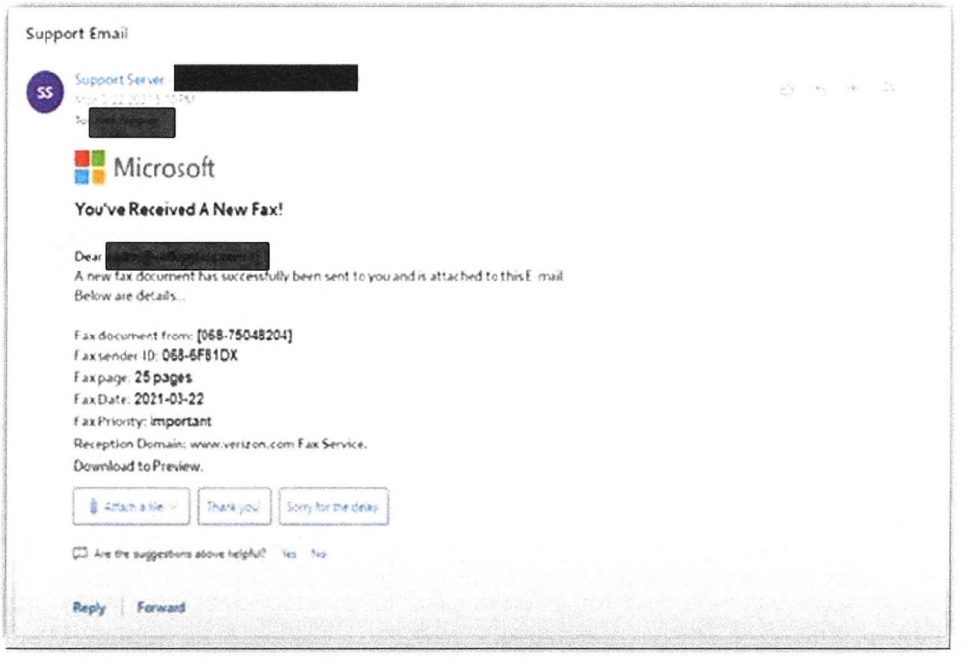


Figure 16

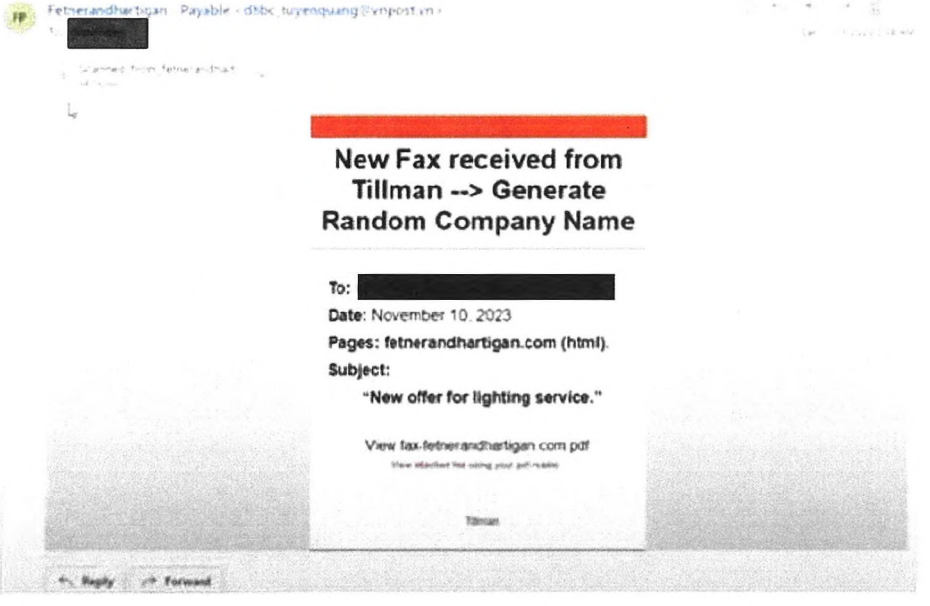


Figure 17

50. Once a victim clicks on the link, they are directed to an ostensibly legitimate Microsoft login page that asks for their credentials. 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 18** (verifying password) and **Figure 19** (completing the 2FA process). At this stage, the Fake ONNX Defendants have now captured the valid email address and credentials the victim used to log into their account. This is the crux of an AiTM attack, where the attacker establishes a permanent, but undetected presence in the victim's account with the ability to intercept communications.

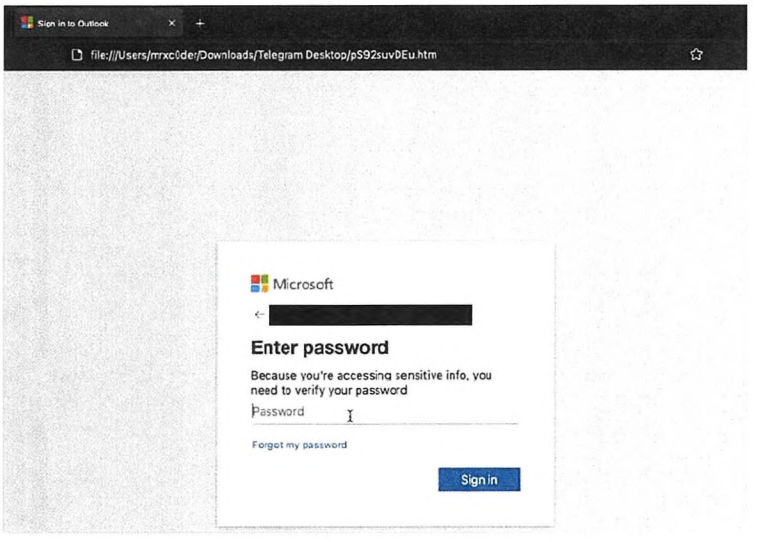


Figure 18

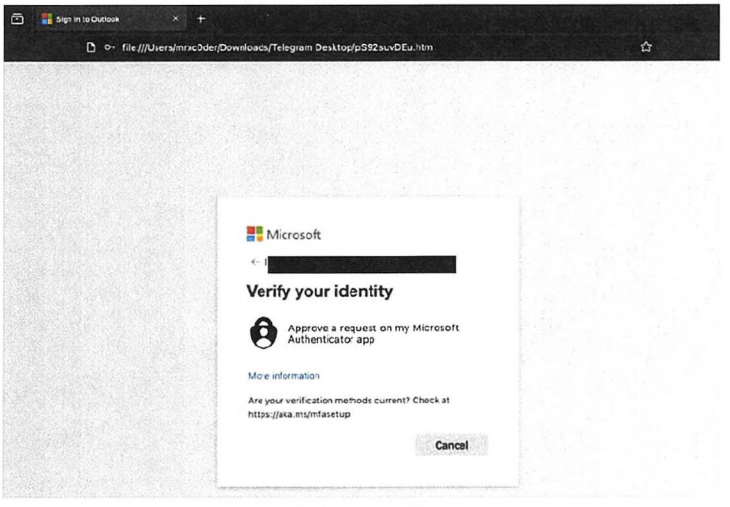


Figure 19

51. Fake ONNX Defendants prompt the victim to reset their password by directing them to provide their phone number where they may be able to receive their 2FA token[19] to verify their identity and access their account. Once the victim enters their authentication details, receives the 2FA token, and enters the token into Fake ONNX Defendants' fraudulent login page, their phone number and 2FA tokens are captured. **Figure 20** is an example of the fraudulent 2FA login page.

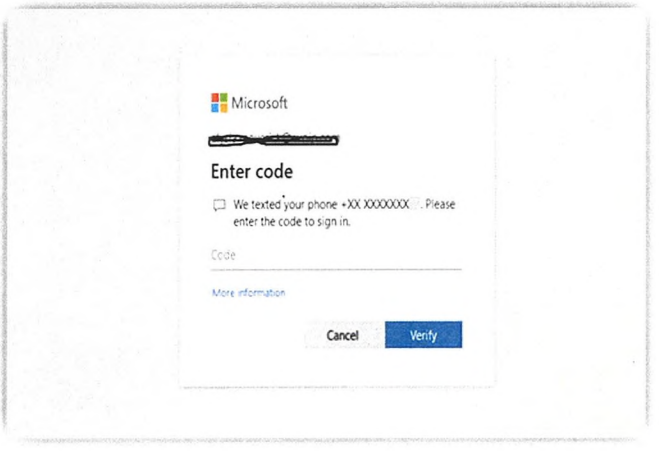


Figure 20

52. This verification then allows Fake ONNX Defendants' malicious website to be perceived by victims' devices as legitimate and any potential access to the site or communication to the victim may be fraudulently permitted. Fake ONNX Defendants subsequently exploit this access to their victim's devices to perpetrate further cybercrime such as ransomware, business email compromise, and financial fraud. See **Appendix D** which includes true and accurate media articles that detail the cybercrimes perpetrated by Fake ONNX Defendants.

[19] A token is a unique piece of data that contains information about a user's identity and the type of access they are authorized for. Tokens are generated by an authentication service and can be either digital or physical.

53. **Figure 21**, below is a visual representation of Fake ONNX Defendants' attack chain, as described in Paragraphs 29-52, *supra.*

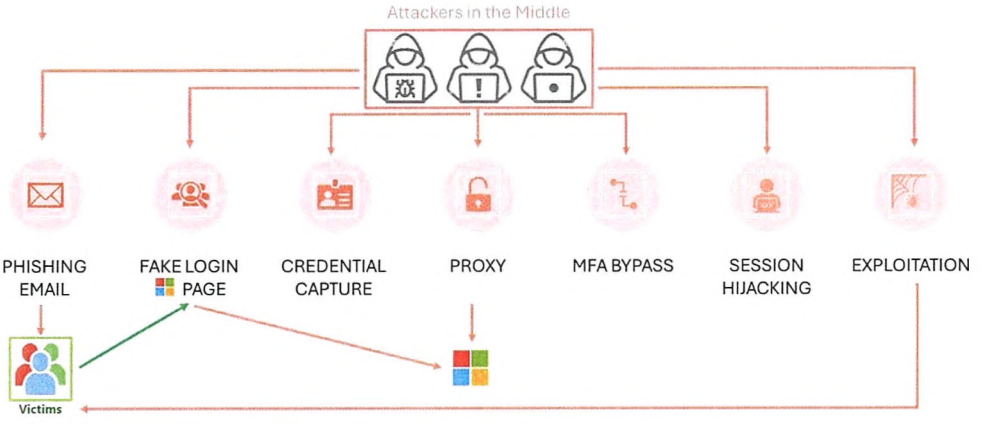


Figure 21

Fake ONNX Defendants Jointly Leverage the Racketeering Enterprise and Each Other's Works

54. Abanoub Nady 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").

55. The Racketeering Enterprise causes significant harm to Microsoft, its customers, the ONNX Exchange, and the public for the purpose of achieving significant monetary gain. The Fake ONNX 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, circumvention of technical security measures to gain access to victim computers and information, and the unauthorized use and dissemination of Plaintiffs' intellectual property.

56. The relationships among Fake ONNX Defendants allow them to collectively pursue the purpose of the Racketeering Enterprise. As **Chart 1** below demonstrates, Abanoub Nady 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 Fake ONNX Defendants leverage each other's work to: (i) create, distribute, and operate the phishing technical infrastructure, (ii) sell, distribute, and use ONNX-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 Fake ONNX 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.

FAKE ONNX DEFENDANTS	FUNCTION
Abanoub Nady	Develops the ONNX-branded phishing kit and controls the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure.
John Does 1	Controls the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure.
John Does 2	Provides technical support for the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure.
John Does 3	Cybercriminals who register a new phishing domain, purchase an ONNX-branded phishing kit, and incorporate the new phishing domain into the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure.
John Does 4	Cybercriminals who use an existing phishing domain that is already connected to an ONNX-branded phishing kit, and is already incorporated into the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure.

Chart 1. Fake ONNX Defendants Function Summary.

57. Upon information and belief, Abanoub Nady and John Does 1-2, the creators, sellers, and distributors of the ONNX-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.

58. Upon information and belief, John Does 3-4 are cybercriminals who (i) register new domains for the purpose of using them in the phishing operation, or (ii) use an existing domain that is already connected to an ONNX-branded phishing kit, and is already incorporated into the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure. This allows the prolific expansion of the Fake ONNX Defendants' phishing operation, which leads to the increase of downstream criminal activities including financial fraud, business email compromise, and ransomware attacks.

59. Plaintiffs' investigation reveals that Fake ONNX Defendants work together in a continuous and coordinated manner to develop, distribute, and use the ONNX-branded phishing kits, and operate the phishing operation and technical infrastructure.

60. The Racketeering Enterprise has continuously and effectively carried out its purpose of developing and operating a global technical infrastructure that facilitates phishing attacks that leads 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.

61. The relationship between the Fake ONNX Defendants is proven by: (i) development and repeated sale of the ONNX-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) Fake ONNX

Defendants' respective and interrelated roles in the sale, operation of, and profiting from the ONNX-branded phishing kits in furtherance of Fake ONNX Defendants' common financial interests.

62. Upon information and belief, Fake ONNX Defendants have conspired to, and have, knowingly with intent to defraud, facilitated phishing attacks against victims in order to steal credentials and gain unauthorized access to a victim's computer and have impersonated Plaintiffs 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 Plaintiffs' request for a temporary restraining order.

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

64. Upon information and belief, Fake ONNX 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.

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

Harm to Microsoft and Microsoft's Customers

66. Through research and investigation, Microsoft has determined that Fake ONNX Defendants used the domains identified in **Appendix A** to this Complaint in its technical infrastructure, and have actively and affirmatively targeted Microsoft customers in the United

States. The Fake ONNX Defendants sometimes disguise their technical infrastructure by incorporating into the names of its technical domains the names and trademarks of some well-known companies and organizations, including Microsoft.

67. For example, as seen in **Appendix A** to this Complaint, Fake ONNX Defendants have registered website domains that contain Microsoft's brands and trademarks as disguises. For example: loginmicrosoftonlline[.]com, micr0softsharepo1nt[.]com, office-outlook-verify[.]com, and sharepointonliine[.]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. Fake ONNX Defendants relies on the Microsoft brand and trademark to perpetrate its phishing and malware attacks. And, as shown in **Figure 18-20**, *supra* ¶ 50, the login page includes 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 and trustworthy, when in fact, it is malicious.

68. Microsoft determined that Fake ONNX Defendants also cause great harm to the company and its customers through the unauthorized access of the Microsoft 365 or Azure platform, which serves as a cloud platform that grants access to a victim's other computer applications and information. When the Fake ONNX Defendants access the Microsoft 365 or Azure platform, they are able to move through other computer applications and facilitate additional criminal activities like ransomware, financial fraud, and business email compromise.

69. Fake ONNX Defendants irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Fake ONNX Defendants' use 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 Fake ONNX Defendants impersonates

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.

70. Microsoft has invested considerable resources in developing high-quality products and services, including significant resources to combatting Fake ONNX Defendants and other cybersecurity threats. Microsoft spent at least $650,000 and 3,500 hours investigating and remediating Fake ONNX Defendants' activities, including engaging teams across four different countries. Through the development of flagship products used by millions of customers, Microsoft has thereby cultivated significant customer good will and globally-recognized trademarks. Trademark registrations for marks infringed by Fake ONNX Defendants are attached as **Appendix B**. A phishing attack where customers blame Microsoft involves a risk that customers may move from Microsoft's products and services because of the Fake ONNX Defendants and their activities.

71. 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.

Harm to LF Projects' ONNX Exchange

72. In addition to causing irreparable harm to its phishing victims, Fake ONNX Defendants have also stolen their name and logo from LF Projects' ONNX Exchange. The "ONNX" name and logo are registered by LF Projects. As seen in **Figure 3** above, ONNX Exchange and the ONNX-branded phishing kit share not only the same name, but also the same geometric shape as the logo. This causes significant confusion between Plaintiff LF Projects' ONNX Exchange and Fake ONNX Defendants' ONNX-branded phishing kits. The mere fact that

Plaintiffs had to create artificial names to describe Plaintiff LF Projects' Open Neural Network Exchange project and Fake ONNX Defendants to distinguish the parties establishes the very real likelihood of confusion.

73. In fact, through research and investigation, LF Projects has found that when searched online, the ONNX Exchange website (onnx.ai) and articles discussing the phishing activities perpetuated by Fake ONNX Defendants appear on the same results page, and make clear reference to the "ONNX" name. See **Figure 22** below.

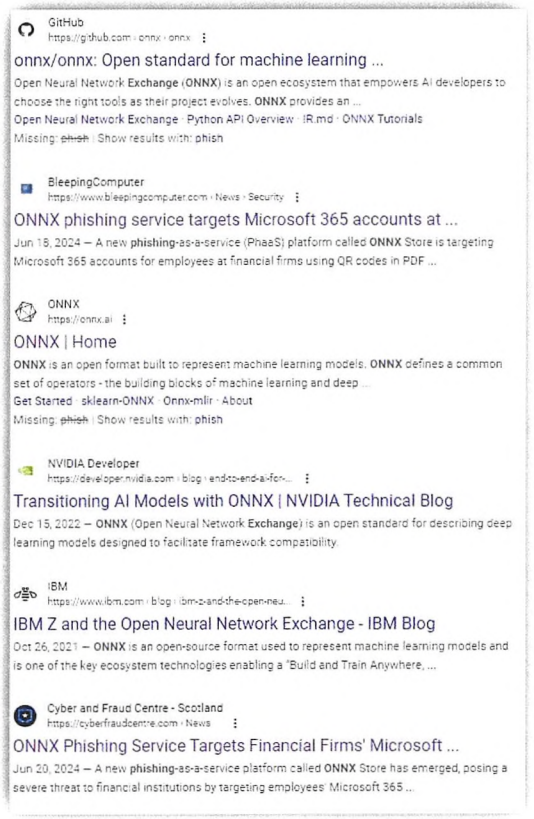


Figure 22

74. Fake ONNX Defendants irreparably harm LF Projects' goodwill by damaging its projects' reputation, brands, and partner goodwill. Fake ONNX Defendants' use of the "ONNX"

trademark leads to confusion as to the malicious phishing activities perpetrated by Fake ONNX Defendants, and may lead to attribution to the ONNX Exchange.

75. Many organizations, as seen in **Figure 23** below, create the community of the ONNX Exchange and malicious activities wrongly attributed to the ONNX Exchange would potentially implicate the community of organizations, and the goodwill cultivated through their cooperative efforts.

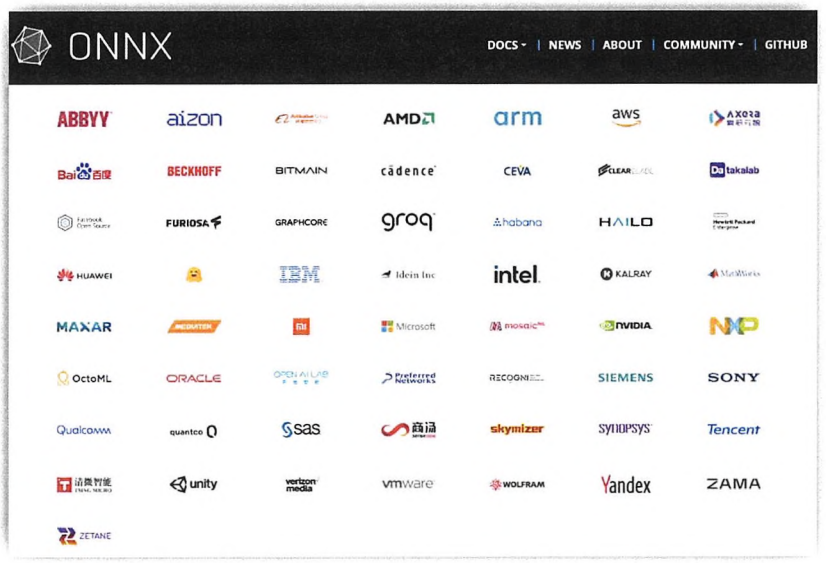


Figure 23

FIRST CLAIM FOR RELIEF

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

(Microsoft)

76. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 75 above.

77. Fake ONNX 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, and Microsoft.

78. Fake ONNX Defendants' conduct involved interstate and/or foreign communications.

79. Fake ONNX 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.

80. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

81. As a direct result of Fake ONNX Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Fake ONNX Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

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

(Microsoft and LF Projects)

82. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 81 above.

83. Beginning in 2020 (which is when Fake ONNX Defendants first began selling what is now being marketed as the ONNX-branded phishing kit as "Caffeine") and continuing up through the filing of this Complaint, Fake ONNX Defendants Abanoub Nady 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,

Fake ONNX 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.

84. Fake ONNX 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).

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

86. Fake ONNX 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 ONNX-branded phishing kits.

87. Fake ONNX 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.

88. Fake ONNX Defendants have knowingly and with intent to proliferate phishing kits used to steal, intercept and obtain credential information through access device (including credentials, 2FA tokens, and cookies) fraud, Microsoft customers by sending emails impersonating

Microsoft and its customers in order to lure victims to unknowingly providing login credentials to Fake ONNX Defendants, in violation of 18 U.S.C. § 1343.

89. Plaintiffs Microsoft and LF Projects have been and continues to be directly injured by Fake ONNX Defendants' conduct. But-for the alleged pattern of racketeering activity, Plaintiffs would not have incurred damages.

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

THIRD CLAIM FOR RELIEF

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

(Microsoft and LF Projects)

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

92. Beginning in or before 2017 (with respect to the first iteration of what is now being marketed as the ONNX-branded phishing kit) and continuing up through the filing of this Complaint, Fake ONNX Defendants, Abanoub Nady 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. Fake ONNX 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).

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

94. Plaintiffs have been and continues to be directly injured by Fake ONNX 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 Fake ONNX Defendants' racketeering activity, and LF Projects has incurred over $27,000 in damages as a direct result of the same racketeering conduct.

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

FOURTH CLAIM FOR RELIEF

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

(Microsoft)

96. Plaintiffs incorporate by references each and every allegation set forth in paragraphs 1 through 95 above.

97. 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.

98. Fake ONNX Defendants knowingly and intentionally accessed the Windows operating system 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.

99. Through this unauthorized access, Fake ONNX 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.

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

101. As a direct result of Fake ONNX Defendants' actions, Microsoft has suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Fake ONNX Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

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

(Microsoft, LF Projects)

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

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

104. LF Projects' trademark is a distinctive mark that is associated with LF Projects and exclusively identifies their project, ONNX Exchange.

105. Fake ONNX Defendants make unauthorized use of Plaintiffs' trademarks. By doing so, Fake ONNX Defendants create false designations of origin as to tainted Plaintiffs' products and projects that are likely to cause confusion, mistake, or deception.

106. Because of their wrongful conduct, Fake ONNX Defendants are liable to Plaintiffs for violation of the Lanham Act, 15 U.S.C. § 1125(a).

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

108. As a direct result of Fake ONNX Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Fake ONNX Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

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

(Microsoft, LF Projects)

109. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 108 above.

110. Fake ONNX 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®, Microsoft Exchange Server®, Teams®, Microsoft Defender®, Windows Vista®, Sway®, and Azure®, among other trademarks. By doing so, Fake ONNX 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.

111. Fake ONNX Defendants have used LF Projects' trademark in interstate commerce, including LF Projects' federally registered trademark for the word, mark and logo "ONNX." By doing so, Fake ONNX Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized use of "ONNX" name and logo.

112. As a result of their wrongful conduct, Fake ONNX Defendants are liable to Plaintiffs for violation of the Lanham Act.

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

114. As a direct result of Fake ONNX Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Fake ONNX Defendants' actions are enjoined.

115. Fake ONNX Defendants' wrongful and unauthorized use of Plaintiffs' trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

SEVENTH CLAIM FOR RELIEF

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

(Microsoft, LF Projects)

116. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 115 above.

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

118. LF Projects' trademark is well known and associated with its project, ONNX Exchange, and exclusively identifies its businesses and services.

119. Fake ONNX Defendants make unauthorized use of Plaintiffs' trademarks. By doing so, Fake ONNX Defendants are likely to cause dilution by tarnishment of Plaintiffs' trademarks.

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

121. As a direct result of Fake ONNX Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Fake ONNX Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

(Microsoft)

122. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 121 above.

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

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

125. Fake ONNX Defendants' actions in operating Fake ONNX Defendants 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.

126. Fake ONNX Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

127. Fake ONNX Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software.

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

129. As a direct result of Fake ONNX Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Fake ONNX Defendants' actions are enjoined.

NINTH CLAIM FOR RELIEF

Conversion

(Microsoft)

130. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 129 above.

131. 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. Fake ONNX 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.

132. Fake ONNX 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.

133. Fake ONNX Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

134. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Fake ONNX Defendants' ill-gotten profits.

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

TENTH CLAIM FOR RELIEF

Unjust Enrichment

(Microsoft, LF Projects)

136. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 135 above.

137. The acts of Fake ONNX Defendants complained of herein constitute unjust enrichment of the Fake ONNX Defendants at the expense of Plaintiffs in violation of the common law.

138. Fake ONNX Defendants used, without authorization or license, software belonging to Plaintiffs to facilitate unlawful conduct inuring to the benefit of Fake ONNX Defendants.

139. Fake ONNX Defendants profited unjustly from their unauthorized and unlicensed use of Plaintiffs' intellectual property.

140. Upon information and belief, Fake ONNX Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Plaintiffs' intellectual property.

141. Retention by the Fake ONNX Defendants of the profits they derived from their malfeasance would be inequitable.

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

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

PRAYER FOR RELIEF

WHEREFOR, Plaintiffs pray that the Court:

1. Enter judgment in favor of Plaintiffs and against the Fake ONNX Defendants.

2. Declare that Fake ONNX Defendants' conduct has been willful, and that Fake ONNX Defendants have acted with fraud, malice, and oppression.

3. Enter a preliminary and permanent injunction enjoining Fake ONNX 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 injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction giving Plaintiffs control over the domains used by Fake ONNX Defendants to cause injury and enjoining Fake ONNX Defendants from using such instrumentalities.

5. Enter judgment awarding Plaintiffs actual damages from Fake ONNX Defendants adequate to compensate Plaintiffs for Fake ONNX Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment disgorging Fake ONNX Defendants' profits.

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

8. Enter judgment awarding attorneys' fees and costs, and

9. Order such other relief that the Court deems just and reasonable.

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: November 12, 2024

Robbie Rogart Jost (VA Bar No. 84377)
David J. Ervin (VA Bar No. 34719)
Jeffrey L. Poston (*pro hac vice* forthcoming)
Garylene Javier (*pro hac vice* forthcoming)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
T: 202-624-2500
F: 202628-5116
RJost@crowell.com
DErvin@crowell.com
JPoston@crowell.com
GJavier@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

Counsel for Plaintiffs Microsoft Corporation and LF Projects LLC