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**

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'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 Fake ONNX Defendants. DCU also collaborates with MSTIC, Microsoft's threat intelligence community, which is made up of thousands world-class experts, security researchers, analysts, and threat hunters. MSTIC publishes a threat intelligence blog alerting customers and the public of cybersecurity threats.[2]

3. In my role at Microsoft as part of DCU, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are 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.

4. Before joining Microsoft, I worked for Xerox as the Manager of Xerox's Cyber Intelligence 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

---

[1] *Digital Crimes Unit: Leading the fight against Cybercime, 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).

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**.

5. My declaration concerns the investigation into a foreign-cybercriminal organization comprised of Abanoub Nady and a series of unknown individuals—John Does 1-4—who are collectively known as "Fake ONNX Defendants." I have investigated the structure and function of Fake ONNX Defendants' criminal organization, including completing a test buy, which I discuss in this declaration. I have also investigated and address below Fake ONNX Defendants' victim targeting methodology, attack techniques, and the tools used to execute their cybercriminal attacks. I also address the impact and harm that Fake ONNX Defendants cause Microsoft, its customers, including LF Projects, and the public, and the continuation of this irreparable harm if the Fake ONNX Defendants are permitted to carry out their cybercriminal activity. Finally, my declaration explains what I believe to be the most effective way of disrupting Fake ONNX Defendants' illegal activity.

CYBERCRIME AT ISSUE: PHISHING-AS-A-SERVICE

6. I, along with other Microsoft investigators, investigate cybercrime campaigns like phishing-as-a-service ("PhaaS") that are perpetrated by threat actors that target Microsoft and its customers. In this role, I have investigated Fake ONNX's PhaaS campaign.

7. As an experienced cybercriminal investigator, I am familiar with a tactic known as phishing. Phishing is a method of attack involving the 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"). 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.

8. Fake ONNX Defendants have developed, sold, and facilitated the deployment of a pre-packaged sets of tools ("phishing kits") that enable other cybercriminals to create and deploy phishing attacks with relative ease. This business model of selling phishing kits and services for use by other cybercriminals is also referred to as "PhaaS. These phishing kits include email templates, fake website templates, domain registration services, how-to videos, and customer support features designed to help the cybercriminal customer evade detection. The kits are essentially "how to" manuals to assist Fake ONNX Defendants' cybercriminal customers in developing and executing 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, Yahoo, 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 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.

9. 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.

10. PhaaS lowers the barrier to entry for cybercrime from a technical skillset perspective, which allows even novices to launch effective phishing attacks—would-be cybercriminals no longer need to have the technical ability to develop sophisticated infrastructure, they can rely on an "off the shelf" product. 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 make it an attractive option for would-be cybercriminals. The Fake ONNX 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.

THE FAKE ONNX DEFENDANTS

11. Fake ONNX Defendants are prolific cyber criminals that manufacture and sell ONNX-branded phishing kits, and also provide PhaaS to other cybercriminals. Other downstream cybercriminals 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 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 January 2024 transitioned to the brand "ONNX."[3] In 2024, Caffeine/Fake

[3] Co-Plaintiff LF Projects owns the trademarks for Open Neural Network Exchange, or "ONNX," and well as ONNX's logo. This exchange is a well-known ecosystem of technology

ONNX was considered the most prevalent phishing operation with over 16.8 million phishing emails observed from December 2023 to June 2024. **Figure 1** depicts the various named under which the Fake ONNX Defendants have advertised, sold, or distributed their phishing kits.

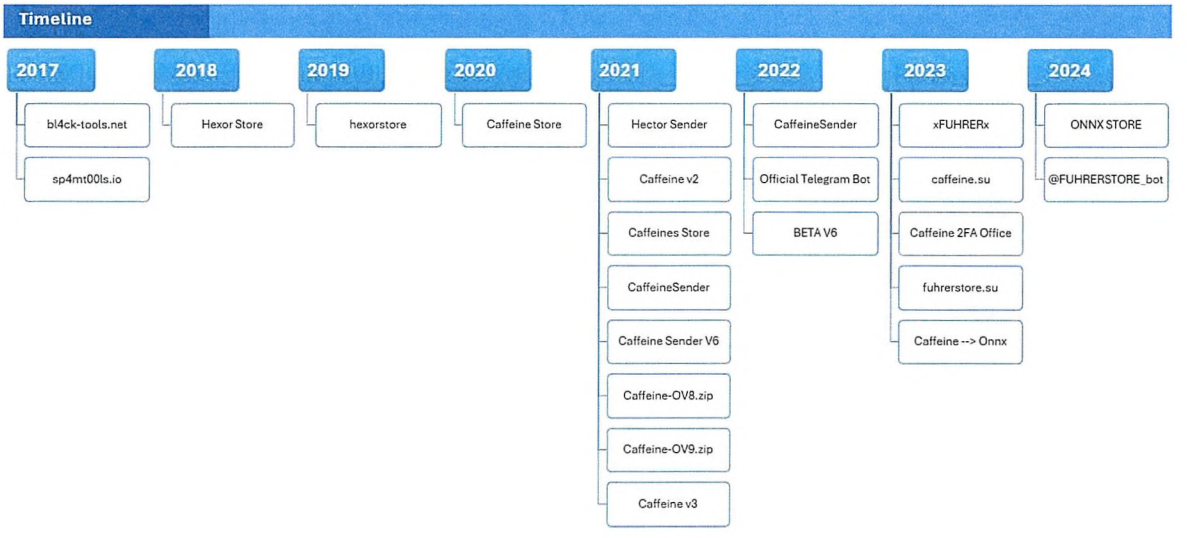


Figure 1

12. DCU investigated the Fake ONNX Defendants and was able to identify Abanoub Nady as an individual involved in the criminal organization. First, DCU investigators identified that the persona "MRxC0DER" was advertising the ONNX/Caffeine-branded phishing kits on the Caffeine Store and were able to connect this username to the domain "mrxc0der.xyz." Using the WHOIS history lookup (this shows the history of previous owners of the domain and other registration details) DCU investigators connected the domain to the following email address

---

companies. *See* Declaration of Michael Dolan ISO TRO Application ¶¶ 3-5. Although Defendants used to market their products, under the name "Caffeine," they have since illegally adopted the "ONNX" name and logo. Thus, they now market their phishing kits under the ONNX name. For purposes of this declaration, "Fake ONNX" refers to the Defendants' cybercriminal operation, their 'Caffeine' phishing kits, and their PhaaS operation, and is meant to distinguish Defendants from the Co-Plaintiff's LF Projects legitimate ONNX branding.

belonging to the registrant of the domain: mrprincex0[@]gmail[.]com. We then used Microsoft internal telemetry to further investigate this email address. This investigation revealed the account name "Abanoub Nady," who is believed to reside in Egypt. Additionally, DCU investigators were able to connect the email address mrprincex0[@]gmail[.]com directly to five other email addresses that also have an account name of "Abanoub Nady": mrxcodereg[@]outlook[.]com, bebonady82[@]yahoo[.]com, bnady19[@]yahoo[.]com, mrxc0der[@]hotmail[.]com, and abanoubxcoder[@]outlook[.]com. Once we had linked these email addresses, we used open source threat intelligence data to connect the email address bebonady82[@]yahoo[.]com to a YouTube channel. The name of the YouTube channel was @abanoubnady1034 with the name Abanoub Nady, and the Channel featured a playlist named MUSIC | MRxC0DER, as seen in **Figure 2**. The same YouTube profile picture and account name corresponds to a LinkedIn profile abanoub-nady-49baa3237 for Abanoub Nady which listed the company name 'Caffeine," as seen in **Figure 3.**

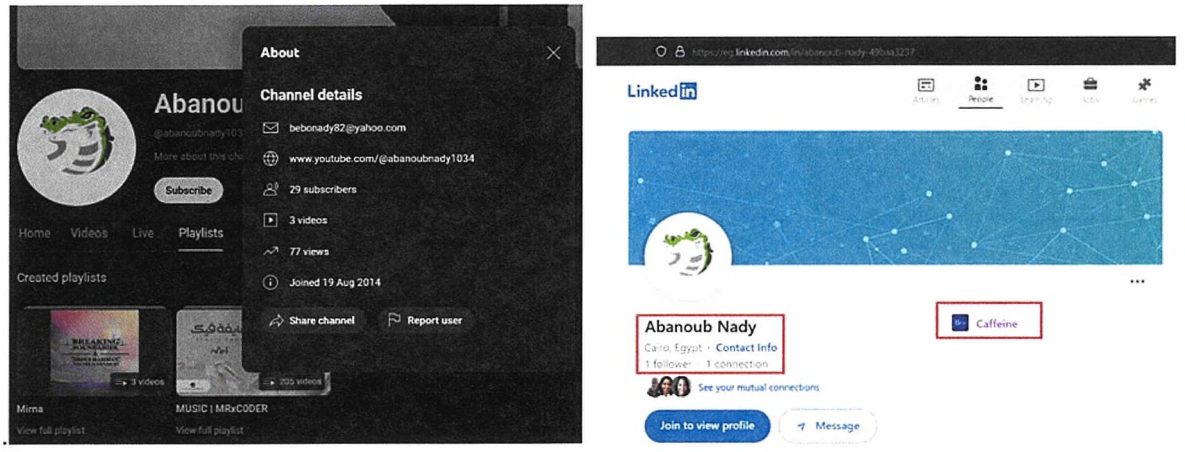


FIGURE 2 and 3

13. Subsequently on June 19, 2024, Dark Atlas[4] published an exposé identifying Mr. Nady as the creator and developer of the ONNX-branded phishing kits and the administrator of Defendants' phishing operation. Attached to my declaration as **Exhibit 2** is a true and correct copy of the Dark Atlas publication naming Mr. Nady as the mastermind behind the operation. Mr. Nady is also known by the username MRxC0DER. **Figure 4** demonstrates the handle "MRxC0DER is associated with the Administrator of "Caffeine Store" (the former name of the online store where customers can purchase the ONNX-branded phishing kits).

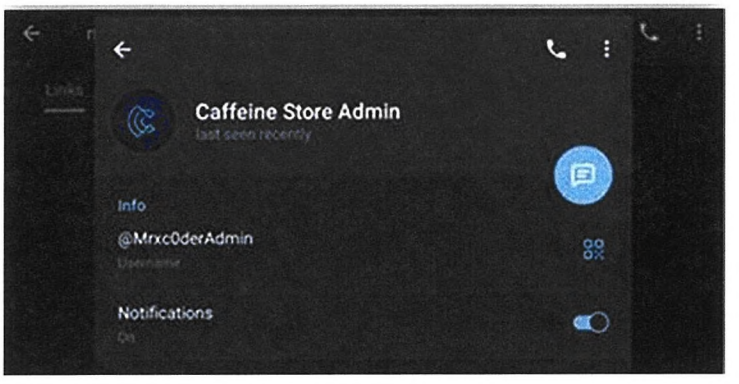


Figure 4

14. To support this phishing operation, Fake ONNX Defendants have established and operate 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. Fake ONNX Defendants use the domains as part of their phishing operation by including the domains in their phishing emails and encouraging the victims to click on the malicious domains where they are redirected to a Fake ONNX-controlled webpage and then unknowingly provide their credentials to Defendants. The identity of the website domains used by Fake ONNX Defendants to support their phishing

[4] According to its website, Dark Atlas is an AI-powered Cyber Intelligence Platform (https://darkatlas.io/). One of its offerings is a blog, where it publishes information about various cyber threats for the public (*see* https://darkatlas.io/blog).

operation are set forth at **Appendix A** to this Complaint and constitutes Fake ONNX Defendants' technical infrastructure.

15. The remaining identities of the Fake ONNX cybercriminal organization are unknown or uncertain because Defendants take great measures to obfuscate their identity. However, I have been able to identify specific functions or responsibilities of these individuals who collectively carry out Fake ONNX's cybercrime operation.

16. Based on my investigation, I am informed and believe that John Doe 1 controls the Fake ONNX criminal phishing organization and the technical infrastructure.

17. Based on my investigation, I am informed and believe that John Doe 2 provides technical support for the Fake ONNX Defendants' criminal phishing organization and the technical infrastructure, including facilitating the sale and promotion of the ONNX-branded phishing kits.

18. Based on my investigation, I am informed and believe that 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.

19. Based on my investigation, I am informed and believe that John Does 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.

20. The Fake ONNX Defendants each have specialized roles within the cybercriminal organization. Each Fake ONNX 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 and LF Projects intellectual property. Their ongoing association with one another and reliance on each other's specialized role and contribution allows the Fake ONNX Defendants to function as a single unit within a lucrative operational structure. Based on my investigation, I have concluded that this allows the Fake ONNX Defendants to scale their operation and increase the financial profitability of their criminal activity. Because the creator, sellers and distributors of the ONNX-branded phishing kits work collectively with the cybercriminal customers, they are able to expand the scope and reach of the Fake ONNX Defendants' phishing operation. This leads to the significant increase of downstream criminal activities, such as financial fraud, business email compromise, theft of proprietary information, and potential ransomware attacks.

FAKE ONNX DEFENDANTS' MODUS OPERANDI: PHISHING

21. Fake ONNX 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 Fake ONNX Defendants' criminal operation when they, in turn, use and deploy the ONNX-branding phishing kits to conduct their own cybercrimes directed at Microsoft and its customers. The ONNX-branded phishing kits allows the cybercriminal customer to infiltrate the systems of Microsoft customers undetected and steal credentials belonging to users of the infiltrated network, often through deceit or tricking the victims. The cybercriminal customers then use these stolen credentials to further access and infiltrate the victim's network. Through this behavior, the cybercriminal customers take on what

is known as an AiTM role, whereby the cybercriminal customer position themselves between communications directed to and from Microsoft customers. **Figure 5** demonstrate how cybercriminal customers become part of the Fake ONNX Defendants criminal organization as they purchase the phishing kit, deploy the kit, and engage in phishing attacks (in collaboration with other, existing Fake ONNX Defendants) against a victim.

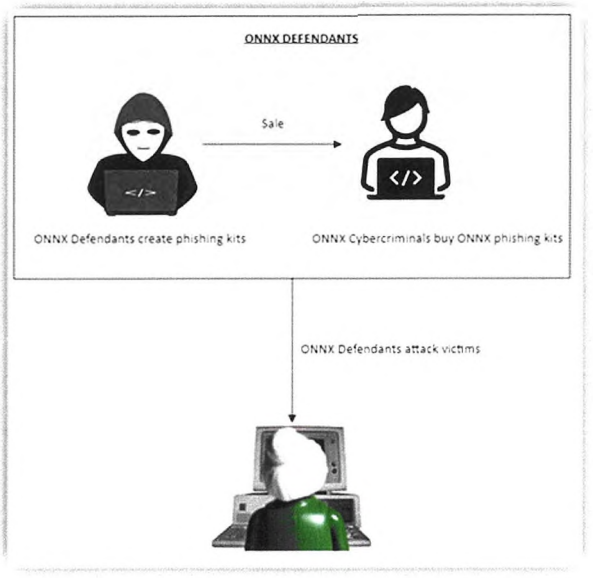


Figure 5

22. 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 that is 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 Fake ONNX-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.m1crosoft.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. **Figure 6** represents the Fake ONNX-controlled domains identified in **Appendix A** that reference Microsoft, its well-known products and services, and employ the tactic described here of typosquatting.

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	outlorklive.com
2fa-0ffice03protection-65auth.com	login-strems-outlook.com	myofficesdocusviews.com	pdf-login-outlook.cc
2fa-auth-outlook.com	loginteams.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	mautenticator-365.com	off356reviewdocs.com	securesharepointprotection.xyz
app-office0365voicemail-protection.com	mfa-auth-outlook.com	off356reviewdocu.com	servr-0365-protection.com
app-office03auth-65protection.com	miclst.com	off356reviewsign.com	servr-office365check.com
app-office03auth-65protections.com	miclosoft.us	officce.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	microsofuiti.com	officeauthmicrpdfreciept.com	sharepointproposals.com
auth-protection365office.com	microsofofficials.org	office-authmllmwdfdolkcxfbtsathhfdfdorlkcxauthdietetoutloe.com	sharepointscloud.com
azureendpoint.com	microsofstonline.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	mircr-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	msdocvieeewlivce.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
loginmicrosoftonlline.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	verificationoultook365s.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-office-files.vip	msoftshareonedriive.com	outloko-oficeo365o20.com	verifysharepointfi1es.us
login-office-outlook.com	msoftshareonedrive.com	outlook365-online-login.com	verify-signinoutlexchangeadmin.com
login-online-outlook365.com	msoftstorage.com	outlook-live-authentitcitework.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 6

23. 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.

FAKE ONNX DEFENDANTS ATTACK CHAIN

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

24. The phishing kits that are designed, developed, and sold by the Fake ONNX Defendants are specifically designed 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 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.

25. Fake ONNX Defendants' phishing kits are specifically developed to target: Microsoft 365 and Azure[5] users, and include two-factor (2FA) authentication[6] bypass features for

[5] Microsoft365 is a product family of productivity software, collaboration and cloud-based services owned by Microsoft. Microsoft365 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.

[6] Multi-factor authentication 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

the Microsoft Authenticator[7] application and Microsoft Office, specifically the Outlook application. For example, one observed phishing kit is named the "Office 2FA Cookies Stealer," because it is designed to intercept the transmission of a victim's 2FA (two factor authorization) code used to verify the victim's identity when they log into their Outlook account. These malicious phishing kits support credentials theft, information exfiltration, and subsequent end-user attacks which include business email compromise, ransomware, and financial fraud. Fake ONNX Defendants are able to execute these end-user 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 through global Microsoft network infrastructure.

26. The ability to use the phishing kit to trick Microsoft customers to hand over their credentials and thus allowing infiltration Microsoft's systems is a "selling point" of the ONNX-branded phishing kits. Cybercriminal customers purchase these ONNX-branded kits because they have the capability to infiltrate Microsoft systems and the significant security protocols that Microsoft implements to protect against cyberattacks.

27. Another advertised feature is the ability to customize logos and email templates to further create authenticity in the phishing email. This feature is depicted in **Figure 7.**

---

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.

[7] 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.

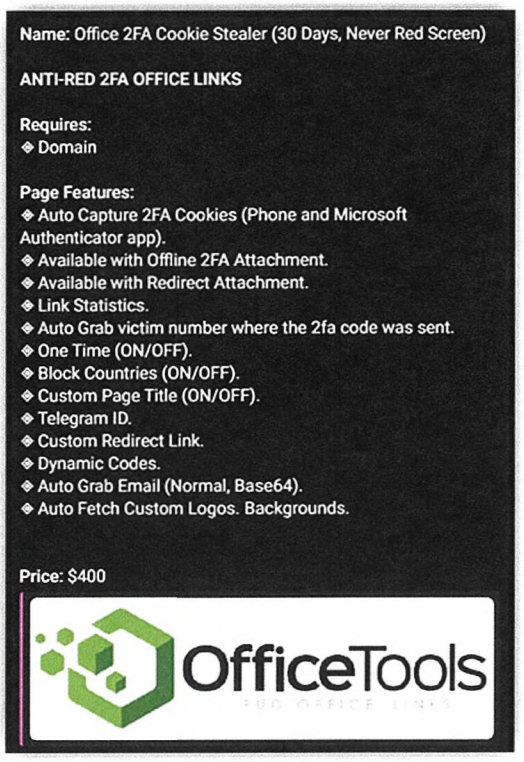


Figure 7

28. The Fake ONNX Defendants sell their ONNX-branding kits online at the "ONNX Store" (formerly known as the "Caffeine Store") for cybercriminals to purchase, as demonstrated in **Figure 8**.

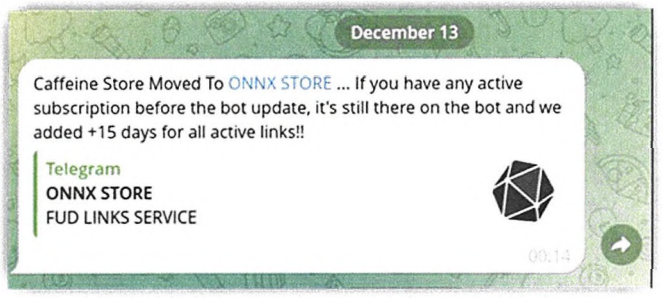
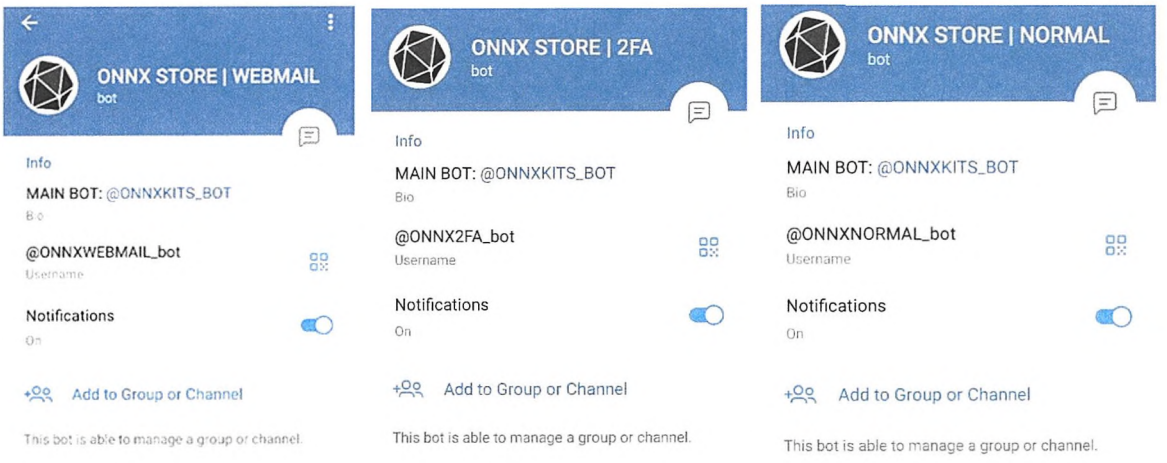


Figure 8

29. The Fake ONNX-branded phishing kits are promoted through Telegram Messenger, a secure, cloud-based messaging platform. It is known for its end to end encryption. Fake ONNX 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 Fake ONNX Defendants and potential customers interested in purchasing the phishing kits. *See* **Figures 9-11** for screenshots of Telegram channels used by the Fake ONNX Defendants.



Figures 9, 10, and 11

30. To advertise their phishing kits, Fake ONNX Defendants also use social media platforms, like YouTube to provide "how to" videos on the purchase and implementation of these phishing kits. Mr. Nady also uses the MRxC0DER handle to advertise the phishing kits on Telegram, as shown in the screenshot at **Figure 12**.

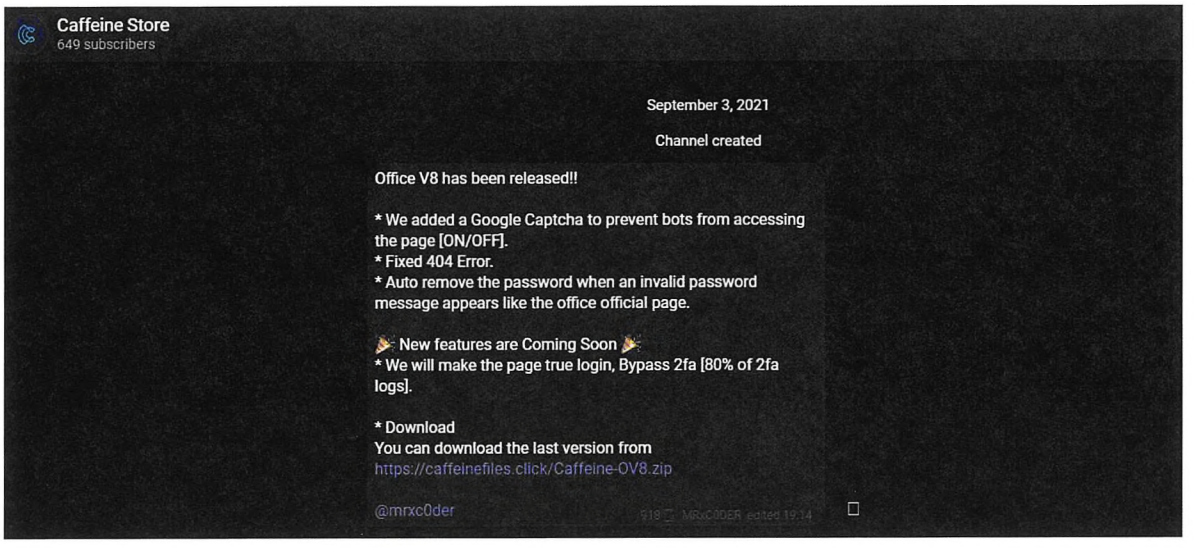


Figure 12

31. The Fake ONNX Defendants do not just sell their phishing kit for one time use. Rather, to maximize their financial gain, they take steps to ensure the repeated use of their products. The Fake ONNX Defendants offer their customers a phishing kit subscription model, offering Basic, Professional, and Enterprise subscriptions, each for different tiers of access. Enterprises users can also purchase the add-on feature of "Unlimited VIP Support," essentially ongoing technical support that provides step-by-step instructions on how to successfully commit cybercrime. The ONNX Store's pricing models are show in **Figure 13**.

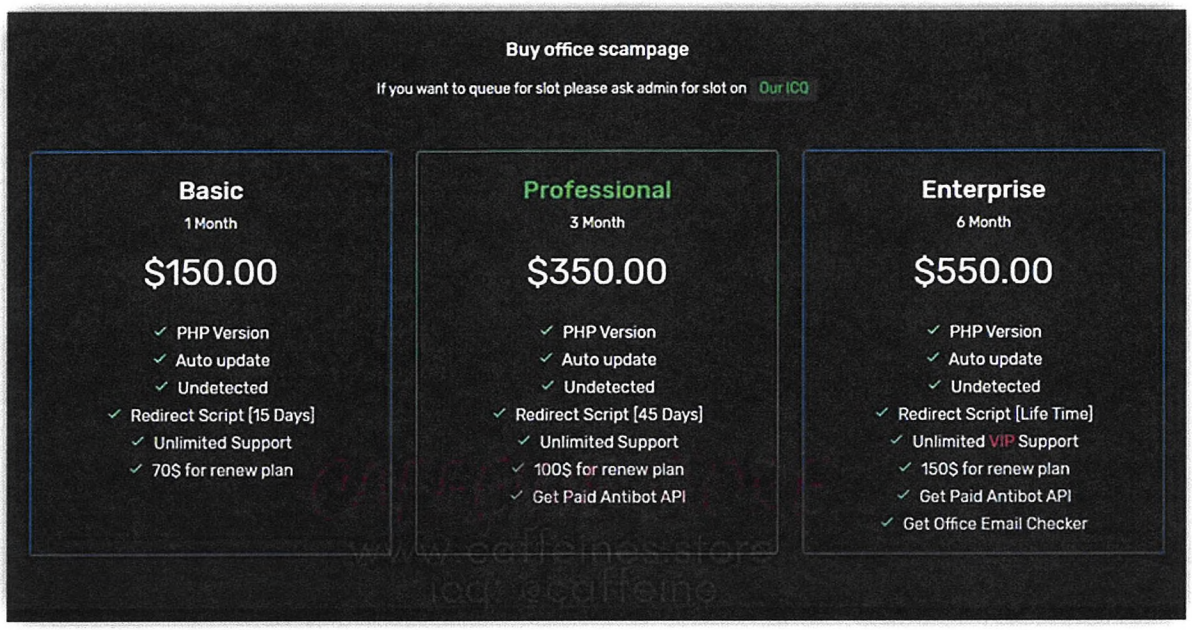


Figure 13

32. Another advertised feature of the phishing kits is their undetectable nature. Based on my experience investigating cybercriminals and threat actors, many will make extensive efforts to avoid detection and conceal their identity. This makes sense; if they remain undetected, they can avoid law enforcement and continue their criminal activities. The Fake ONNX are no different. Their phishing kits include an anti-bot application programming interface ("API"). Ordinarily legitimate websites check to determine if the user accessing the website is a human or a bot (a computer program that runs tasks without human intervention). This may involve requiring the user to select all images that show the same object or require the end user to enter in a series of letters and numbers displayed in an image. Only when the user correctly "proves" they are a human are they able to access a website. The anti-bot API is used to circumvent and bypass these security tools on a victim's computer by preventing an email service from being able to scan for bot activity or scan to determine whether an email contains malicious content of links to

malicious websites. In general, an email service like Outlook has sophisticated security tools to scan incoming email for potential phishing emails, spam, or compromised messages. The anti-bot API serves as a blocker to prevent these security tools from working as they are supposed to, which allows the Fake ONNX Defendants to circumvent the security tools, these steps are demonstrated in **Figure 14**.

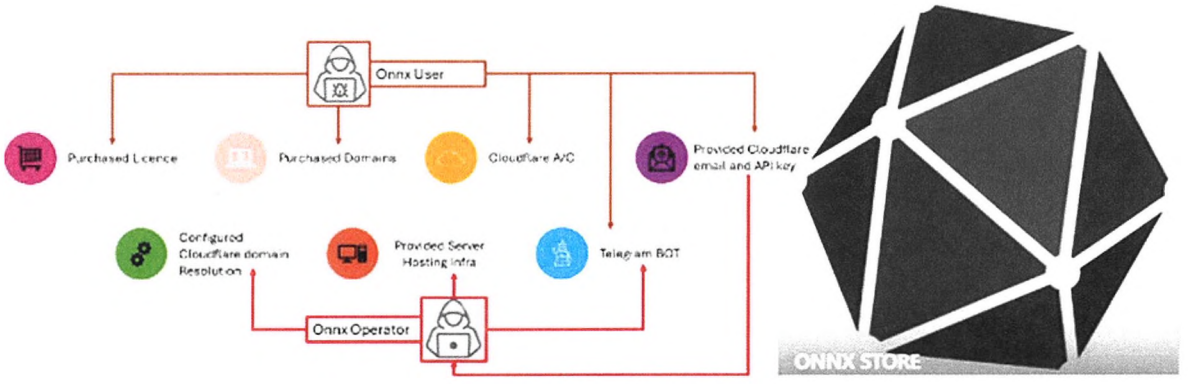


Figure 14

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

33. Once the Fake ONNX Defendants sell an ONNX-branded phishing kit to a cybercriminal customer, the customer must take several steps to activate the phishing kit and incorporate the malicious domain into the Fake ONNX Defendants technical infrastructure. The cybercriminal must purchase a domain, they must establish the infrastructure needed to evade detection, and the customer must connect their malicious domain to the overall technical infrastructure.

34. The first activation step is purchasing domains. The Fake ONNX Defendants' cybercriminal customers must purchase a domain from a registrar (a third-party company, like GoDaddy that makes domains available for purchase). The Fake ONNX 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 Fake ONNX technical infrastructure. As described in Paragraph 22 and in **Figure 6**, *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.*, "onliine" (with two of the letter "i) instead of "online" (the word correctly spelled), which as I described in Paragraph 22, *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, Fake ONNX Defendants focus on manufacturing "legitimacy" and employing tactics like typosquatting to hide the sinister nature of the malicious domain.

35. The second activation step is to establish infrastructure that can be used to obfuscate identity. Fake ONNX Defendants direct their cybercriminal customers to create an account on Cloudflare, Inc. ("Cloudflare") to further evade detection. Cloudflare is a company that provides a variety of legitimate network services and security features to protect their users from online cyberthreats and attacks. These features include IP proxying[8] and a CAPTCHA[9] service to authenticate that a website link is legitimately clicked by a human.

36. 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 Fake ONNX Defendants have hijacked this proxy to conceal their "home address" (their real IP address). This

[8] 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.

[9] 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.

means that the IP address will show a fictitious location, which further allows Fake ONNX Defendants to evade detection.

37. 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 perform specific tasks (like access a website). CAPTCHAs are designed to protect normal consumers. 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 any issue. **Figure 15** is a depiction of an image solving CAPTCHA.

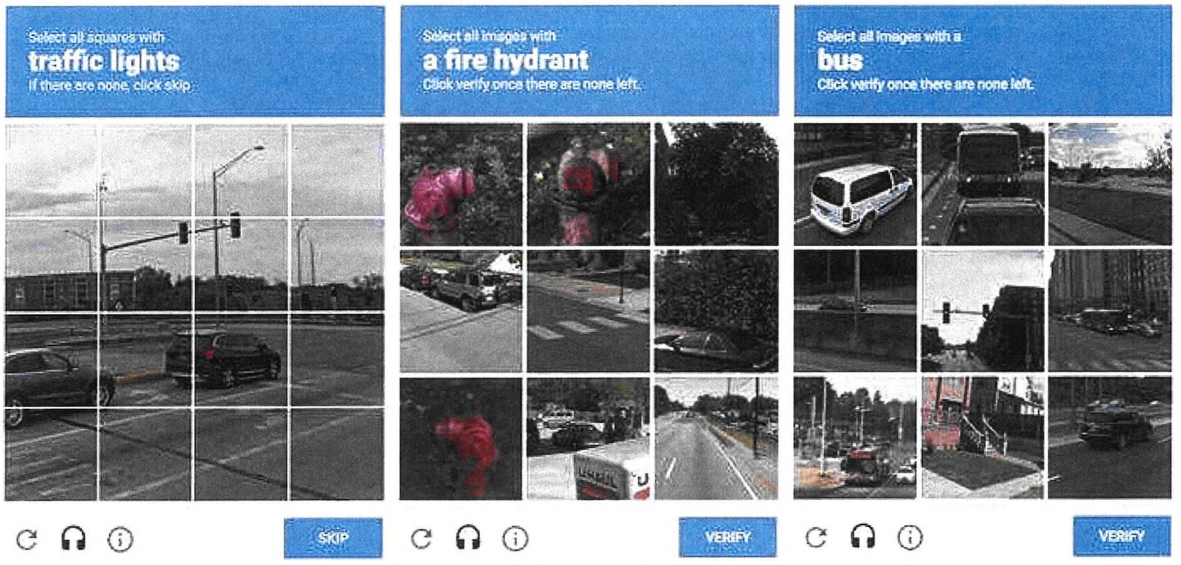


Figure 15

38. The Fake ONNX Defendants abuse and misuse these legitimate services offered by Cloudflare to perpetrate their cybercrimes. In my experience, it is common for a cybercriminal to abuse and misuse an otherwise legitimate software or tool for the purposes of committing cybercrime. This is done intentionally because the cybercriminal 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."

39. By misusing Cloudflare's services, Fake ONNX 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 Fake ONNX Defendants are able to increase their phishing campaign efficiency: they protect themselves from being discovered which lessens the chance that they are shutdown, either by the third party registrars or law enforcement.

Step Three: Connecting to the Fake ONNX's Defendants Phishing Operation

40. Next, Cloudflare provides an API key (a code used to identify and authenticate a user in Cloudflare). At the request of the Fake ONNX Defendants, the cybercriminal customer provides the API key to Fake ONNX Defendants. On the backend, the Fake ONNX Defendants use the API key code to connect the cybercriminals' domain (the one that is designed to look like it actually refers to Microsoft or a Microsoft product) into the overarching technical infrastructure. The screen recorded video, which Fake ONNX Defendants post on their store's FAQ page demonstrates this process, which is also depicted in **Figure 16.**

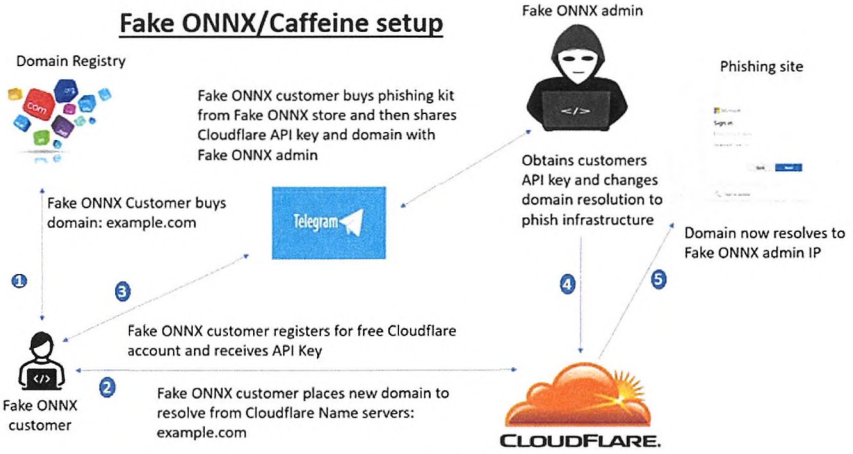


Figure 16

Step Four: Further Phishing Attacks by Fake ONNX

41. The next step involves the Fake ONNX Defendants deploying the phishing kits and engaging in phishing attacks. The Fake ONNX Defendants will send phishing emails to victims that prompt the victim to click on a link. The phishing email will often use Microsoft's logos with an invitation to click on a link. This unauthorized use of the logo makes it appear as if Microsoft is sending an email to its customer with a call to action related to one of Microsoft's services. **Figure 17** and **Figure 18** are examples of such phishing emails.

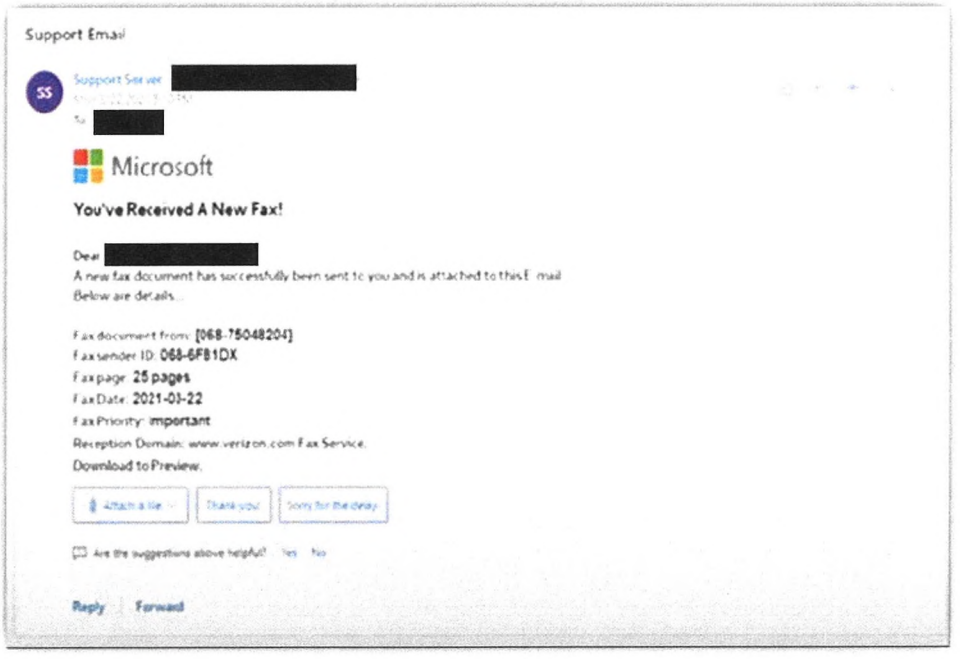


Figure 17

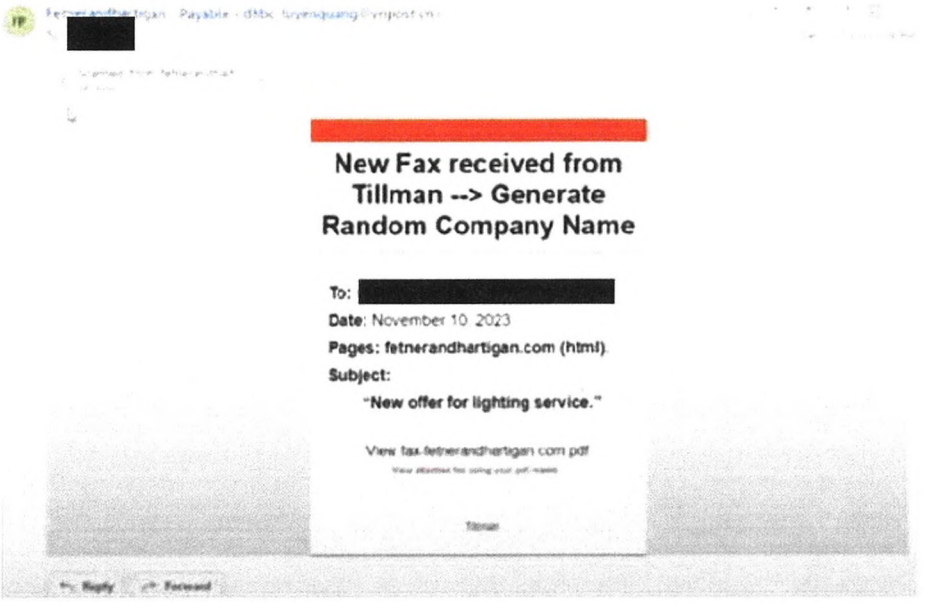


Figure 18

42. The phishing email will also invite the victim to click on a link contained in the body of the email, click on a link contained within a pdf file, or click on a QR code. The link is one that was purchased by the cybercriminal customers and connected to the overarching technical infrastructure. As described above, because the domains appear to be related to Microsoft or a Microsoft product the victims believe the domain is safe, and they are lulled into a false sense of security. If the victim clicks on the link to the malicious phishing domain, they are directed to a website that contains a login page. Although the login page is fabricated to look like an authentic Microsoft login page by using Microsoft's name and branding, in reality the login page is fake. Based on my investigation, in many instances the fake login page was created by using the template that was provided in the ONNX-branded phishing kit. 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 19** (verifying password) and **Figure 20** (completing the 2FA process).

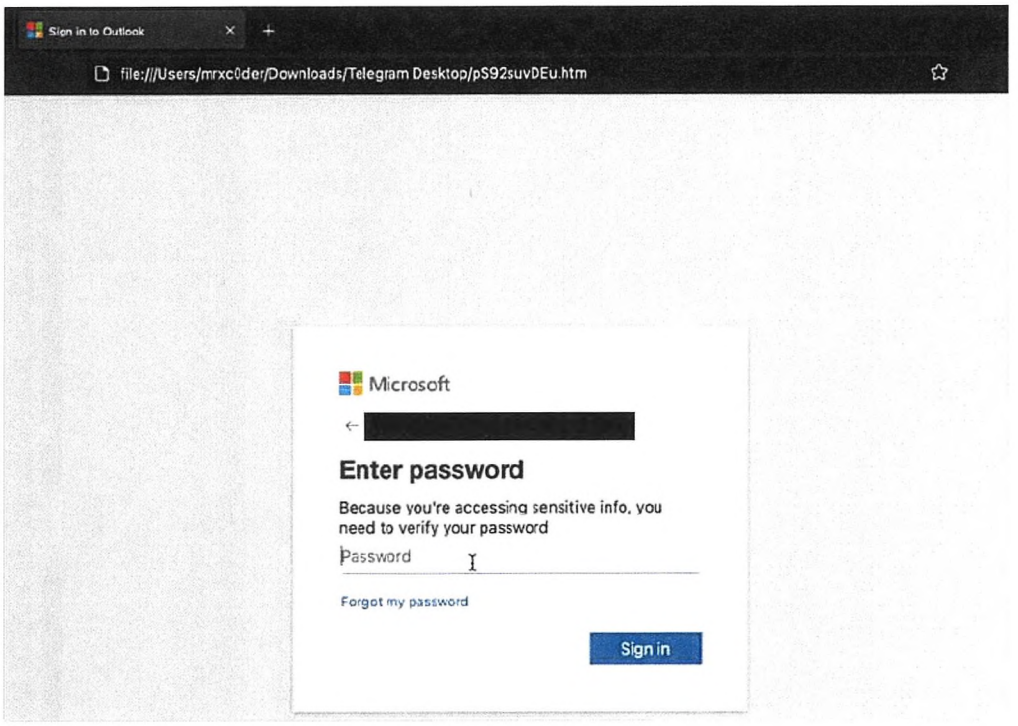


Figure 19

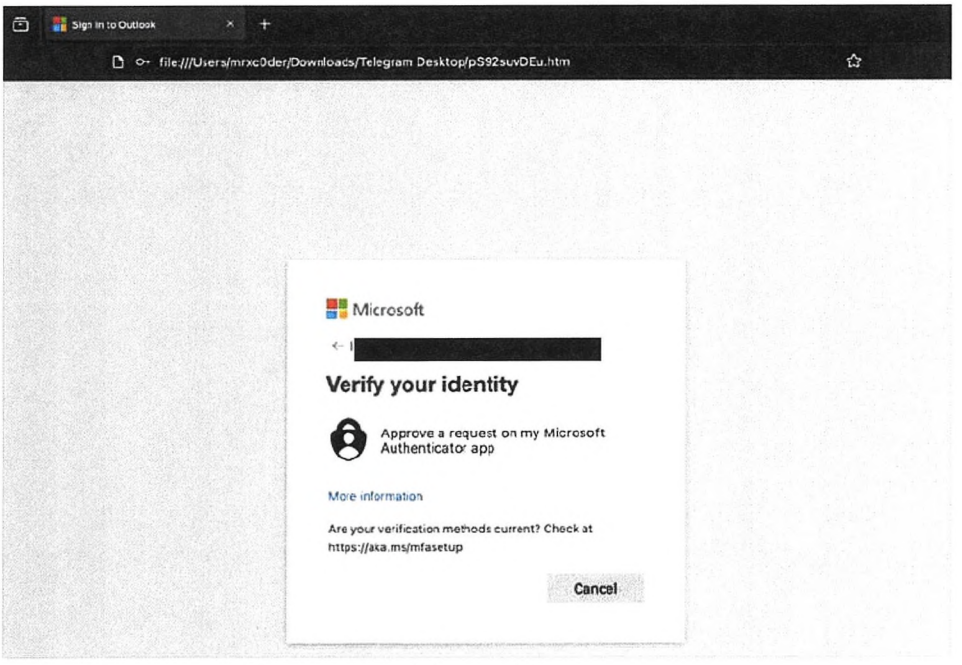


Figure 20

43. Through asking the victim to enter their password and verify their identity, Fake ONNX Defendants have captured the victim's account credentials. At this point, the Fake ONNX Defendants will prompt the victim to provide their phone number to receive their 2FA token to verify their identity and access their account. 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 phone number, receives the 2FA token, and enters the token into Fake ONNX Defendants' fraudulent login page, their phone number and 2FA tokens are captured by Fake ONNX Defendants. **Figure 21** depicts this process.

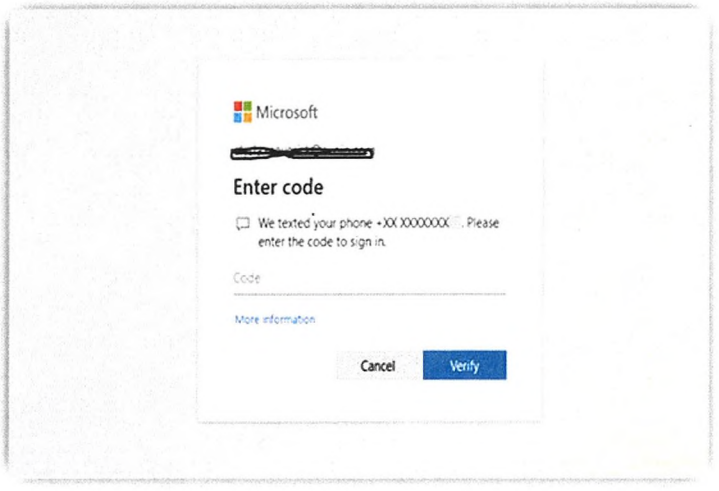


Figure 21

44. 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. At this point, Fake ONNX Defendants have the ability to login in to the user's real account and take control of the account, even though Fake ONNX Defendants did not have authorization is access these accounts. For example, if the victim

entered their Outlook email credentials, Fake ONNX Defendants would now have complete access to the victim's Outlook account, including the inbox, the sent folder, their calendar, contact list, and any files attached to emails within the account. 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. They can also use this access to identify additional phishing victims and facilitate those additional attacks. For example, if the victim is a manager at a company, Fake ONNX Defendants can impersonate the manager and then phish other employees.

45. At this point, a Fake ONNX Defendant may engage in additional phishing attacks, may purchase additional domains to connect to the technical infrastructure, or if their subscription to the ONNX-branded phishing kits has lapsed, purchase an additional subscription. This process can be replicated with ease, which allows Fake ONNX Defendants to scale their criminal organization.

46. The attack methodology described in Paragraphs 21 to 45 of this declaration are depicted in **Figure 22**.

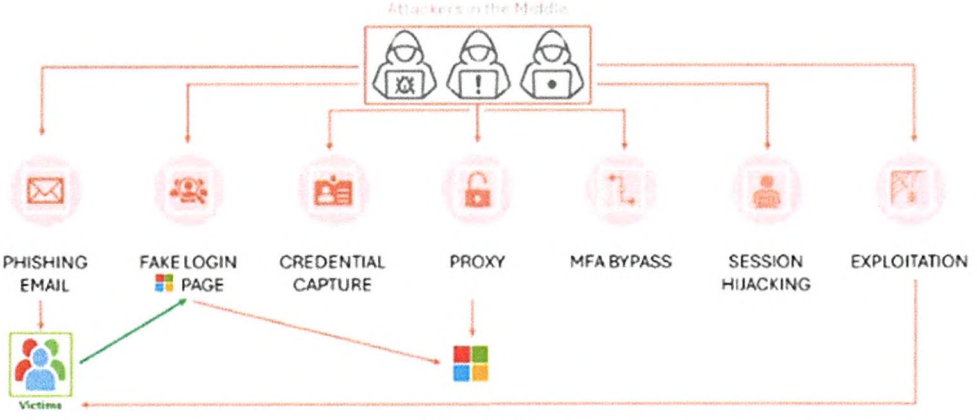


Figure 22

TEST BUY

47. As part of my investigation, on April 18, 2024, I conducted a test buy of the ONNX-branded phishing kits. To do so, I first accessed the ONNX Store where I began communicating via Telegram with the Fake ONNX Defendants who have the specific responsibility for promoting, advertising, and selling the ONNX-branded phishing kits. I expressed interest in purchasing a phishing kit to further the communication with Fake ONNX Defendants. Once I had demonstrated my interest in purchasing a phishing kit, I continued my engagement in the chat until I was provided with payment information that would allow me to transfer money via a Bitcoin wallet. Once the money was transferred, I received a message that my order had been successfully placed for the phishing kit. A screenshot of my Telegram conversation documenting the test buy is included as **Figure 23**.

Figure 23

48. Once I successfully purchased the phishing kit, I was instructed to add the domain, and I was directed to the FAQ page with instructions on how to add the domain I separately purchased to the Fake ONNX Defendants' infrastructure.[10] **Figure 24** is the FAQ page that includes a link to a how-to video on how to add the domain using the API key.

[10] I purchased several domains in connection with the test buy: securitydomainregistration.com and securedomainregistry.com. Both of these domains mimicked the style of the malicious domains used by the Fake ONNX defendants.

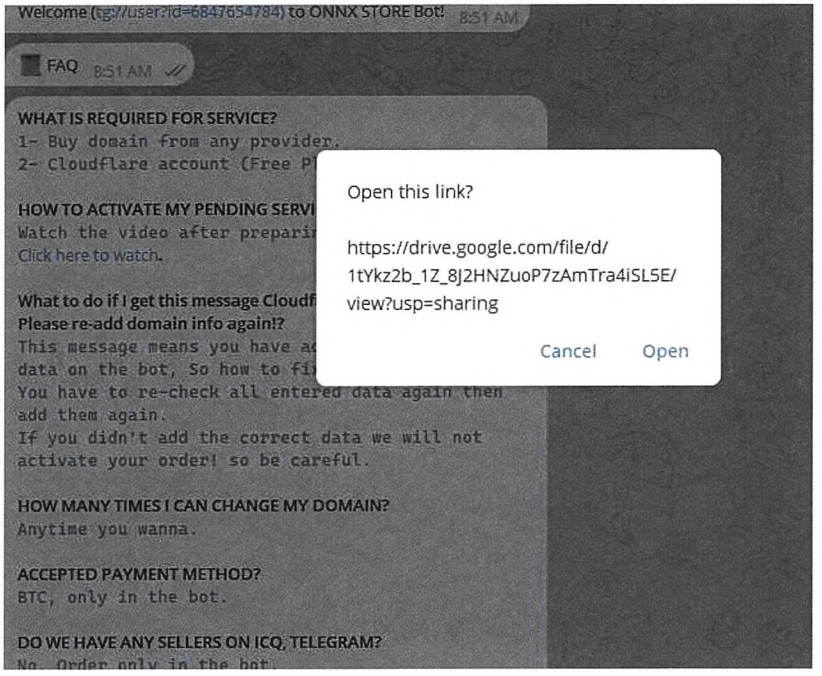


Figure 24

49. In the video, the Fake ONNX Defendants walk through how to change where the malicious domain resolves (or redirects) to further obfuscate the identity. This involves creating a free Cloudflare account, and then changing the name server of the malicious domain to Cloudflare. A name server is a computer application that translates a domain name into an IP address, which connects the user to the website they are trying to visit. By changing the name server to Cloudflare, someone trying to investigate the domain will simply see Cloudflare, but nothing more. On the backend, however, because the cybercriminal customer provided the API key to the Fake ONNX Defendants, the malicious domain actually redirected to the Fake ONNX technical infrastructure—but this is undetected. Using the FAQ and how to video, I was able to follow these steps to provide my API key to the Telegram channel as instructed, which allowed me to connect the domains I had purchased to the overall Fake ONNX Defendants' technical infrastructure.

50. Because I purchased these domains, I was able to use the domains to gain telemetry about the technical infrastructure. Additionally, I was able to conduct a test phishing attack by using the phishing kit I had purchased to "phish" a Microsoft account that was specially created for this investigation. This allowed me to observe how the phishing kit operated.

ATTRIBUTION TO THE FAKE ONNX DEFENDANTS

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

52. Cybercriminals, such as the Fake ONNX Defendants, are known to obfuscate their identities to evade capture by law enforcement and continue their cybercrime.

53. In the course of 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 was able to determine that the domains identified in Appendix A belong to and are used by the Fake ONNX Defendants. Specifically, the following indicators were used in my assessment: domain registration patterns, phishing URL patterns and components based on known Fake ONNX 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.

54. These features when taken together, provide a high level of confidence that a given domain is a Fake ONNX 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 Fake ONNX 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 Fake ONNX Defendants. At times, other researchers in the security community independently identify Fake ONNX 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 USE INSTRUMENTALITIES LOCATED IN VIRGINIA

55. The Fake ONNX domains include a number of different top level domains (such as ".com," ".net," ".org," ".info"). The overwhelming majority of the Fake ONNX domains are ".com" domains. If Fake ONNX Defendants are trying to mimic Microsoft and its services in the phishing domains, it makes sense that all the domains are .com, because this is the top level domain that Microsoft uses in connection with its authentic and legitimate products and service, and thus a ".com" domain is less likely to alert the victim to the phishing. Third-party Verisign is a registry that oversees the registration of all domains ending in ".com" or ".net" and is located at 12061 Bluemont Way, Reston, Virginia 20190.

HARM TO MICROSOFT AND ITS CUSTOMERS

56. Fake ONNX Defendants have targeted Microsoft, its customers, and the public in order to advance their financially – motivated cybercrimes. Fake ONNX Defendants have caused and continue to cause irreparable injury, to Microsoft, its customers, LF Projects, and the public. The Fake ONNX Defendants' activities irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill.

57. 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®, Microsoft Exchange Server®, Teams®, Microsoft Defender®, Windows Vista®, Sway®, and Azure®, among other trademarks. The registrations for these trademarks are attached to the Complaint as **Appendix B**.

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

59. *First*, Fake ONNX-branded phishing kits 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. 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..

60. *Second*, Fake ONNX Defendants leverage Microsoft systems and programs, such as Outlook and Microsoft 365, to further enhance the perceived legitimacy of the attack. Similarly, because the login pages that Fake ONNX Defendants use 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. In doing so, Fake ONNX Defendants capitalizes on and misuses the brand recognition that Microsoft has cultivated and the trust Microsoft has built with its customers and that customers have come to expect.

61. *Third*, the domains used by Fake ONNX are intentionally designed to mimic the name Microsoft and its products. This means that when a victim is phished and is redirected to a Fake ONNX-controlled domain, the victim will see a domain that on its face looks like a Microsoft domain. Entirely unsuspecting to Fake-ONNX criminal activities, the victim will not be suspicious of these domains because of how similar they appear. For example, sharepointonline-microsoft[.]com incorporates both "Microsoft" and "SharePoint," which is Microsoft's online document management platform. Likewise, loginoffice[.]com references "Office," which is the name Microsoft gives to a family of software that includes Word, Excel, and PowerPoint. In each instance, a victim who sees these domains would believe she is visiting a Microsoft website.

62. 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 in this way in the future. There is a

great risk that 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 blaming Microsoft for a phishing attack or believes that Microsoft's systems and products are not secure, it may be costly or impossible to convince the customer to return to Microsoft.

63. In connection with my investigation, I became aware that Fake ONNX Defendants and their phishing kits poses a significant risk to the financial sector. For example, In June 2024, The Financial Industry Regulatory Authority (FINRA), which acts as a self-regulatory organization that member brokerage firms and exchange markets published a cyber alert cautioning its member organizations about the dangers of Fake ONNX and their phishing kits[11]. Phishing is of particular concern for members the financial sector. Attached to my declaration as **Exhibit 3** is a true and correct copy of a letter I received from FINRA related to my investigation into Fake ONNX, which details the risk that Fake ONNX poses to its member organizations.

64. Microsoft has invested significant resources in excess of $5,000 to address and attempt to remediate the harm caused by Fake ONNX Defendants' crimes. Specifically, Microsoft has spent approximately $650,000, which represents the time that Microsoft DCU personnel have spent in efforts to investigate the Fake ONNX Defendants and their infrastructure.

DISRUPTING FAKE ONNX'S ILLEGAL ACTIVITY

65. The most vulnerable point in the Defendants' operations are technical infrastructure domains that are used by the Fake ONNX Defendants use to carry out their phishing campaigns.

[11] *ONNX Store Purportedly Targeting Firms in Quishing Attacks*, FINRA Cybert Alert, available at https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-onnx-store-purportedly-targeting-firms-quishing-attacks (last accessed Nov. 10, 2024).

These 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 exploit other Microsoft platforms like OneDrive.

66. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Fake ONNX 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 be prevented from going to the Defendants at the Fake ONNX-controlled domains, because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of the Fake ONNX Defendants.

67. Redirecting these Fake ONNX 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.

68. I believe that the most effective way to suspend the injury caused to Microsoft, its customers, including LF Projects, and the public, is to take the steps described in the Proposed Order. This relief will significantly hinder the Fake ONNX 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 Fake ONNX's malicious activities.

69. The Fake ONNX Defendants' techniques are designed to resist technical mitigation efforts, eliminating the ability to curb the injury purely through technical means. For example, once domains in the Fake ONNX 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.

70. For this reason, providing notice to the Fake ONNX Defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Fake ONNX 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. For this reason, as well, providing notice to the Fake ONNX Defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft.

71. Based on my experience observing the operation of numerous intrusions such as those carried out by the Fake ONNX Defendants, prior investigations, and legal actions involving such intrusions and actors, I believe that Fake ONNX 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.

72. 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.

73. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Fake ONNX 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 November 11, 2024 in Washington D.C.

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

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

EXHIBIT 2

Demo

Blog

June 19, 2024

5 min read

Dark Atlas Squad

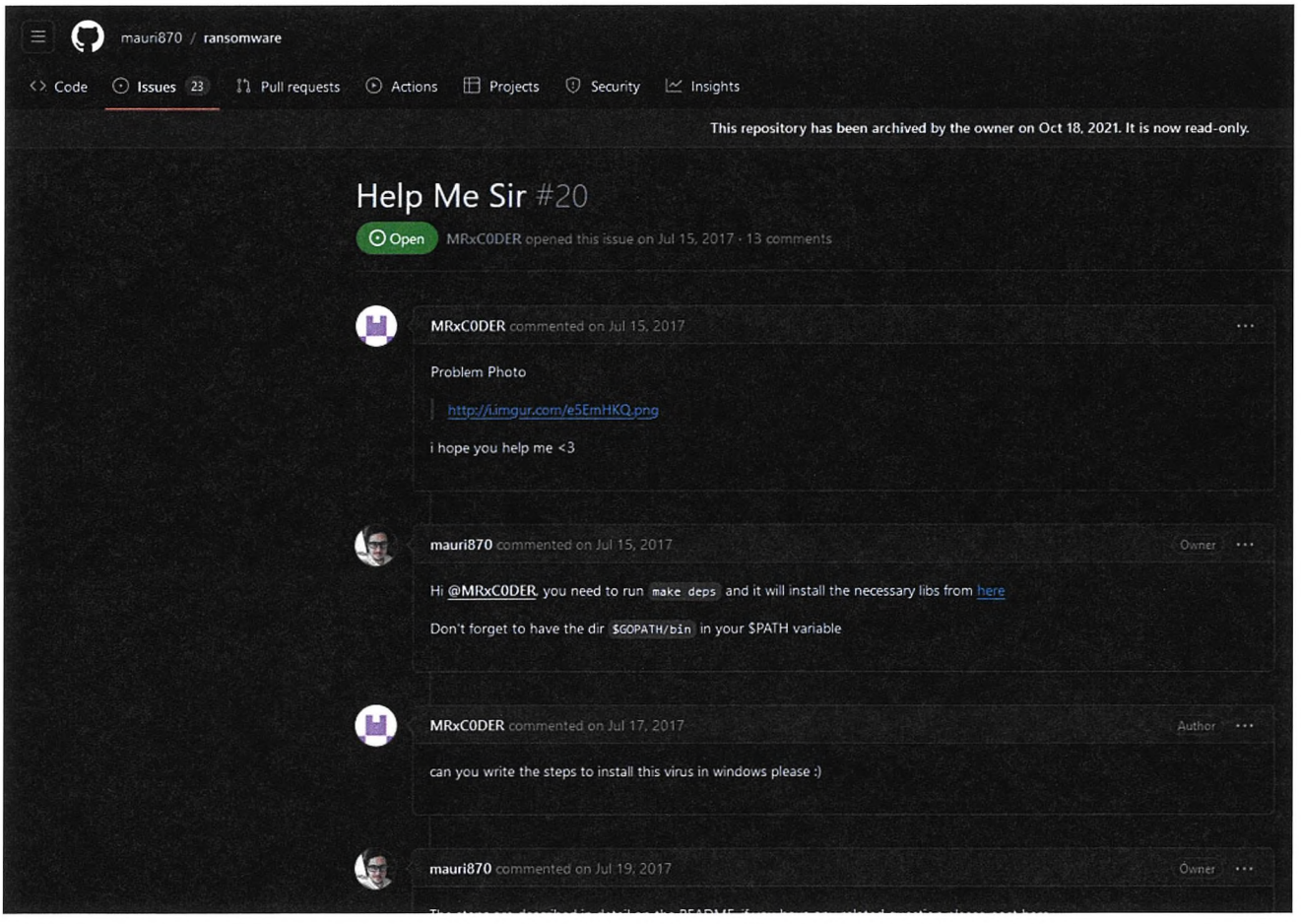
Share

Identity Reveal: The Threat Actor Behind ONNX Store and Caffeine Phishing Kit

Demo

Dark Atlas Squad initiated a thorough investigation into this threat actor, focusing not only on his infrastructure but also on his overall activities.
We started by performing Surface-Web Dorking using his username and alternative n ames.

We found a hit on GitHub for the username "MRxC0DER." The account was mostly empt y, except for one issue that opened in 2017, titled "Help Me Sir," which was related to a r ansomware problem.



Further investigation led us to any.run, where we discovered that "MRxC0DER-EG" had uploaded a ransomware sample from his computer. The "EG" in the username likely in dicates his nationality.

Demo

FileDescription:	MoWare H.F.D
FileVersion:	1.0.0.0
InternalName:	MoWare H.F.D.exe
LegalCopyright:	Copyright © 2017
OriginalFilename:	MoWare H.F.D.exe
ProductName:	MoWare H.F.D
ProductVersion:	1.0.0.0
Assembly Version:	1.0.0.0

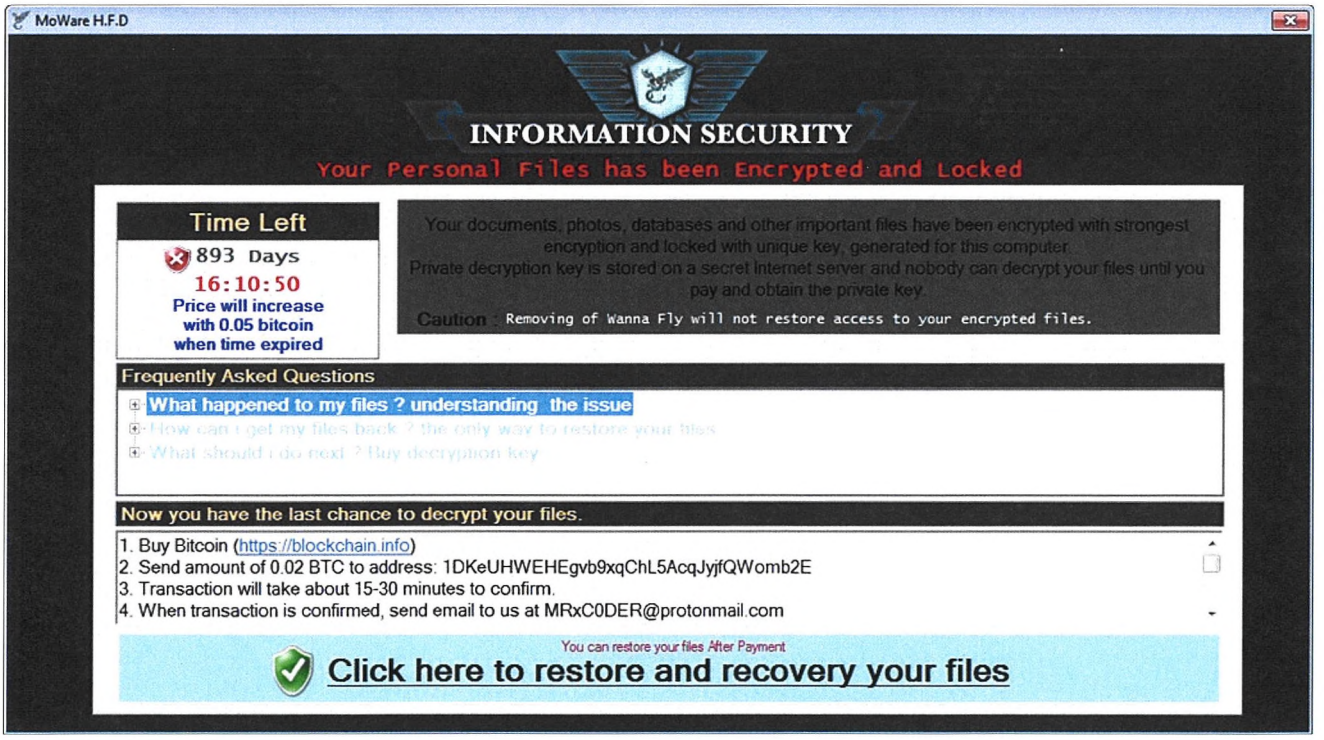
DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	4
Time date stamp:	26-Jul-2017 00:15:20
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE
	IMAGE_FILE_EXECUTABLE_IMAGE

The threat actor deployed and spread his ransomware version in 2017.



We also conducted Dark-Web Dorking using his username in the DarkAtlas.io InfoStealer Malware Logs database and found a match.

Demo


```
 country :  EG ,
"malware": "redline",
"operation_system": "Windows 10 Enterprise x64",
"source": "dark_atlas",
"source_index": "logs-000004",
"win_user": "Ra3'nar0x22",
"url": "https://forum.vnhax.com/index.php",
"backup_file": "KAqSBfeBxOHGWZSbwpBK.zip",
"password": "R@66729901rr",
"application": "Microsoft_[Edge]_Default",
"log_date": "2022-10-06",
"domain": "vnhax.com",
"sub_domain": "forum",
"email_domain": "",
"id": "KAqSBfeBxOHGWZSbwpBK",
"email": "MRxC0DER",
"hash": "9b8f38053c0a40616820be9ee9a97ccf",
"raw_url": "forum.vnhax.com",
"hardware": [
  "Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 6 Cores",
  "Intel(R) UHD Graphics, 1073741824 bytes",
  "NVIDIA GeForce RTX 2060, 4293918720 bytes",
  "Total of RAM, 16201.22 MB or 16988209152 bytes"
]
```


Further investigation revealed that this device belonged to an Egyptian affiliate, "A.G" (I dentity Masked)

During our investigation, we found an account on Zone-H with the same username. Th e account's last activity was in 2019, including his name and an associated domain. The "EG" in his defacement index further confirmed his nationality.

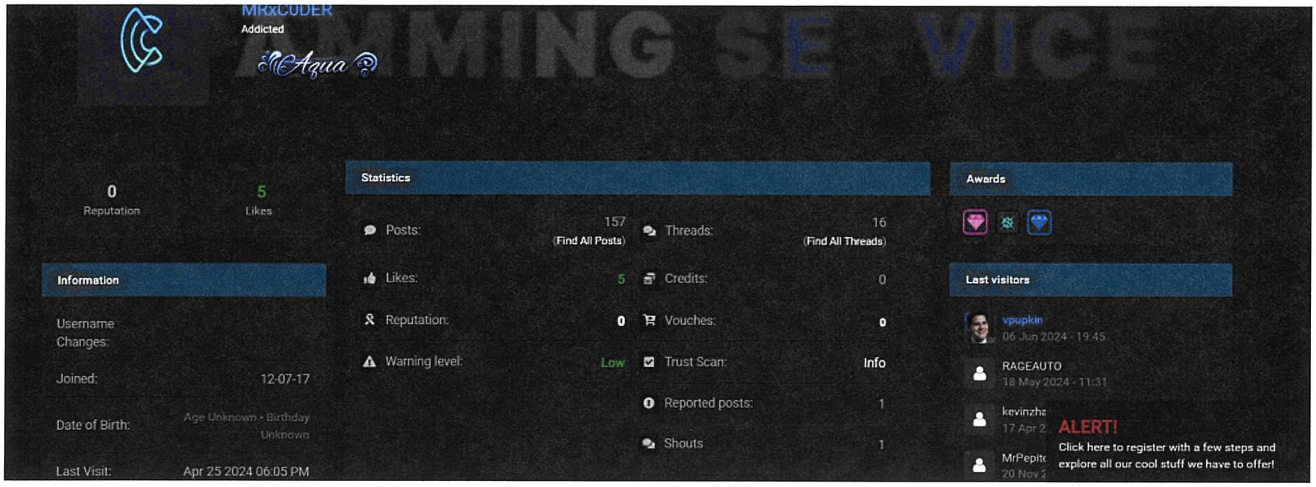
Demo

After examining the domain history of noxcheckers.com, we discovered it was hosted on GoDaddy and owned by an Egyptian.

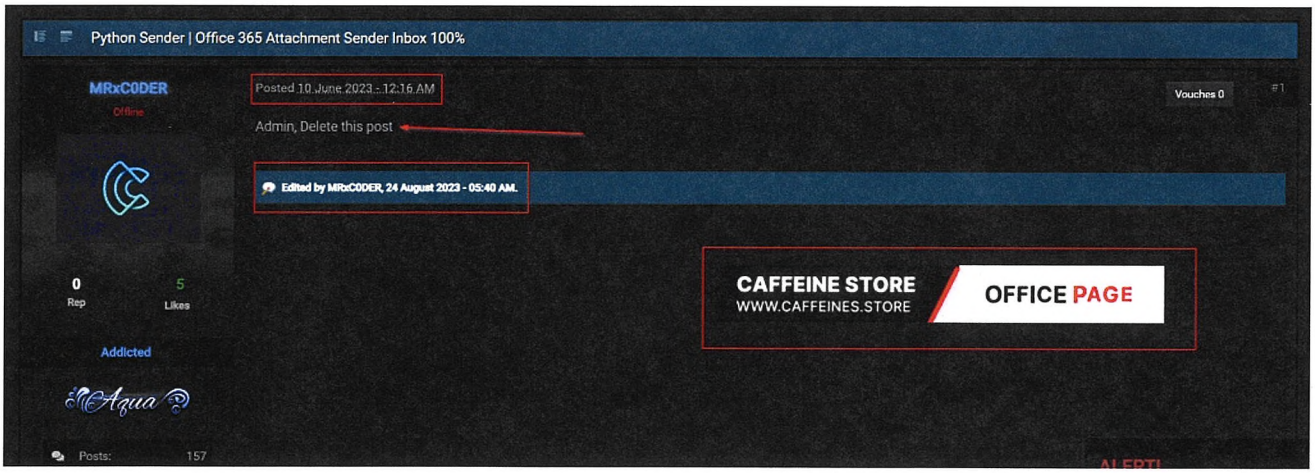
```
53892 noxcheckers.com 2018-11-25 17:13:45 2018-11-24 2018-11-24 2019-11-24 146
"GoDaddy.com, LLC" whois.godaddy.com http://registrar.godaddy.com Egypt Egypt
ns77.domaincontrol.com ns78.domaincontrol.com
```

We also searched underground forums and found a match for the same username on the Nulled forum, which has been active since 2017.

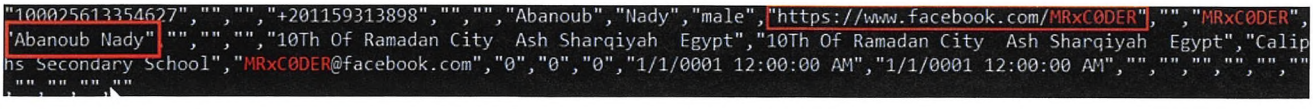
Demo



On June 10, 2023, he posted a thread on Nulled advertising his phishing kit "caffeines[.] store."
He later edited the thread and requested the admin to delete the post, which occurred after he gained attention in security news.



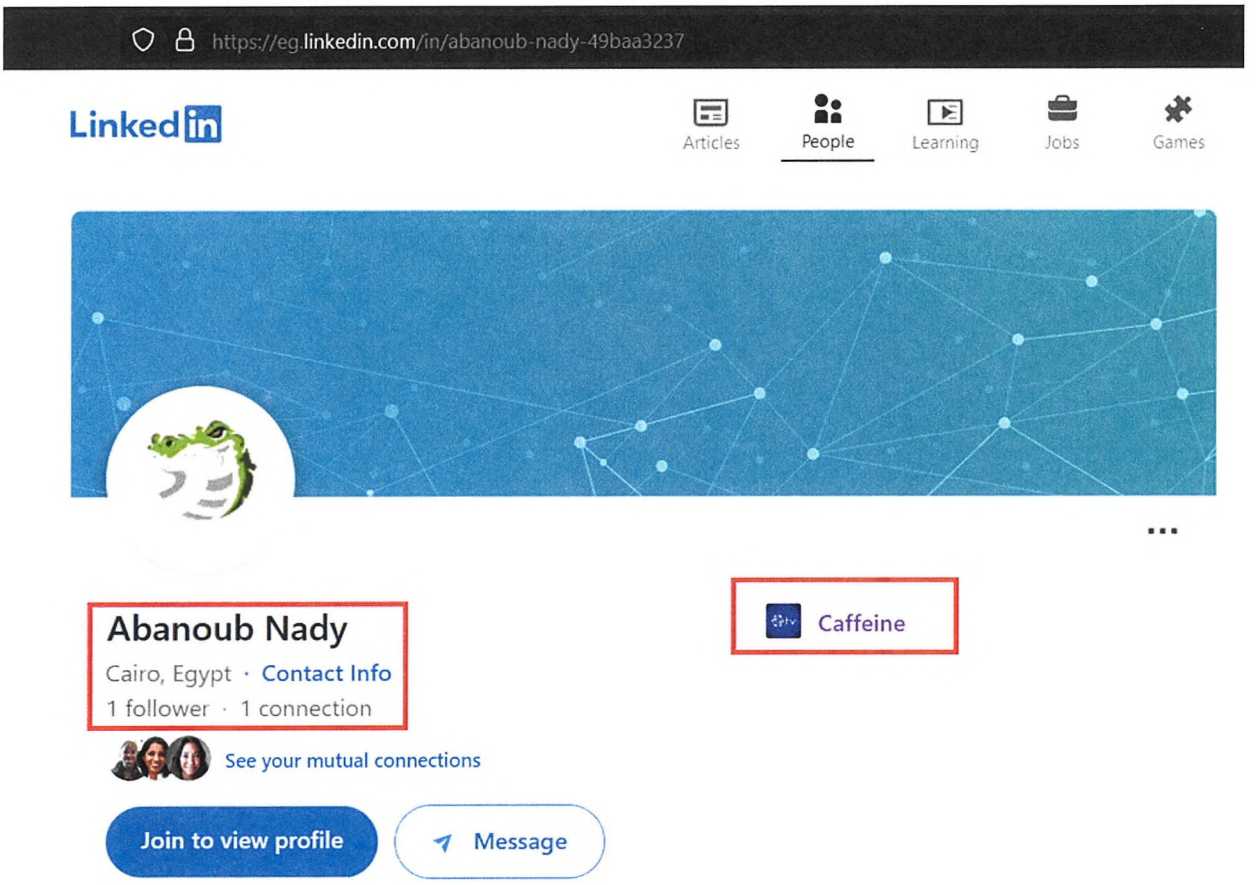
Next, we searched on social media for his nickname and found a matching account o n Facebook scraped data. This gave us his phone number, country, address, city, and f ull name.
Also, we noticed that he disabled this account.



Demo

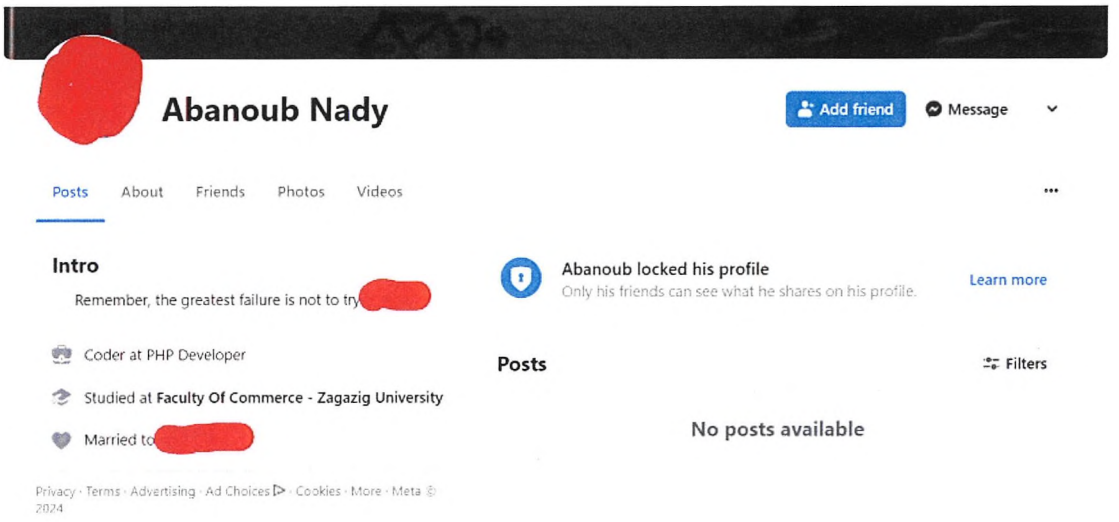
```
(186258,  'bebonady82@yahoo.com', '$2y$08$YhCcfVjA0U074UjUtMNxlObnbep6eGT4SY5EKALzRvbGuhuJkfLcy', 'Abanoub Nady', 2, 1, 1, 'الشرقية',
01159313898', '', 1, '826092790856765', '0 ,'' ,'' ,'' ,0 ,0 ,'["\20"\,"\18"\,"\6"\,"\3"\,"\2"\,"\1"\]' ,'الخلفاء الراشدين', NULL, 0, 0,
0, '1', '2016-03-31 19:14:33', '2016-03-31 23:41:19', '0000-00-00 00:00:00', '', 1, 1, 1, 0, 1, 0, 1, NULL, '1999-05-19', NULL,
0),
```

Using the collected data, we created some indicators leading us to his LinkedIn accou nt.



We also found his personal Facebook account.

Demo



Finally, using our underground agents and sources, we confirmed the credibility of the data.

Conclusion:

First Name: Abanoub
Last Name: Nady
Nickname: MRxC0DER
Alt names: MRxC0DER-EG, mrxc0derii
Projects: ONNX Store, Caffeine Phishing-as-a-Service Platform
Emails: bebonady82@yahoo.com, mrxc0der@protonmail.com, abanoubnady777@gmail.com
Country: Egypt
City: Sharqia
LinkedIn: https://www.linkedin.com/in/abanoub-nady-49baa3237/
Facebook: https://facebook.com/abanoubii

References

Demo

- https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_mowware.a

1.

Hashtags

Caffeine Phishing Kit ONNX Store Threat Actors

Share

Author

Dark Atlas Squad

Leave A Comment

Name

Demo

Send

Comments

Demo

New Security Updates Weekly!

Enter your email

DARK ATLAS

Call us

+1 (702) 381-9571

Send to us

info@darkatlas.io

Social Media

Threat Intelligence

Dark Web Monitoring

Attack Surface Management

Brand Protection

Demo

Careers

Privacy

Solutions

By Use Case

Data Leak Detection

Ransomware Protection

Dark & Deep Web Monitoring

Anti-Privacy

By Role

Threat Intelligence Teams

CISO

Security Operations

Solutions

By Industry

Financial Services

Technology

Healthcare

Government

Cyber Insurance

Demo

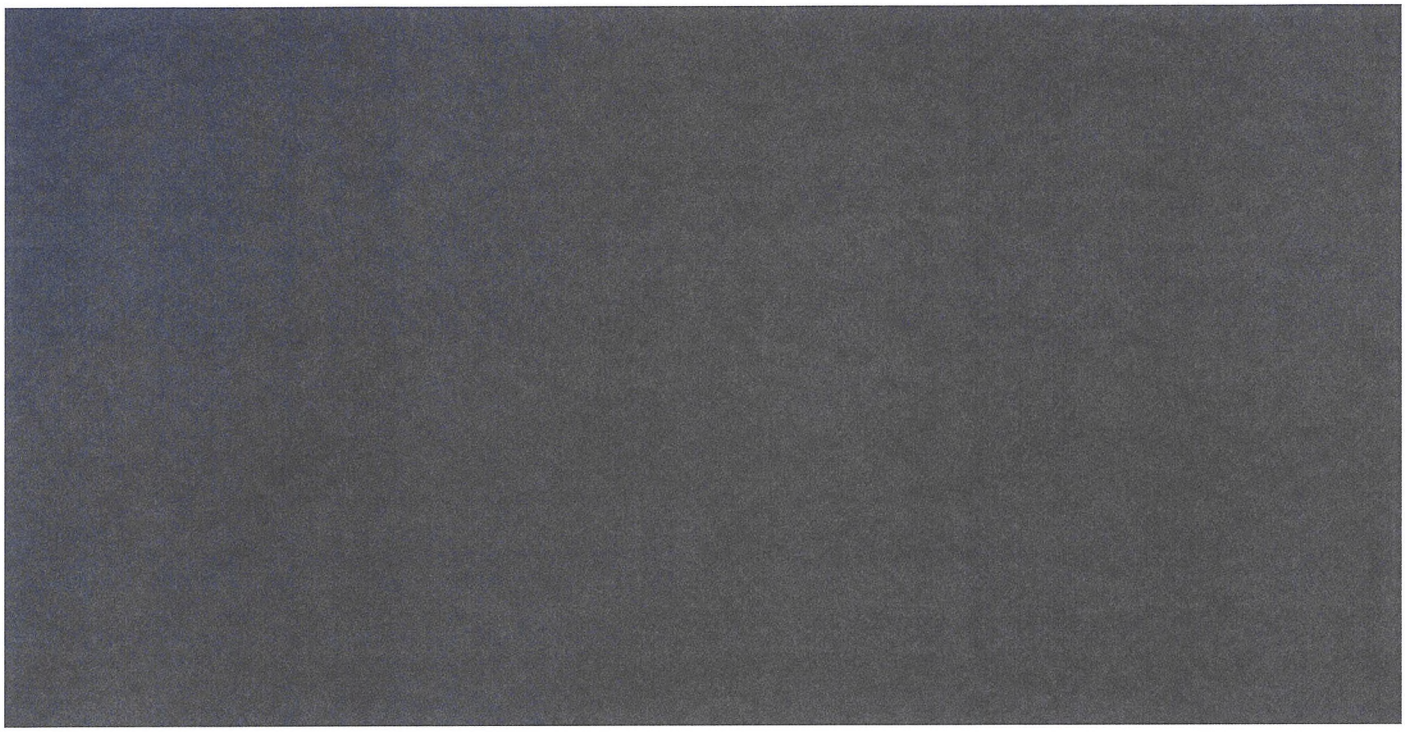


EXHIBIT 3

FINRA

November 11, 2024

Dear Jason Lyons,

I am a Senior Vice President overseeing the Cyber and Analytics Unit and the Cyber-Enabled Fraud Group at the Financial Industry Regulatory Authority, Inc. ("FINRA"). FINRA is a private, not-for-profit, self-regulatory organization that is tasked by Congress to make sure the broker-dealer industry operates fairly and honestly. FINRA's mission is to protect investors and the integrity of the securities markets.

FINRA member firms are broker-dealers that buy and sell securities on behalf of their customers, their own accounts, or both. FINRA makes rules with which its member firms, and their associated persons, are required to comply as a condition of their membership. Among its regulatory activities, FINRA enforces compliance by its member firms, and their associated persons, with FINRA's rules and the federal securities laws.

The Cyber and Analytics Unit conducts investigations in the cybersecurity, cyber-enabled fraud, and crypto-asset disciplines impacting investors and FINRA member firms. The Cyber-Enabled Fraud Group at FINRA investigates cyber incidents impacting investors and FINRA member firms. In addition to ensuring member firms comply with SEC and FINRA rules related to cybersecurity, FINRA reminds member firms that cybersecurity remains one of the principal operational risks facing broker-dealers. Cybersecurity incidents, such as account takeovers, ransomware or network intrusions, and any related exposure of customer information or fraudulent financial activity can expose member firms to financial losses, reputational risks, and operational failures that may compromise firms' ability to comply with a range of rules and regulations.

Given the evolving nature, increasing frequency, and mounting sophistication of cybersecurity attacks – as well as the potential for harm to investors, firms, and the markets – cybersecurity practices are a key focus for firms and FINRA. FINRA provides extensive resources to assist member firms with managing and addressing risks and threats that could pose harm to their business, compliance programs, and investors. For example, FINRA has recently seen an increase in the frequency and sophistication of cyberattacks – such as imposter websites and phishing campaigns – that target member firms, their customers and their employees. FINRA responds to these attacks, in part, by promptly issuing cybersecurity alerts or notices to warn firms.

In June 2024, FINRA published a cybersecurity alert on its website to notify member firms that ONNX Store, a Phishing-as-a-service platform (PhaaS), was targeting Microsoft 365 accounts at FINRA member firms with an advanced social

engineering attack known as quishing (a business email compromise attack that uses QR codes in embedded PDF documents to redirect victims to phishing URLs).[1] FINRA issued the alert to warn member firms of the threat. FINRA also advised member firms of effective practices they could implement to avoid becoming a victim of the ONNX Store's tactics. Providing member firms with information about potential cybersecurity threats is essential to FINRA's mission of protecting investors and the national securities markets.

Kind Regards,

Bryan Smith
Senior Vice President
Cyber and Analytics Unit and Cyber-Enabled Fraud Group
Financial Industry Regulatory Authority, Inc.

[1] https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-onnx-store-purportedly-targeting-firms-quishing-attacks