UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Seizure of Twelve (12) Domain Names, further described in Attachments A-1 and A-2	)	Case No. 4:24MJ3161 NCC

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

I, [redacted], being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that there is now certain property namely

Twelve (12) Domain Names, further described in Attachments A-1 and A-2

which is

subject to forfeiture under Title 18, United States Code, Sections 981(a) and 982(a) and Title 28, United States Code, Section 2461, and therefore, is subject to seizure under Title 18, United States Code, Sections 981(b)& 982(b), Title 21, United States Code, Sections 853(e)&(f) and Title 28, United States Code, Section 2461concerning a violation of Title 18, United States Code, Section 1956 and Title 50, United States Code, Section 1705.

Because the violation giving rise to this forfeiture occurred within the Eastern District of Missouri, this Court is empowered by 18 U.S.C. § 981(b)(3) and 28 USC § 1355(d) to issue a seizure warrant which may be executed in any district in which the property is found. The seized property is to be returned to this district pursuant to 28 U.S.C. § 1355(d).

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

Continued on the attached sheet and made a part hereof. X **Yes** ____ **No**

[redacted]

Signature of Affiant, Special Agent [redacted]

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

May 3, 2024
Date and Time Issued

at St. Louis, Missouri
City and State

Honorable Noelle C. Collins, U.S. Magistrate Judge
Name and Title of Judicial Officer

[redacted]

Signature of Judicial Officer

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF MISSOURI

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Case No.: 4:24MJ3161 NCC
NINE (9) .COM,	)	**Filed Under Seal**
ONE (1) .CLOUD,	)	
ONE (1) .NET, AND,	)	
ONE (1) .US	)	
DOMAIN NAMES	)	
	)	
	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [redacted], a Special Agent with the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent at the FBI. I have been a Special Agent with the FBI since March 4, 2007. Since [redacted]2010, I have been assigned to a cyber squad in the FBI's St. Louis Field Office. I have received training regarding computer fraud and computer hacking. I have conducted investigations into various forms of online criminal activity and am familiar with the ways in which such crimes are commonly conducted. In addition, I have participated in the execution of search warrants involving electronic evidence.

2. I submit this application in support of seizure warrants for the twelve (12) domain names described below and in Attachments A-1 and A-2 (the "**Subject Domain Names**") used by North Korean IT workers to support their scheme to generate revenue for the North Korean regime. Based on my training and experience and the facts as set forth in this affidavit, there is

probable cause to believe that the **Subject Domain Names** are subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1) because they are property involved in transactions or attempted transactions that violate 18 U.S.C. § 1956(a)(2)(A) (International Promotion Money Laundering), done with the intent to promote the carrying on of specified unlawful activity, specifically felony violations of 50 U.S.C. §§ 1701-1706 (the International Emergency Economic Powers Act, or "IEEPA"). As explained in more detail below, unknown and known foreign persons transferred funds from a place outside the United States to a place in the United States to register the **Subject Domain Names** with the intent to promote the carrying on of a North Korean revenue generation scheme in violation of U.S. sanctions. Because the **Subject Domain Names** are subject to civil and criminal forfeiture, they may be seized by warrant pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(f). The procedure by which the government will seize the **Subject Domain Names** is described in Attachments A-1 and A-2, hereto and below.

3. The facts set forth in this affidavit are based on my personal knowledge, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

APPLICABLE STATUTES AND REGULATIONS

International Emergency Economic Powers Act (IEEPA)

4. IEEPA, enacted in 1977 and codified at 50 U.S.C § 1701 *et seq.*, authorizes the President of the United States (the "President"), among other things, to impose economic sanctions in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States. Pursuant to that authority, the President may declare a national emergency through Executive Orders with respect to that threat; those Executive Orders have the full force and effect of law. It is a crime to willfully violate, attempt to violate, conspire to violate, or cause the violation of any license, order, regulation, or prohibition issued pursuant to IEEPA. 50 U.S.C. § 1705(a).

5. Beginning with Executive Order 13466, issued on June 26, 2008, the President found the situation "on the Korean Peninsula constitute[s] an unusual and extraordinary threat to the national security and foreign policy of the United States and . . . declare[d] a national emergency to deal with that threat."

6. On March 15, 2016, the President, in order to take additional steps with respect to the previously described national emergency, issued Executive Order 13722 addressing the Government of North Korea's continuing pursuit of its nuclear and missile programs. Executive Order 13722 imposed a comprehensive blocking of the Government of North Korea and the Workers' Party of Korea. Pursuant to that authority, on March 5, 2018, the Secretary of the Treasury amended the "North Korea Sanctions Regulations." 83 Fed. Reg. 9182 (Mar. 5, 2018); *see* 31 C.F.R. § 510.101 *et seq.* Executive Order 13722 and the North Korea Sanctions Regulations prohibit the export of financial services from the United States or by any U.S.

person to North Korea, unless exempt or authorized by the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC"). Under these orders, U.S. financial institutions were barred from providing correspondent banking services to North Korea entities.

7. OFAC administers and enforces economic sanctions programs established by executive orders issued by the President pursuant to IEEPA. Pursuant to Executive Order 13722, OFAC has the authority to block all property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of persons who meet specific criteria.

8. On September 13, 2018, OFAC designated a North Korean information technology firm based in China named Yanbian Silverstar Network Technology Co., Ltd ("Yanbian Silverstar"), as well as its Russia-based front company, Volasys Silver Star, for having engaged in, facilitated, or been responsible for the exportation of workers from North Korea, including exportation to generate revenue for the Government of North Korea or the Workers' Party of Korea, pursuant to Executive Order 13722, and for operating in the IT industry in North Korea, pursuant to Executive Order 13810. OFAC further designated a North Korean national, Jong Song Hwa, identified by OFAC as the CEO of Yanbian Silverstar and Volasys Silver Star.

9. According to the OFAC designation press release, the sanctioned parties channeled "illicit revenue to North Korea from overseas information technology workers disguising their true identities and hiding behind front companies, aliases, and third-party nationals." In other words, the sanctioned parties were conspiring to create and use pseudonymous email accounts, social media accounts, payment platform accounts, websites, and

online job site accounts to obfuscate their true identities as North Koreans, and to solicit and perform information technology freelance jobs to earn money for the North Korean government in violation of U.S. sanctions.

10. Title 18, United States Code, Section 1956(a)(2)(A) (International Promotion Money Laundering) prohibits the transportation, transmission, or transfer of monetary instruments or funds from the United States to or through a place outside the United States, or to the United States from or through a place outside the United States with the intent to promote the carrying on specified unlawful activity. Specified unlawful activity is defined in 18 U.S.C. § 1956(c)(7)(D) to include violations of 50 U.S.C § 1705.

Civil and Criminal Forfeiture

11. 18 U.S.C. § 981(a)(1)(A) (civil forfeiture) provides for the forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of, inter alia, 18 U.S.C. § 1956, as well as any property traceable to such property.

12. 18 U.S.C. § 982(a)(1) (criminal forfeiture) provides that, as part of the sentence for a violation of, inter alia, 18 U.S.C. § 1956, the Court shall order the forfeiture of any property, real or personal, involved in the offense or any property traceable to that property.

13. Pursuant to 18 U.S.C. § 981(b) (civil seizure), property subject to civil forfeiture may be seized by a warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed," and may be executed "in any district in which the property is found," if there is probable cause to believe the property is subject to forfeiture. A civil forfeiture action may be brought in any district where "acts or omissions giving rise to the forfeiture occurred." 28 U.S.C. § 1355(b)(1)(A).

14. 21 U.S.C. § 853(f) (criminal seizures) authorizes the seizure of property subject to criminal forfeiture based upon a warrant supported by probable cause where the property to be seized would, in the event of conviction, be subject to forfeiture.

15. Seeking a restraining order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture because there is reason to believe that the property is under the control of the targets of this investigation, who cannot reasonably be relied upon to abide by an order to maintain the property in substantially the same condition as it is at the present time, in order to ensure that it will be available for forfeiture. More particularly, providing notice may allow the targets to frustrate further efforts of law enforcement by transitioning their enterprise and infrastructure to jurisdictions beyond the reach of United States law enforcement.

BACKGROUND REGARDING NORTH KOREAN INFORMATION TECHNOLOGY WORKERS

16. According to a May 16, 2022, report jointly issued by the U.S. Department of State, U.S. Department of the Treasury, and the FBI, North Korea uses freelance information technology workers to generate a revenue and foreign currency stream for its weapons of mass destruction and ballistic missile programs.

17. The freelance North Korean IT workers deceive their employers by buying, stealing, or counterfeiting the identities and mailing addresses of non-North Koreans when bidding on and completing freelance projects, in order to conceal their identities as North Koreans.

18. North Korean IT workers also either pay or deceive non-North Koreans to

interview for jobs for them, accept payment for freelance projects, and videoconference with their employers when necessary. These non-North Koreans may not be aware that the IT workers are North Korean.

19. North Korean IT workers use multiple accounts and multiple freelance contracting platforms, digital payment platforms, social media and networking applications, and email and messaging applications, in order to obtain and perform IT contracts, receive payment for their work, and launder those funds. North Korean IT workers also create software development companies to hire other developers and provide a presence on the internet to bolster their legitimacy and mask their true identities. These "portfolio websites" allow North Korean IT workers to showcase previous development activity and generate freelancer jobs.

20. The North Korean IT workers are often located in China and Russia. In order to avoid suspicion that they are North Korean and be able to use U.S.-based online services, North Korean IT workers use virtual private networks, virtual private servers, and proxy IP addresses to appear that they are connecting to the internet from false locations. North Korean IT workers also use remote desktop software to access U.S.-based computers to make it appear as though that they are connecting to online services from different locations.

BACKGROUND ON DOMAIN NAMES

21. Based on my training and experience and information learned from others, I am aware of the following:

a. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric or alphanumeric address used by computers on the Internet (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from

and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

b. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

c. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and is the web server.

d. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol ("IP") addresses.

e. Registry: For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".com" and ".net" top-level domains are Verisign, Inc., which has its headquarters in Reston, Virginia. The ".cloud" domain is owned by Aruba PEC SpA which is one of Europe's largest hosting providers based in Italy. The ".us" domain is owned by

GoDaddy Inc., which is headquartered in Tempe, Arizona.

f. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular domain resolves to through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

g. WHOIS: A "WHOIS" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A WHOIS record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a WHOIS record for the domain name XYZ.COM might list an IP address range of 12.345.67.0-12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0-12.345.67.99.

FACTS ESTABLISHING PROBABLE CAUSE TO BELIEVE CRIMES HAVE BEEN COMMITTED

22. In August 2019, the FBI interviewed an individual ("Individual 1") who had allowed another person, subsequently identified as a North Korean IT worker working for Yanbian Silverstar, to use Individual 1's online account at a U.S. based freelancer platform.

Additionally, Individual 1 allowed the North Korean IT worker to remotely access laptops at Individual 1's residence in the United States for freelance work, and the North Korean IT worker paid Individual 1 $100 per month per hosted laptop.

23. The investigation subsequently identified hundreds of financial and communication accounts associated to Yanbian Silverstar and other North Korean IT worker groups. In February 2022 and July 2022, United States Magistrate Judges Shirley P. Mensah and John M. Bodenhausen in the Eastern District of Missouri signed search warrants for numerous Google and Microsoft accounts associated with Yanbian Silverstar actors. The communications from these Google and Microsoft accounts discussed using identities of U.S. citizens and individuals based around the world to open accounts at payment and freelancer platforms. They also used Korean language and North Korean honorifics to communicate with each other. Those communications clearly identified them as North Koreans doing IT work on behalf of North Korea.

24. During the course of the investigation, I discovered that North Korean IT workers create and use domain names and limited liability companies (LLCs) in furtherance of their fraudulent activity and to mask their true identities as North Koreans. The LLCs are used to recruit "Virtual Assistants" who can receive and ship devices needed for the North Korean IT workers as well as recruit and employ software developers from countries such as Pakistan, India, and China. These LLCs are often registered in the United States through business registry services and sometimes use the identities of individuals who had a previous relationship with North Korean IT workers.

25. In October 2023, United States Magistrate Judge Rodney H. Holmes in the Eastern District of Missouri signed seizure warrants for 17 domain names used by North Korean IT workers. Since these seizures, the FBI has identified additional domains, including the **Subject Domain Names**, used by North Korean IT workers. The **Subject Domain Names** are described below in groups based on their associated LLC or company name.

A. Group A – Eden Programming Solutions

Domains: illusionsoft.net; omegasoftware.us

26. Eden Programming Solutions was identified as a front company used by Yanbian Silverstar IT workers to obtain freelancer jobs and to hire developers and facilitators to assist in their revenue generation.

27. Eden Programming Solutions' domain name, *edenprogram.com*, was seized by the FBI on October 16, 2023, pursuant to a warrant signed on October 5, 2023, by United States Magistrate Judge Rodney H. Holmes (4:23-MJ-09240-RHH). The application for that warrant, including the supporting affidavit, are incorporated into this affidavit by reference. On or about October 17, 2023, the FBI received an online complaint from an individual who had been hired by Eden Programming Solutions to interview for a job Eden Programming found for him. The individual saw the Eden Programming Solutions domain had been seized by the FBI and then checked the [redacted] used by Eden Programming Solutions. According to this individual, and later confirmed by the FBI, the [redacted] name had been changed to "Illusion Software Development" [redacted]) using the domain **illusionsoft.net**.

28. Records provided on or about November 17, 2023, by Tucows Inc. ("Tucows"), a company with offices located in Bellevue, Washington and the registrar for the domain

illusionsoft.net, revealed that the registrant of this domain used the following email address: [redacted]. Additionally, records from Tucows showed that two more domains used the same registrant email address [redacted]): *edenprogram.com* (which was already seized) and **omegasoftware.us**.

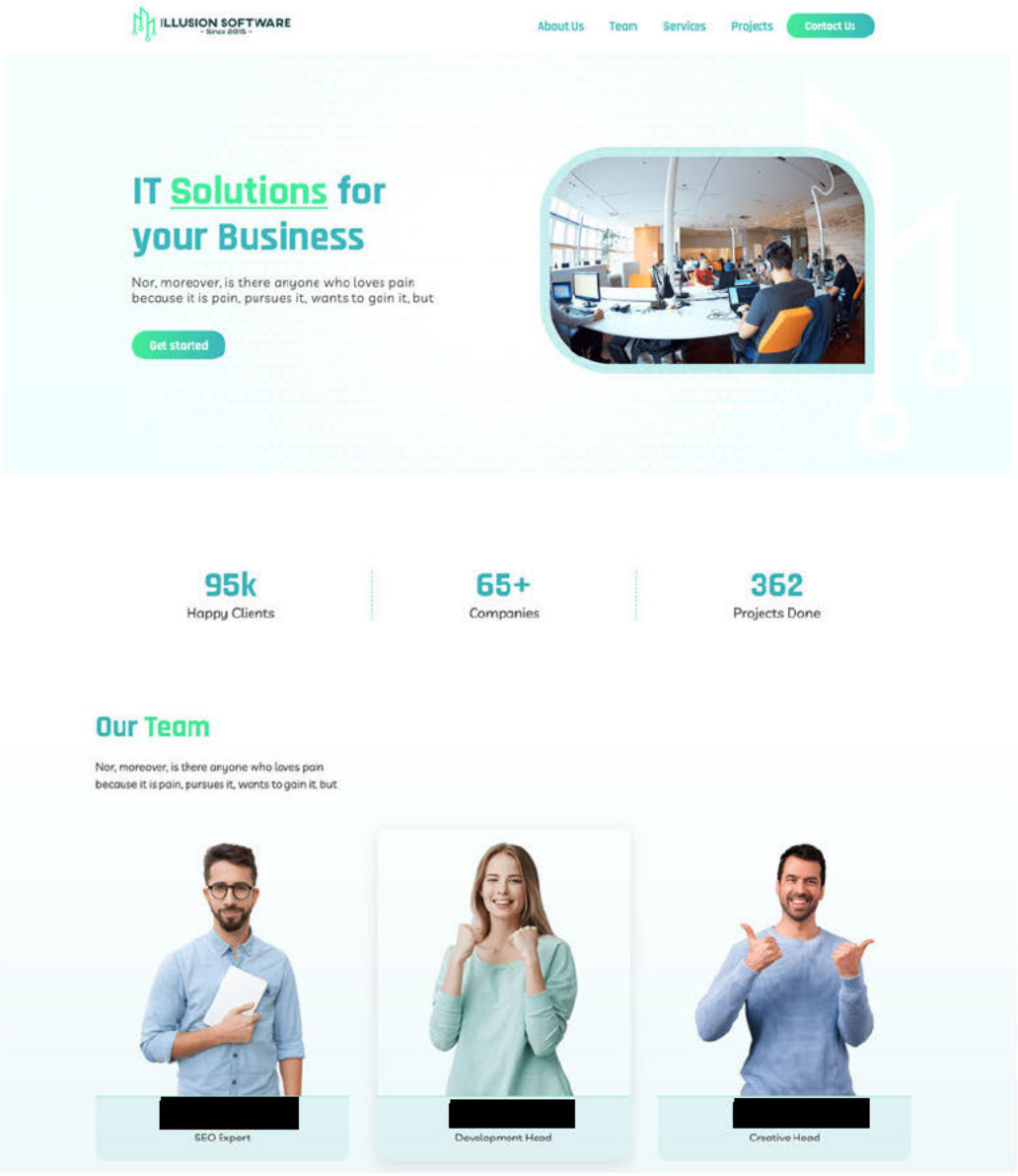
29. According to Tucows records, **illusionsoft.net** and **omegasoftware.us** were registered through Tucows using a reseller, SG Hosting Inc. ("SG Hosting") located in Alexandria, Virginia. Records provided by SG Hosting on or about December 8, 2023, revealed, the following information for the domains:

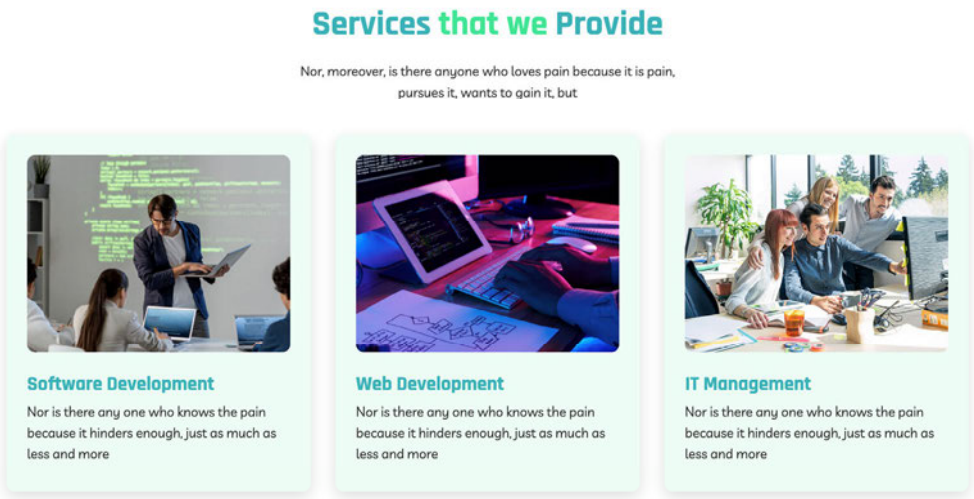
a. **illusionsoft.net** – Created: 10/17/2023; Expires: 10/17/2024

b. **omegasoftware.us** – Created: 10/27/2023; Expires: 10/27/2024

30. A Mastercard in the name of [redacted] (name anonymized) was used to pay for both domains. I know from my training, experience, and the evidence collected in this investigation as detailed in the warrant application in 4:23-MJ-09240-RHH that [redacted]. is an alias used by the North Korean IT worker who controlled the domain *edenprogram.com* and sought employment by U.S.-based companies. Based on information obtained pursuant to a Google search warrant, 4:22-MJ-7027-SPM-09, signed by the Honorable Shirley P. Mensah, on February 9, 2022, I have probable cause to believe the [redacted]. alias is controlled by a North Korean IT worker based outside the United States named [redacted]. Those search returns revealed an email communication, dated December 6, 2017, from [redacted]. in which he identified himself as [redacted]. and provided a resume to a potential employer.

31. On or about November 17, 2023, I visited the website at the domain **illusionosft.net**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

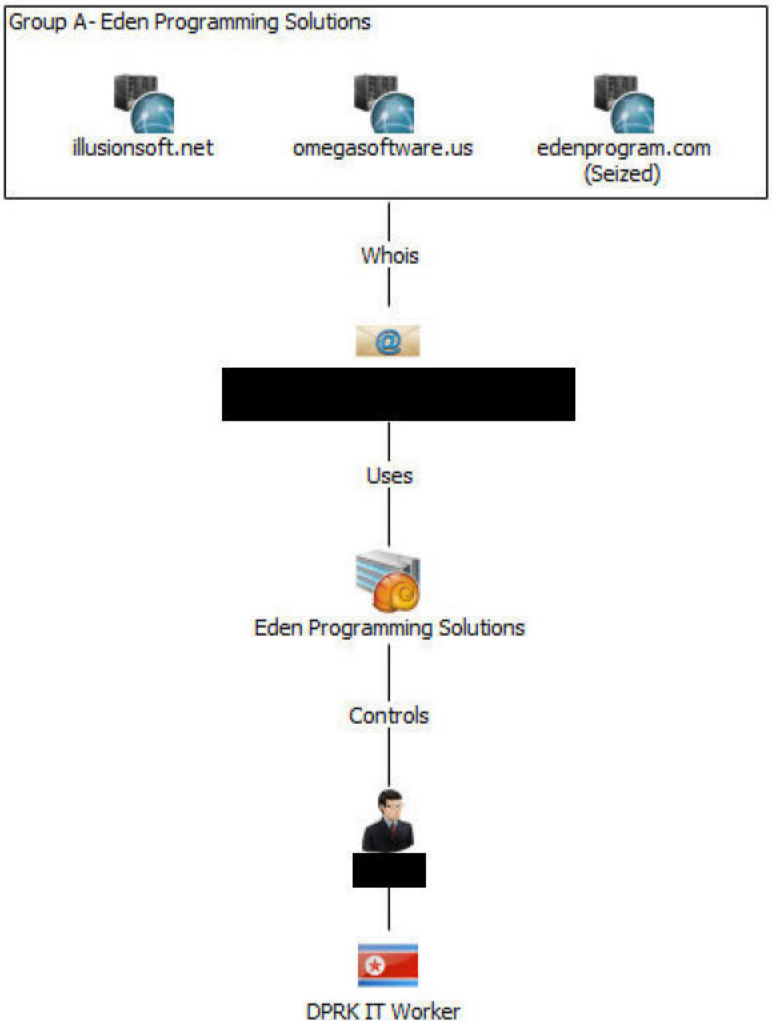




32. On or about January 8, 2024, I visited the website at the domain **omegasoftware.us** which indicated the site was under construction.

33. Below is a chart which summarizes these connections between the domains and a North Korean IT worker:

Chart for Group A – Eden Programming Solutions



34. Based on the above, there is probable cause to believe that the funds originating from [redacted] – a DPRK IT worker based outside the United States – were sent into the United States in order to purchase **illusionsoft.net** and **omegasoftware.us** and that these domains were used with the intent of promoting the carrying on of a conspiracy to violate IEEPA. **Illusionsoft.net** and **omegasoftware.us** are therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

B. Group B – Blackish Tech LLC / Purpleish Tech LLC / Culture Box LLC / Next Nets LLC

Domains: blackishtech.com; logictech.us; purpleishtech.com; culturebx.com; and nextnets.com

35. On or about December 8, 2023, the FBI interviewed Individual 2, who was a "Virtual Assistant" for Eden Programming Solutions, which owned the website *edenprogram.com*. On or about December 8, 2023, Individual 2 received a FedEx package from a U.S. state government entity which contained a laptop. The FBI instructed Individual 2 to cease communications with individuals associated to Eden Programming Solutions and provide the laptop to the FBI. On or about December 11, 2023, Individual 2 was contacted by an unknown person ("Individual 3") by telephone. Individual 3 stated he worked for "Blackish Tech." Individual 3 stated he was instructed to come by and pick up the laptop received by Individual 2. On or about December 12, 2023, Individual 3 came to Individual 2's residence and attempted to get the laptop. The FBI believes Individual 3, who came to Individual 2's residence, worked for the same group of North Korean IT workers and needed the laptop to be shipped to another facilitator so they could access it and maintain their employment with the U.S. state government entity. Individual 3 was subsequently identified from his telephone number and picture, provided by Individual 2's doorbell camera. As described below, Individual 2 is associated with **blackishtech.com**.

36. On or about December 19, 2023, I conducted open source research for Blackish Tech and identified an LLC named, Blackish Tech LLC, registered in Wyoming using a registered agent. A website at the domain, **blackishtech.com**, was identified.

37. A review of WHOIS information for **blackishtech.com** identified the registrant as J.P. (anonymized), stated J.P. was located at [redacted], provided the email address [redacted], and telephone number [redacted]. The domain was created on January 25, 2022, and expires on January 25, 2025, and was registered at Public Domain Registry LTD ("Public Domain Registry"), a domain registrar located in Tempe, Arizona.

38. The FBI had previously identified the domain registration email address, [redacted]. On or about March 17, 2022, in response to a search warrant signed by Magistrate Judge Shirley P. Mensah in the Eastern District of Missouri (4:22-MJ-7028-SPM), the facts of which are incorporated into this affidavit by reference, Microsoft provided records for a communication account used by a North Korean IT worker, identified as [redacted] (anonymized), for Yanbian Silverstar. The records obtained pursuant to 4:22-MJ-7028-SPM show that on or about February 26, 2021, [redacted]. sent the email address [redacted] to a North Korean IT worker group leader, identified as [redacted]. (anonymized). Additional conversations with other North Korean IT workers, which were found in Microsoft's records, indicated payments were to be sent to or withdrawn from an account with an identified payment service provider ("Payment Service Provider 1"). According to records from Payment Service Provider 1, this account was registered to email address [redacted].

39. On or about January 12, 2024, Newfold Digital, Inc. ("Newfold Digital"), which is based in Jacksonville, Florida and owns Public Domain Registry, provided records for **blackishtech.com** which confirmed the registrant information listed on WHOIS and identified

the use of a reseller to register the domain, Sineris Web Services, which is based in Kissimmee, Florida.

40. On or about February 20, 2024, Sineris Web Services provided records for the domain **blackishtech.com**, which confirmed the registrant information listed on WHOIS and provided several payment methods used to pay for the domain. The following payments were made:

Date	Amount	Method
01/12/2023	$12.00	Visa Debit Card - U.S. Financial Bank 1 Card Owner: [redacted]
01/18/2023	$17.95	Visa Debit Card - U.S. Financial Bank Card Owner: [redacted]
08/08/2023	$9.50	Payment Service Provider 1 account [redacted]
01/18/2024	$39.60	Visa Debit Card - U.S. Financial Bank 1 Card Owner: [redacted]

41. As described above, **blackishtech.com** was registered to telephone number [redacted]. A review of records at Domain Tools identified an additional domain registered using the telephone [redacted], **logictech-us.com**. A review of WHOIS information for **logictech-us.com** identified the domain was created on December 3, 2021, expires on December 3, 2024, and had the following registrant information:

Name: [redacted].

Organization: Upwork
Street: [redacted]
City: [redacted]
State: WV
Zip: 25235
Email: [redacted]
Telephone: [redacted]

42. Microsoft search warrant returns for an account owned by [redacted] revealed that, on or about December 3, 2021, [redacted] sent an unidentified North Korean IT worker a copy of an email regarding the setting up of the hosting account for the domain **logictech-us.com** at Ahead Host, LLC, a domain reseller based in Rocky Hill, Connecticut. These returns also revealed that, on or about June 12, 2020, [redacted] sent the telephone number "[redacted]" to North Korean IT group leader [redacted], and subsequently sent two six-digit codes to [redacted]. There were additional instances of [redacted] providing the telephone number and sending a six-digit code to [redacted]. The most recent occurred on or about December 15, 2021. Based on the codes, the FBI believes [redacted] was receiving the verification codes that were sent to telephone number [redacted], which was controlled by [redacted].

43. On or about January 16, 2024, records from Payment Service Provider 1 for an account belonging to Individual 3, identified multiple payments from "Blackish Tech," and associated account identifier [redacted], totaling $5,505.00 USD from December 2022 to September 2023 and one payment from "Purpleish Tech LLC," an associated account identifier [redacted], for $750.00 USD on November 11, 2023. The name "Purpleish Tech" is similar to "Blackish Tech". Based on my training and experience I know that when criminals seek to register multiple domains for the same use, they will often choose a

single theme or motif. Doing this helps the criminal remember the names of multiple domains. In this instance, that theme was clearly color.

44. On February 2, 2024, I conducted open source research on "Purpleish Tech LLC" and identified an LLC registered on July 24, 2023 with the mail address [redacted] and the website at **purpleishtech.com**. According to WHOIS the domain was registered using Tucows on August 2, 2023 and expires on August 2, 2024.

45. On or about February 28, 2024, Tucows provided the registrant information for the domain **purpleishtech.com** as [redacted]'s (anonymized), [redacted], email address [redacted] (same as **blackishtech.com**), and telephone number [redacted] (a digit is missing). The registrant provided their organization as "Blackish Tech LLC." The domain was registered through a domain reseller, InterServer, Inc., located in Englewood Cliffs, NJ.

46. On or about March 29, 2024, InterServer, Inc. provided information for the domain **purpleishtech.com** which confirmed the registrant information on the WHOIS. Additionally, the payment information was provided showing that the domain was registered using a Payment Service Provider 1 account, the email address [redacted], and the business name "Blackish Tech". On or about January 16, 2024, records from Payment Service Provider 1 for "Blackish Tech", [redacted], identified a payment made to InterServer from on August 2, 2023, the date of the domain's registration.

47. According to Tucows, two additional domains used the email address [redacted]: **culturebx.com** and **nextnets.com**, using the reseller InterServer, Inc. The original WHOIS information for **culturebx.com** showed that it was originally owned by [redacted]

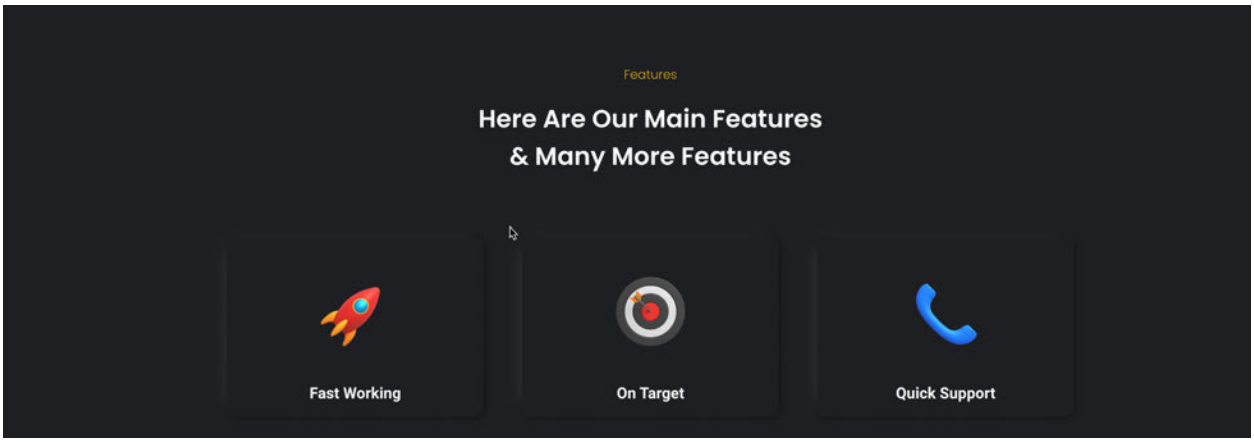
(the same individual discussed above), [redacted], Culture Box, [redacted], and this information was subsequently changed on October 13, 2022, to [redacted]. (the same individual discussed above), [redacted], Culture Box, [redacted]. The domain **culturebx.com** was registered on May 13, 2022, and expires on May 13, 2025. The WHOIS information from Tucows for **nextnets.com** showed that it was registered to [redacted] email address [redacted], and telephone number [redacted]. The domain **nextnets.com** was registered on March 7, 2023, and expires on March 7, 2025.

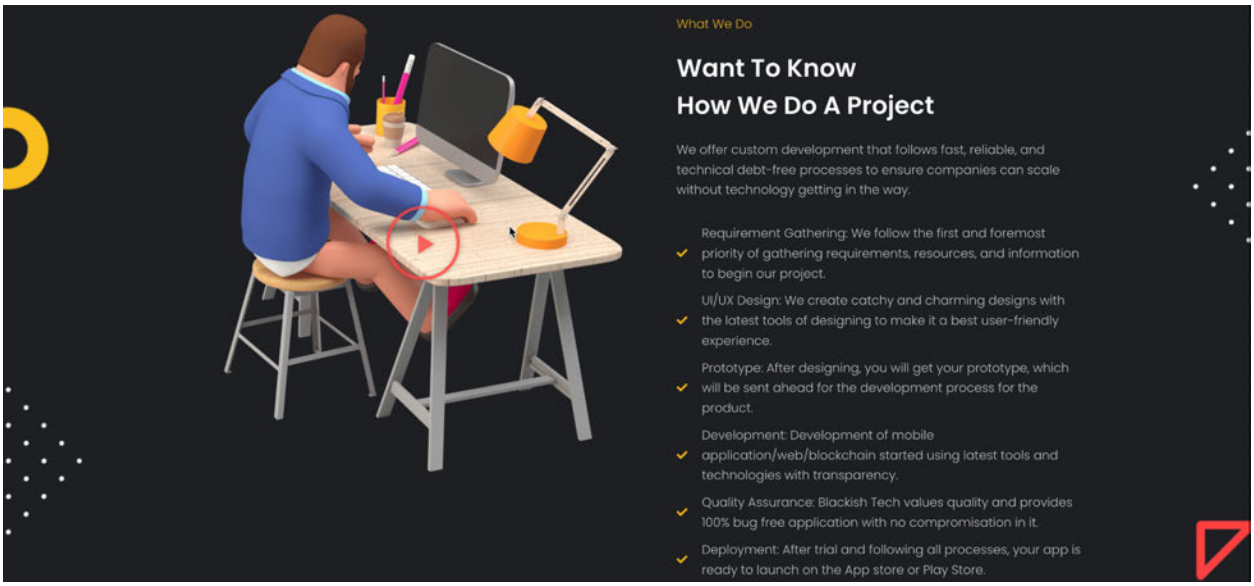
48. On or about March 29, 2024, InterServer, Inc. provided information for the domains **nextnets.com** and **culturebx.com** which confirmed the registrant information on the WHOIS. Additionally, the payment information for the domain **nextnets.com** showed that it was registered using a Payment Service Provider 1 account, the email address [redacted], and the business name "Blackish Tech". On or about January 16, 2024, records from Payment Service Provider 1 for "Blackish Tech" and the email [redacted] identified two payments to InterServer on March 7, 2023 – the date of the domain's registration. A payment for the domain **culturebx.com** was made on May 12, 2022, using a MasterCard credit card in the name of [redacted]. – a suspected Brazilian national, with the address of [redacted], and the email address [redacted]. The alias of M.T. has been observed in Payment Service Provider 2 records receiving payments from known North Korean IT worker-controlled payment accounts.

49. On or about March 20, 2024, records from Payment Service Provider 2 identified an account for "Culture Box LLC" in the name of [redacted] and the telephone number [redacted], which is the same telephone identified on the [redacted] Payment Service Provider 1 account discussed above. A review of the in network payments at Payment Service Provider 2 identified a payment of $240 was sent on December 28, 2023 to [redacted]'s account (Blackish Tech). Additionally, a payment of $780 was sent from Individual 3 to [redacted]'s account on November 15, 2023.

50. On or about January 8, 2024, I visited the website at the domain **blackishtech.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

blackishtech.com

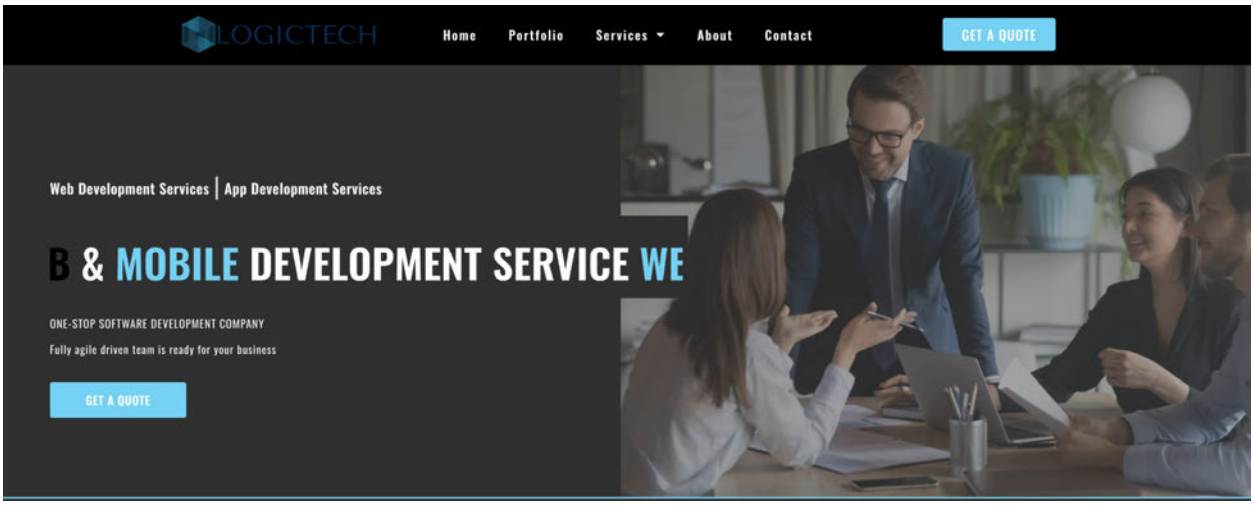


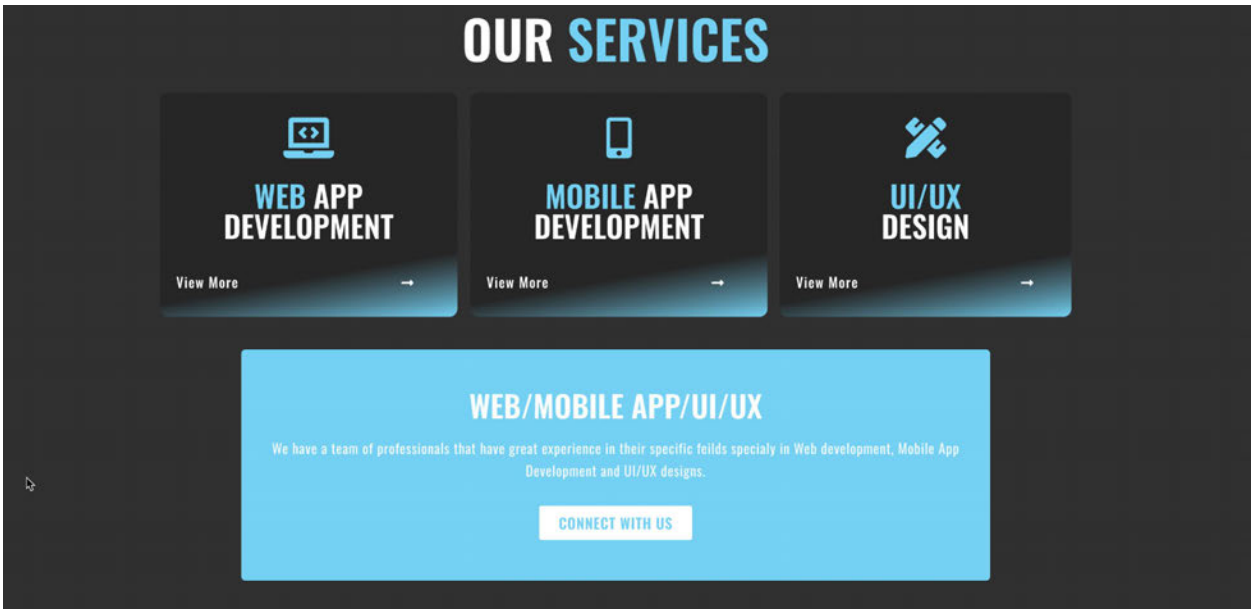


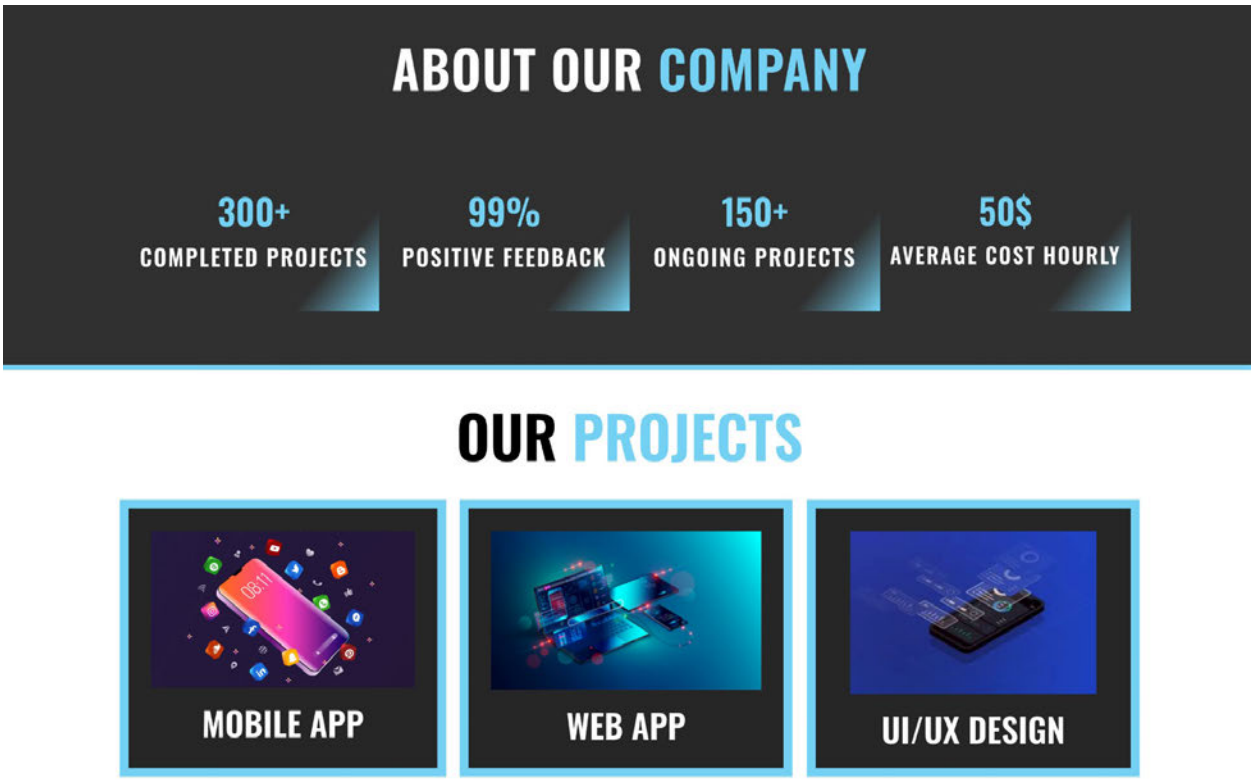
51. Additionally, the website listed the company's address as [redacted]. On January 12, 2024, I conducted open-source research for that address. No business was located at the address.

52. On or about December 20, 2023, I visited the website at the domain **logictech-us.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

logictech-us.com

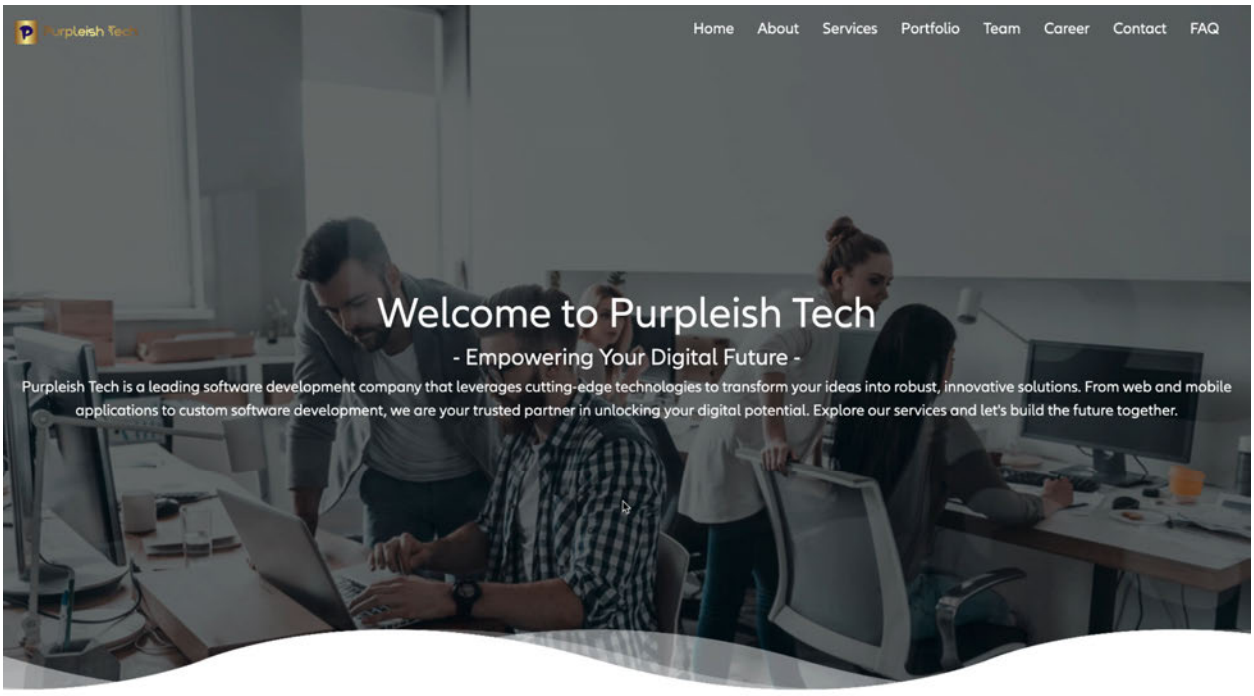

LOGICTECH
Home
Portfolio
Services
About
Contact
GET A QUOTE
Web Development Services | App Development Services
B & MOBILE DEVELOPMENT SERVICE WE
ONE-STOP SOFTWARE DEVELOPMENT COMPANY
Fully agile driven team is ready for your business
GET A QUOTE

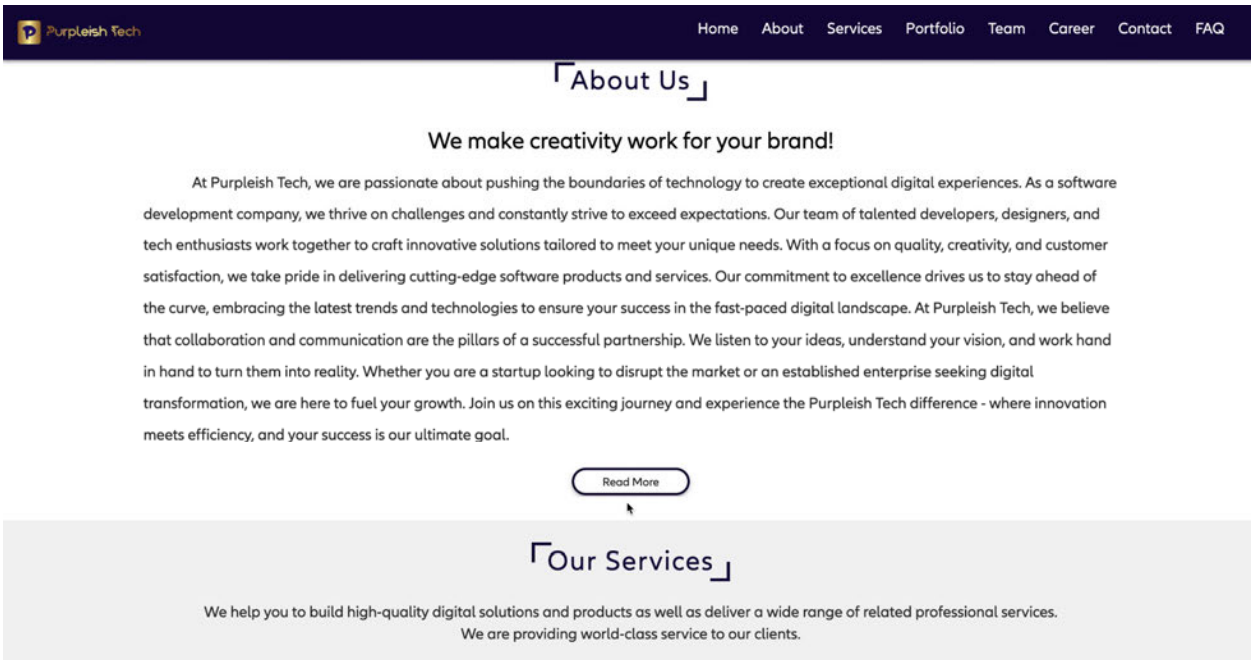

OUR SERVICES
WEB APP DEVELOPMENT
View More
MOBILE APP DEVELOPMENT
View More
UI/UX DESIGN
View More
WEB/MOBILE APP/UI/UX
We have a team of professionals that have great experience in their specific feilds specialy in Web development, Mobile App Development and UI/UX designs.
CONNECT WITH US

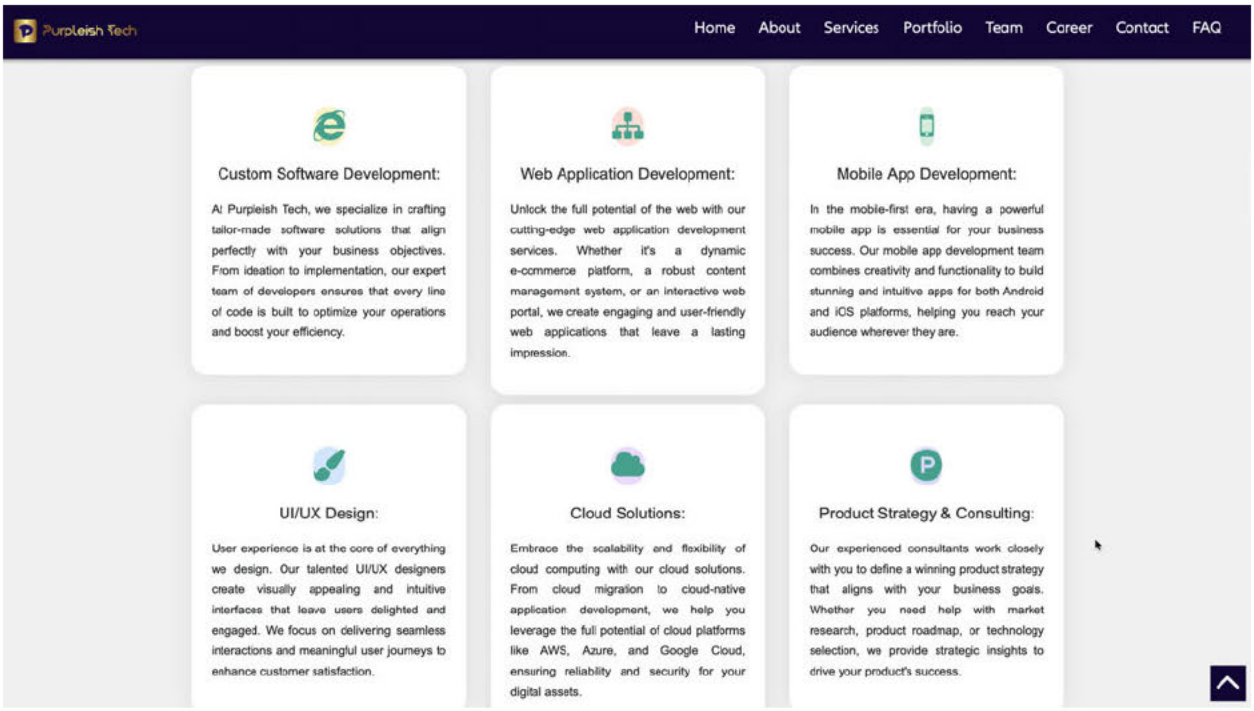


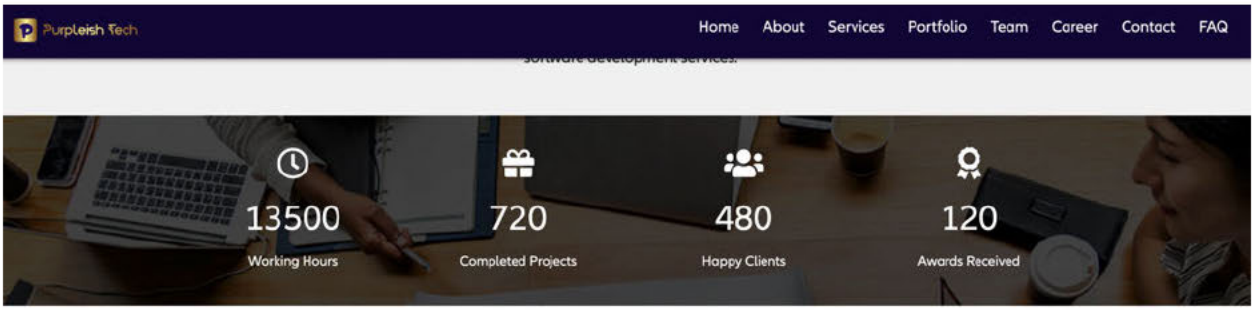
53. On or about February 2, 2024, I visited the website at the domain **purpleishtech.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

purpleishtech.com


Purpleish Tech
Home
About
Services
Portfolio
Team
Career
Contact
FAQ
Welcome to Purpleish Tech
- Empowering Your Digital Future -
Purpleish Tech is a leading software development company that leverages cutting-edge technologies to transform your ideas into robust, innovative solutions. From web and mobile applications to custom software development, we are your trusted partner in unlocking your digital potential. Explore our services and let's build the future together.

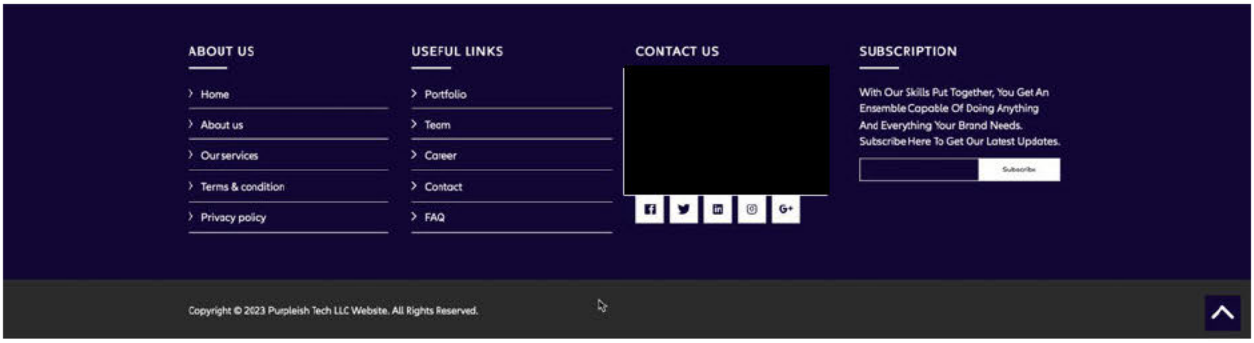

Purpleish Tech
Home
About
Services
Portfolio
Team
Career
Contact
FAQ
About Us
We make creativity work for your brand!
At Purpleish Tech, we are passionate about pushing the boundaries of technology to create exceptional digital experiences. As a software development company, we thrive on challenges and constantly strive to exceed expectations. Our team of talented developers, designers, and tech enthusiasts work together to craft innovative solutions tailored to meet your unique needs. With a focus on quality, creativity, and customer satisfaction, we take pride in delivering cutting-edge software products and services. Our commitment to excellence drives us to stay ahead of the curve, embracing the latest trends and technologies to ensure your success in the fast-paced digital landscape. At Purpleish Tech, we believe that collaboration and communication are the pillars of a successful partnership. We listen to your ideas, understand your vision, and work hand in hand to turn them into reality. Whether you are a startup looking to disrupt the market or an established enterprise seeking digital transformation, we are here to fuel your growth. Join us on this exciting journey and experience the Purpleish Tech difference - where innovation meets efficiency, and your success is our ultimate goal.
Read More
Our Services
We help you to build high-quality digital solutions and products as well as deliver a wide range of related professional services.
We are providing world-class service to our clients.





Our Projects

The objective of Purpleish Tech is to enable a large number of youth to take up industry-relevant skill training that will help them in securing a better livelihood.

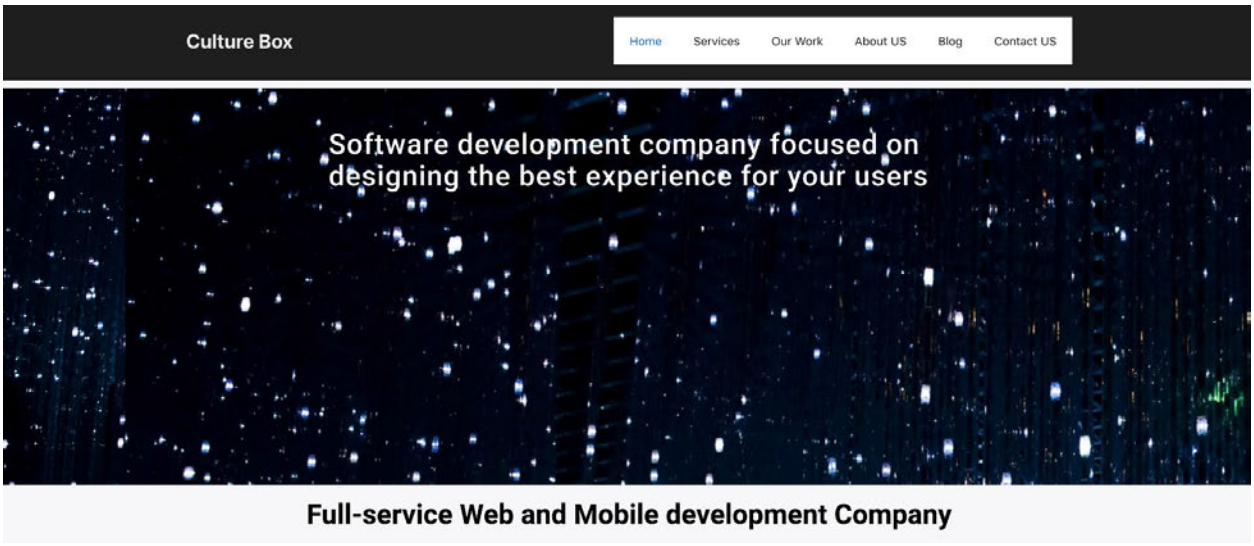


54. The website listed the business's contact address as [redacted], and telephone number as [redacted]. On Google Maps that address appears to be a family home.

55. On or about January 16, 2024, records from Payment Service Provider 1 for "Blackish Tech" and the email [redacted], listed multiple addresses including [redacted], the telephone number [redacted], and the business URL as **www.blackishtech.com**. This is the same location and phone number as Purpleish Tech.

56. On or about February 28, 2024, I visited the website at the domain **culturebx.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

culturebx.com



Product Business Analysis

Our business analysts are experts in translating your business idea into the optimal technical solution. We will work closely with you to learn about your business and understand your users, so that we make sure the app we create is tailored to their needs

QA & TESTING

Studies show that low rankings in the app stores are usually a result of the users' frustration with the bugs. We will keep testing and fixing the app until it becomes state-of-the-art even before launch. Oh, did we mention that we offer one-month free bug fixing after launch? We've got your back!

UI/UX DESIGN

Our business analysts are experts in translating your business idea into the optimal technical solution. We will work closely with you to learn about your business and understand your users, so that we make sure the app we create is tailored to their needs

LAUNCH AND MAINTENANCE

Studies show that low rankings in the app stores are usually a result of the users' frustration with the bugs. We will keep testing and fixing the app until it becomes state-of-the-art even before launch. Oh, did we mention that we offer one-month free bug fixing after launch? We've got your back!

IOS, ANDROID AND BACKEND DEVELOPMENT

We pride ourselves on delivering the utmost quality apps. Apart from a need of a solid architecture, we understand that an app is not only about 'looks' but also about 'feels' so we pay close attention to each transition, animation and loading time

Your business is in good hands

We are a passionate and experienced team with big ambitions

We are a team of professionals based in US and Europe. We've been living and breathing software development since 2010.

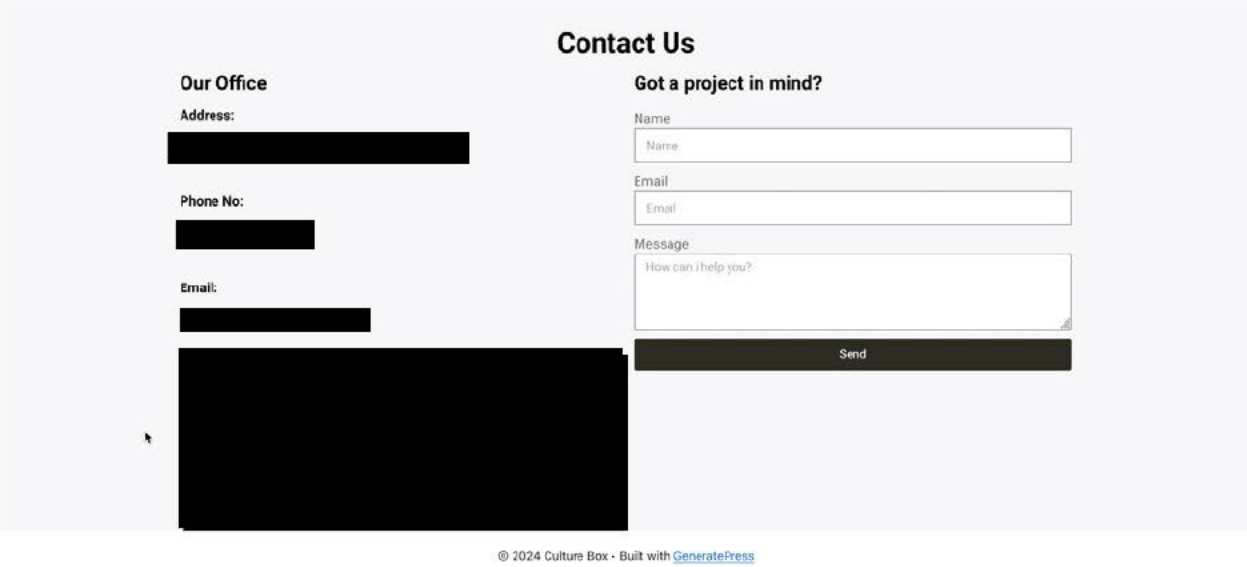
We pride ourselves on our excellent customer service. You will not walk the path to web & mobile success alone. We are here for you, guiding you along the way and offering our vast expertise starting from sketching an idea with pen and paper to implementing the best solution and celebrating success with you.

In short, we are the kind of team who likes to focus on results, such as best user experience, engagement, user satisfaction, retention, and scalability.

350 +
Apps Built

200 +
Happy Clients

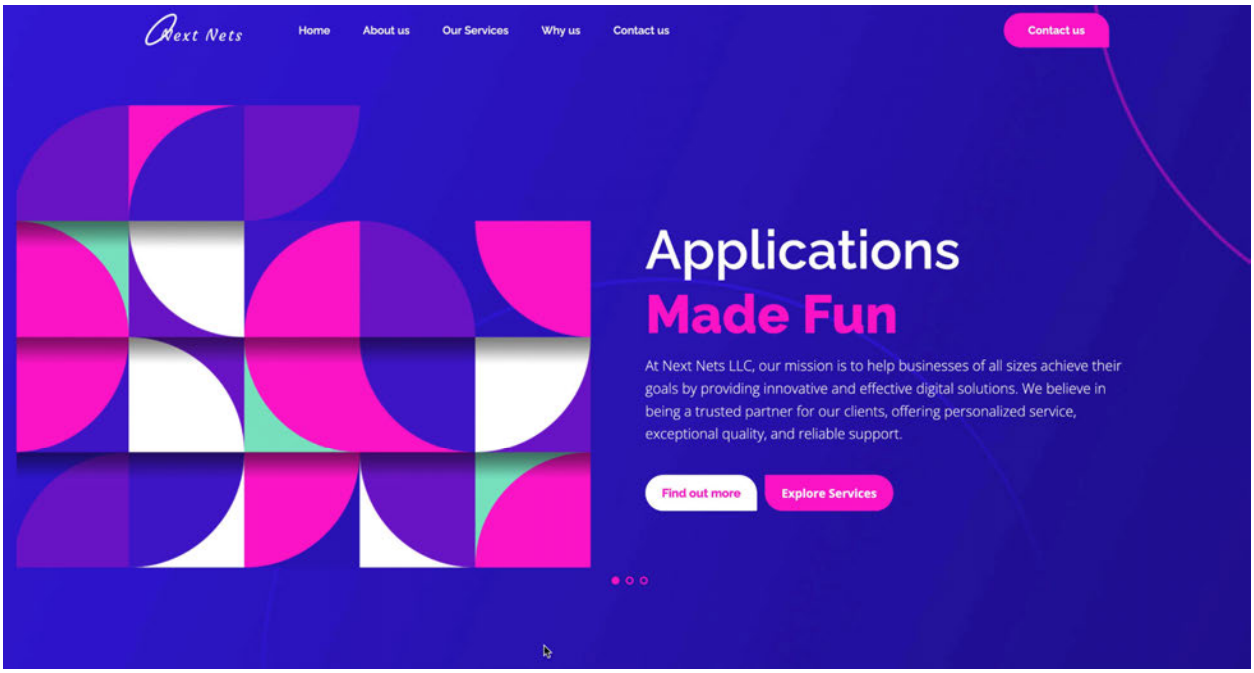
9,000 +
Coffee Cups Drank

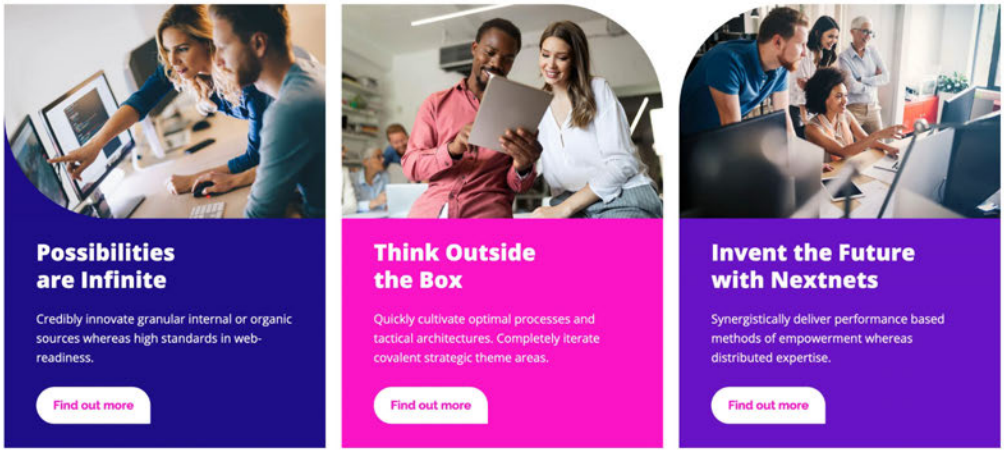


57. The website stated it was part of a company named "Culture Box" with the contact address as [redacted], and telephone number [redacted]. A search for Culture Box identified an LLC registered in Wyoming as "Culture Box LLC" on October 12, 2022, which was "Administratively Dissolved (tax)" on December 9, 2023.

58. On or about February 28, 2024, I visited the website at the domain **nextnets.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

nextnets.com


Next Nets
Home
About us
Our Services
Why us
Contact us
Contact us
Applications
Made Fun
At Next Nets LLC, our mission is to help businesses of all sizes achieve their goals by providing innovative and effective digital solutions. We believe in being a trusted partner for our clients, offering personalized service, exceptional quality, and reliable support.
Find out more
Explore Services


Possibilities are Infinite
Credibly innovate granular internal or organic sources whereas high standards in web-readiness.
Find out more
Think Outside the Box
Quickly cultivate optimal processes and tactical architectures. Completely iterate covalent strategic theme areas.
Find out more
Invent the Future with Nextnets
Synergistically deliver performance based methods of empowerment whereas distributed expertise.
Find out more

Technology for Investors

At Next Nets LLC, we understand the importance of staying ahead of the curve in the fast-paced world of technology. That's why we invest heavily in research and development, constantly exploring new technologies and solutions that can help our clients achieve their goals.

Our team of experts includes skilled developers, designers, and digital marketers who have a passion for leveraging the latest technologies to deliver innovative and effective solutions. We specialize in a wide range of technologies, including:

Find out more

Simple Solutions for Complex Challenges

React Native

We are experts in building cross-platform mobile applications using React Native, a popular framework for developing mobile apps that work seamlessly on both iOS and Android platforms.

Cloud Computing

We offer cloud-based solutions that enable our clients to store, manage, and access their data securely and efficiently, using platforms such as Amazon Web Services (AWS) and Microsoft Azure.

Artificial Intelligence (AI)

We leverage the power of AI and ML to help our clients gain insights from their data and automate routine tasks, using frameworks such as TensorFlow and PyTorch.

Internet of Things (IoT)

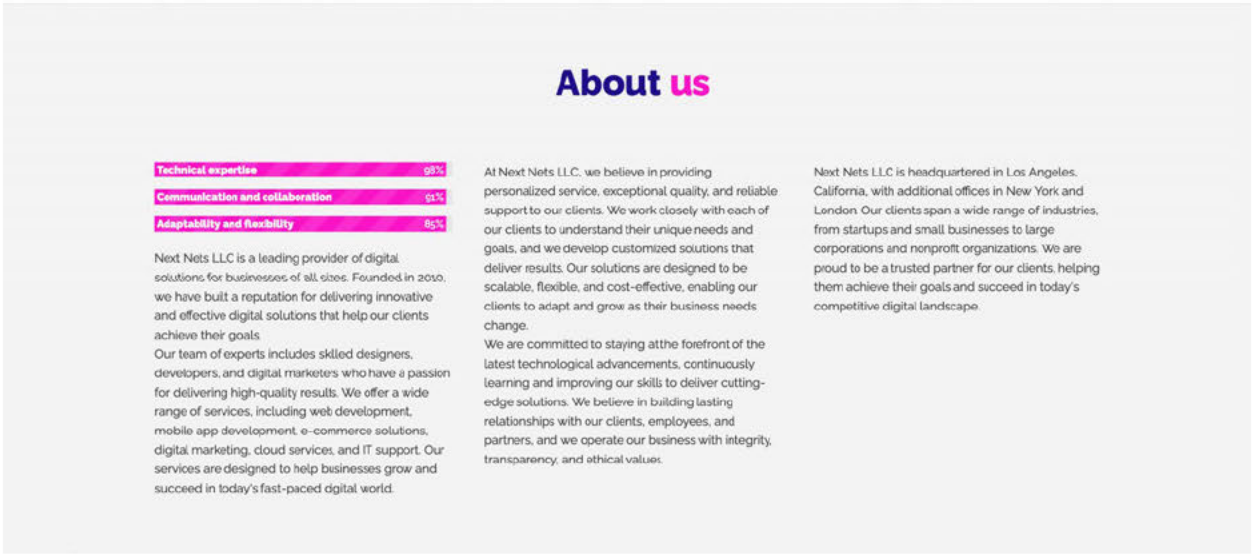
We develop IoT solutions that enable our clients to connect and automate their devices, using platforms such as AWS IoT and Google Cloud IoT.

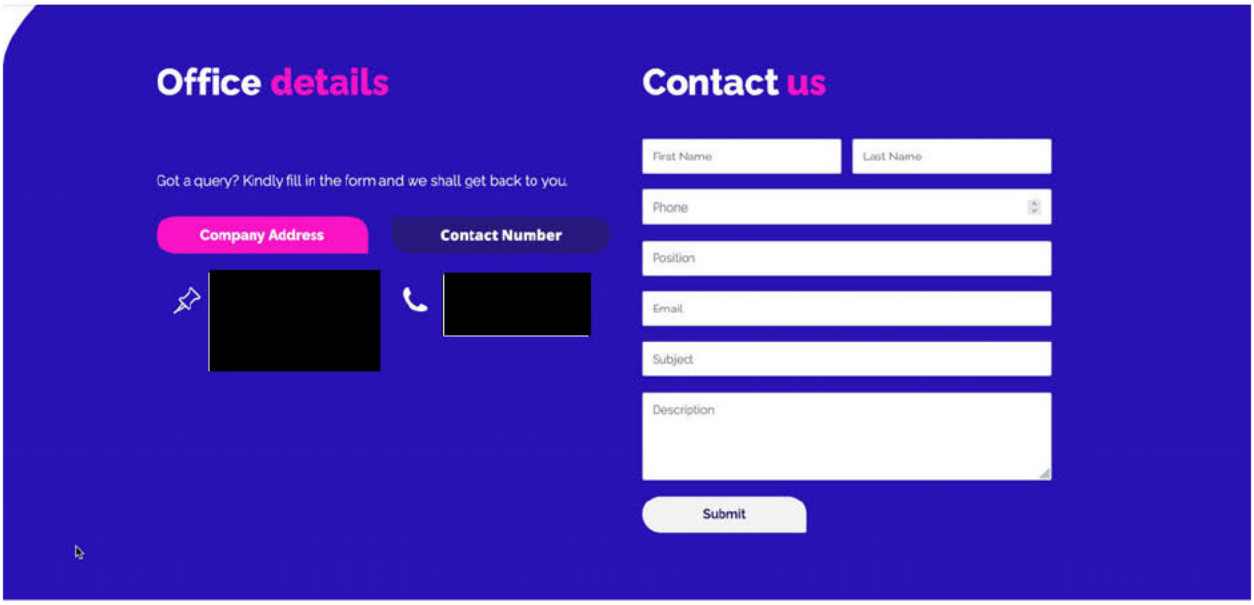
Blockchain

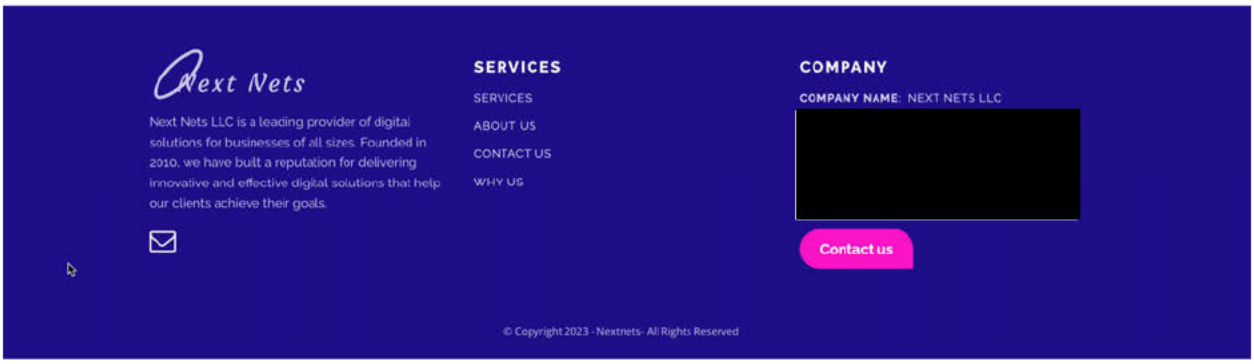
We offer blockchain solutions that enable secure and transparent transactions and data sharing, using platforms such as Ethereum and Hyperledger Fabric.

Machine Learning (ML)

We integrate Machine Learning in our service, which helps to unlock the full potential of your data, whether it's in the form of images, text, or numerical values.


About us
Technical expertise 98%
Communication and collaboration 91%
Adaptability and flexibility 85%
Next Nets LLC is a leading provider of digital solutions for businesses of all sizes. Founded in 2010, we have built a reputation for delivering innovative and effective digital solutions that help our clients achieve their goals.
Our team of experts includes skilled designers, developers, and digital marketers who have a passion for delivering high-quality results. We offer a wide range of services, including web development, mobile app development, e-commerce solutions, digital marketing, cloud services, and IT support. Our services are designed to help businesses grow and succeed in today's fast-paced digital world.
At Next Nets LLC, we believe in providing personalized service, exceptional quality, and reliable support to our clients. We work closely with each of our clients to understand their unique needs and goals, and we develop customized solutions that deliver results. Our solutions are designed to be scalable, flexible, and cost-effective, enabling our clients to adapt and grow as their business needs change.
We are committed to staying atthe forefront of the latest technological advancements, continuously learning and improving our skills to deliver cutting-edge solutions. We believe in building lasting relationships with our clients, employees, and partners, and we operate our business with integrity, transparency, and ethical values.
Next Nets LLC is headquartered in Los Angeles, California, with additional offices in New York and London. Our clients span a wide range of industries, from startups and small businesses to large corporations and nonprofit organizations. We are proud to be a trusted partner for our clients, helping them achieve their goals and succeed in today's competitive digital landscape.

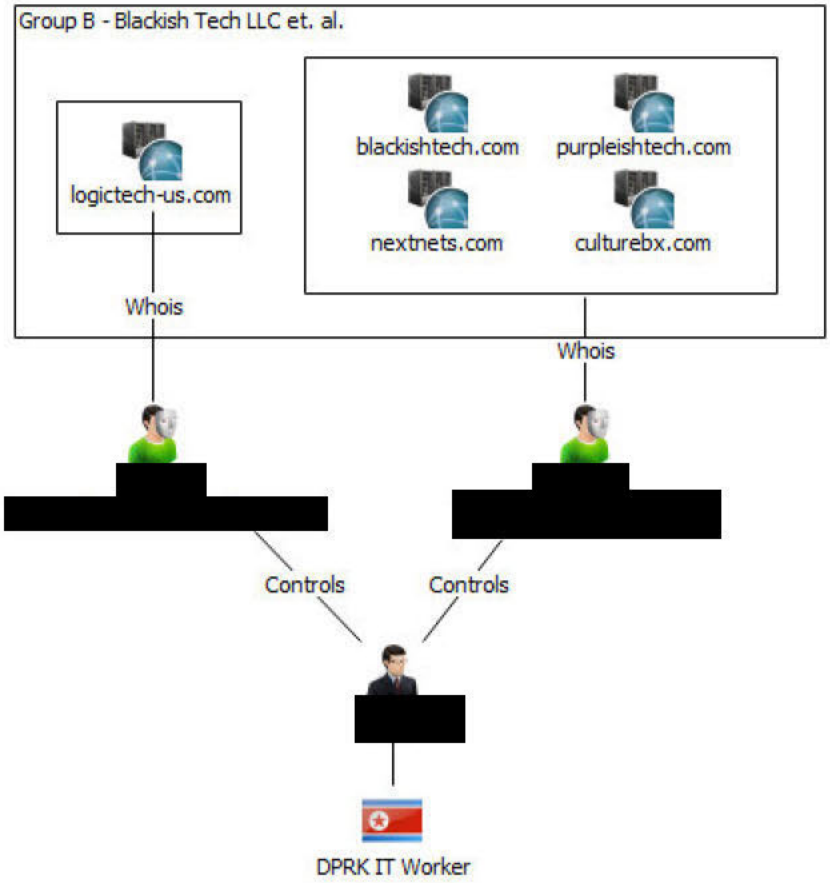

Office details
Got a query? Kindly fill in the form and we shall get back to you.
Company Address
Contact Number
[redacted]
[redacted]
Contact us
First Name
Last Name
Phone
Position
Email
Subject
Description
Submit


Next Nets
Next Nets LLC is a leading provider of digital solutions for businesses of all sizes. Founded in 2010, we have built a reputation for delivering innovative and effective digital solutions that help our clients achieve their goals.
SERVICES
SERVICES
ABOUT US
CONTACT US
WHY US
COMPANY
COMPANY NAME: NEXT NETS LLC
[redacted]
Contact us
© Copyright 2023 - Nextnets- All Rights Reserved

59. The website listed the company name as "Next Nets LLC" with the contact address as [redacted], and telephone number [redacted]. However, their website identified they were headquartered in Los Angeles, California with offices in New York and London. The area code 323 is for the Los Angeles area. A search for Next Nets LLC identified an LLC registered in Wyoming on March 16, 2023.

60. Below is a chart that summarizes the connections between the domains and the North Korean IT worker responsible for them:

Chart for Group B – Blackish Tech LLC, et al.



61. Based on the above, there is probable cause to believe that funds originating from a DPRK IT worker based outside the United States were sent into the United States in order to purchase **blackishtech.com**, **logictech-us.com**, **purpleishtech.com**, **culturebx.com**, and **nextnets.com** and that these domains were used with the intent of promoting a conspiracy to violate IEEPA. **Blackishtech.com**, **logictech-us.com**, **purpleishtech.com**, **culturebx.com**, and **nextnets.com** are therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

C. Group C – M Solution LLC

Domains: babyboxinfo.com; helix-us.com; cubixtechus.com

62. A seizure warrant for *babyboxtech.com*, 4:23-MJ-9240-RHH, was signed by Magistrate Judge Rodney H. Holmes in the Eastern District of Missouri on October 5, 2023, and its facts are incorporated into this affidavit by reference. On or about January 12, 2024, I conducted open source research for Baby Box and identified a domain, **babyboxinfo.com**, which is similar in name to *babyboxtech.com*. A review of WHOIS information for **babyboxinfo.com** identified that the domain was created on February 3, 2022, expires on February 3, 2025, and had the following registrant information:

Name: [redacted] (same alias discussed above)
Street: [redacted]
City: New York
State: NY
Zip: 10128
Email: [redacted]
Telephone: [redacted]

63. A review of DomainTools identified two additional domains registered using the same information (name, address, email and telephone): **cubixtechus.com** and **helix-us.com**.

The domain **cubixtechus.com** was created on January 22, 2022, and expires on January 22, 2025. The domain **helix-us.com** was created on January 27, 2022, and expires on January 27, 2025.

64. The domains **babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com** were registered at NameCheap, Inc. ("NameCheap"), located in Pheonix Arizona, and, on or about November 20, 2023, NameCheap provided records which identified they were registered by the reseller Ahead Host.

65. On or about December 2, 2023, Ahead Host provided the subscriber information for the account associated with the email address [redacted] that registered **babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com**. The account was registered using the name [redacted] (anonymized real name) the address [redacted], the telephone number [redacted], and purchased these three domains using the Payment Service Provider 1 account [redacted].

66. On or about January 24, 2024, records from Payment Service Provider 1 for [redacted] identified the account was in the name of [redacted]. (the same name that registered **babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com**) and had multiple email addresses using the name [redacted]. I know from my training and experience the use of multiple email accounts on a payment account is a technique used by North Korean IT workers to send/receive money and mask their true identity. A review of the account's transactions identified the following payments to Ahead Host for $13.00 each. These records correspond to payment records also obtained from Ahead Host:

Date	Subject
March 12, 2021	Ahead Host LLC – Invoice #17657
January 17, 2022	Ahead Host LLC – Invoice #20764
February 10, 2022	Ahead Host LLC – Invoice #21003
March 20, 2022	Ahead Host LLC – Invoice #21312
March 20, 2022	Ahead Host LLC – Invoice #21428

67. On or about December 13, 2023, Microsoft provided records for any accounts associated with telephone number [redacted] (the number that registered **babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com**). According to the Microsoft records, this account was subscribed to by "[redacted]", using the email address [redacted], and purchased services using a Payment Service Provider 1 account registered with the email address [redacted] and the name "[redacted]." The Microsoft account had the associated [redacted] username [redacted]".

68. Microsoft search returns for an account used by North Korean IT worker [redacted] (described above) in response to the 4:22-MJ-7028-SPM search warrant revealed a communication, on or about November 9, 2020, in which "[redacted]" shared with [redacted]. the password associated with email address [redacted] (the email that registered **babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com**) and email address [redacted] (the email account for the Payment Service Provider 1 account that purchased **babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com**). Based on these

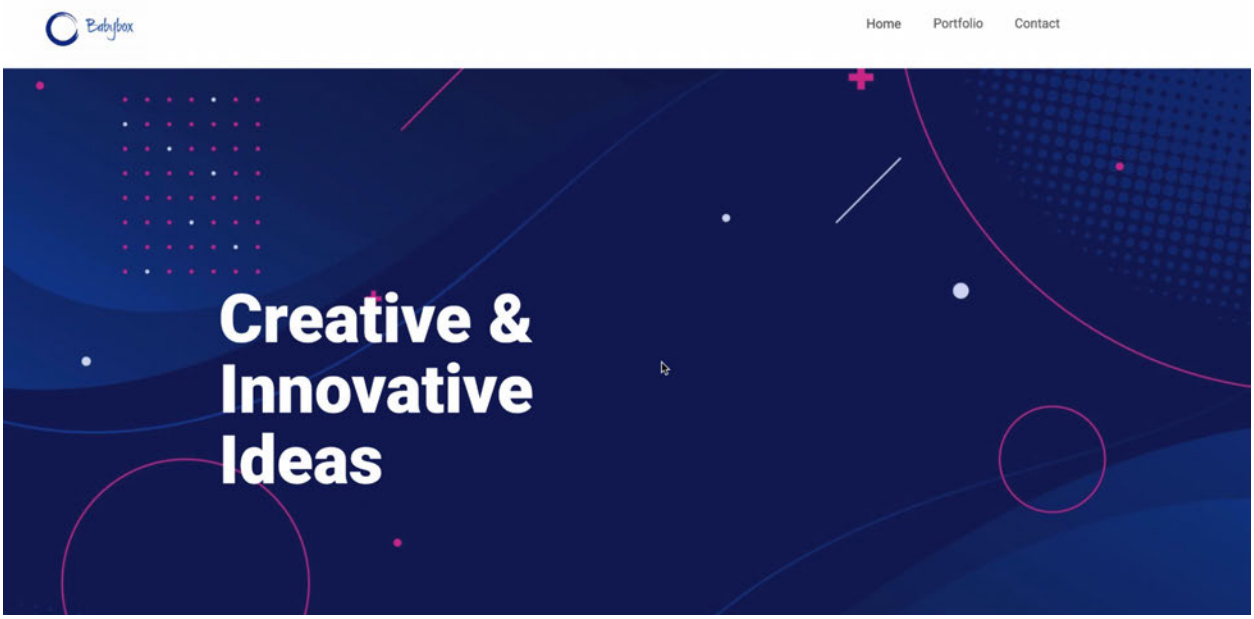
communications, I have probable cause to believe the alias "[redacted]," is an unidentified North Korean IT worker who works with [redacted].

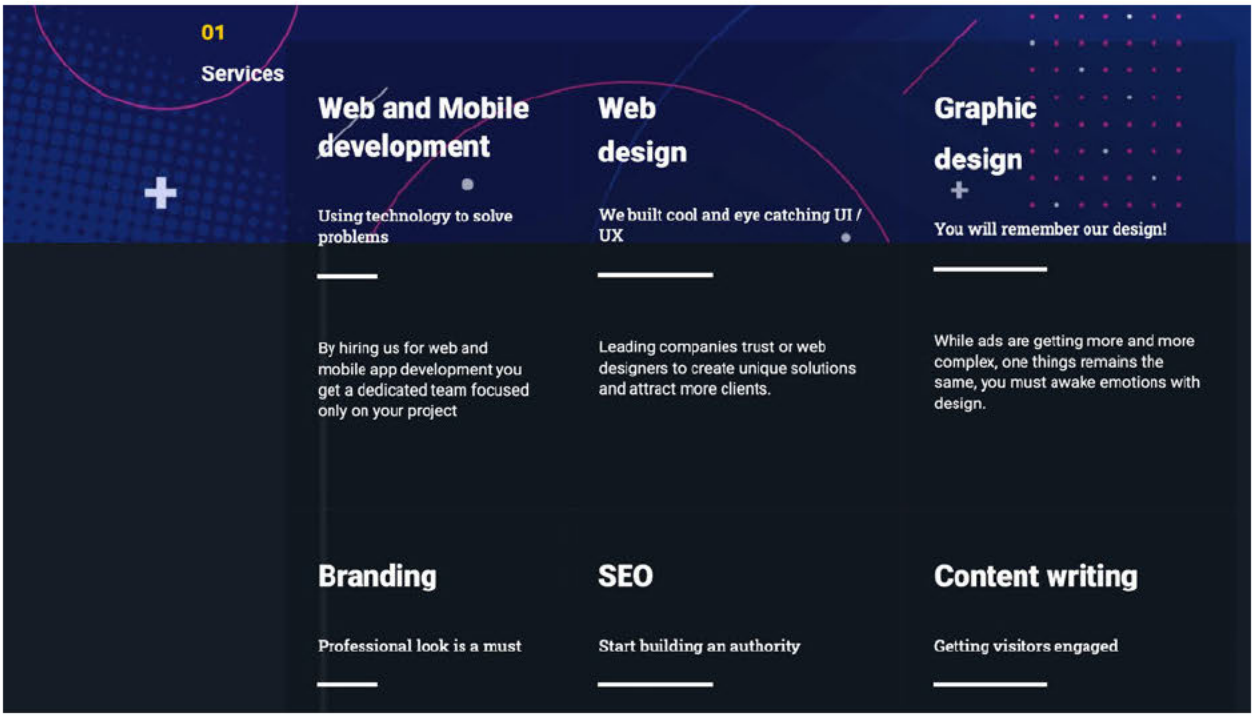
69. On or about December 7, 2023, Google provided the subscriber information for the email address [redacted] which had the recovery email of [redacted].

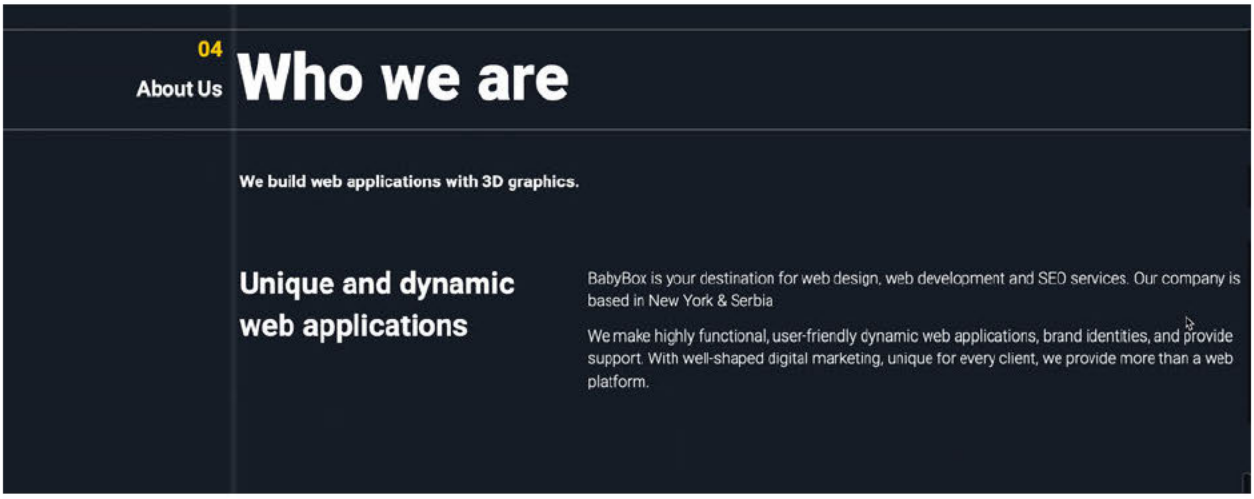
70. As described above, as early as 2021, the name [redacted]. was previously observed being used by North Korean IT workers who, based on the search warrant returns discussed above, I have probable cause to believe worked with [redacted].

71. On or about November 17, 2023, I visited the website at the domain **babyboxinfo.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

babyboxinfo.com



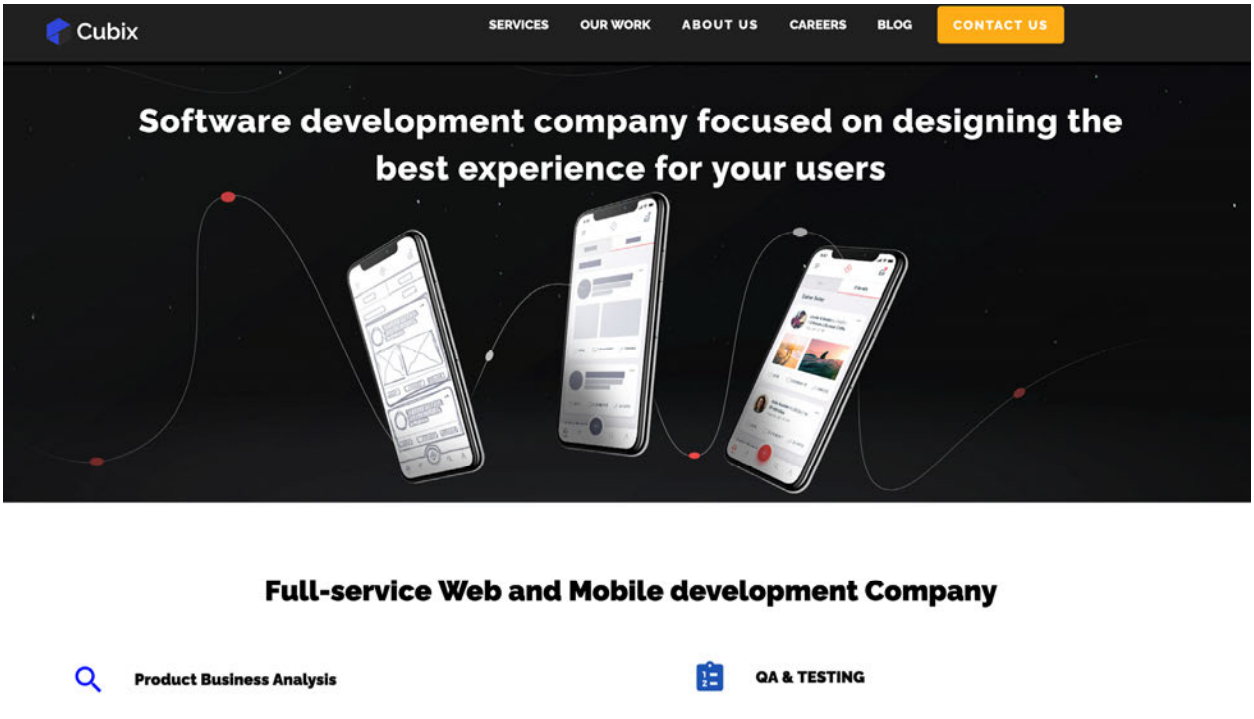

01
Services
Web and Mobile development
Using technology to solve problems
By hiring us for web and mobile app development you get a dedicated team focused only on your project
Web design
We built cool and eye catching UI / UX
Leading companies trust or web designers to create unique solutions and attract more clients.
Graphic design
You will remember our design!
While ads are getting more and more complex, one things remains the same, you must awake emotions with design.
Branding
Professional look is a must
SEO
Start building an authority
Content writing
Getting visitors engaged

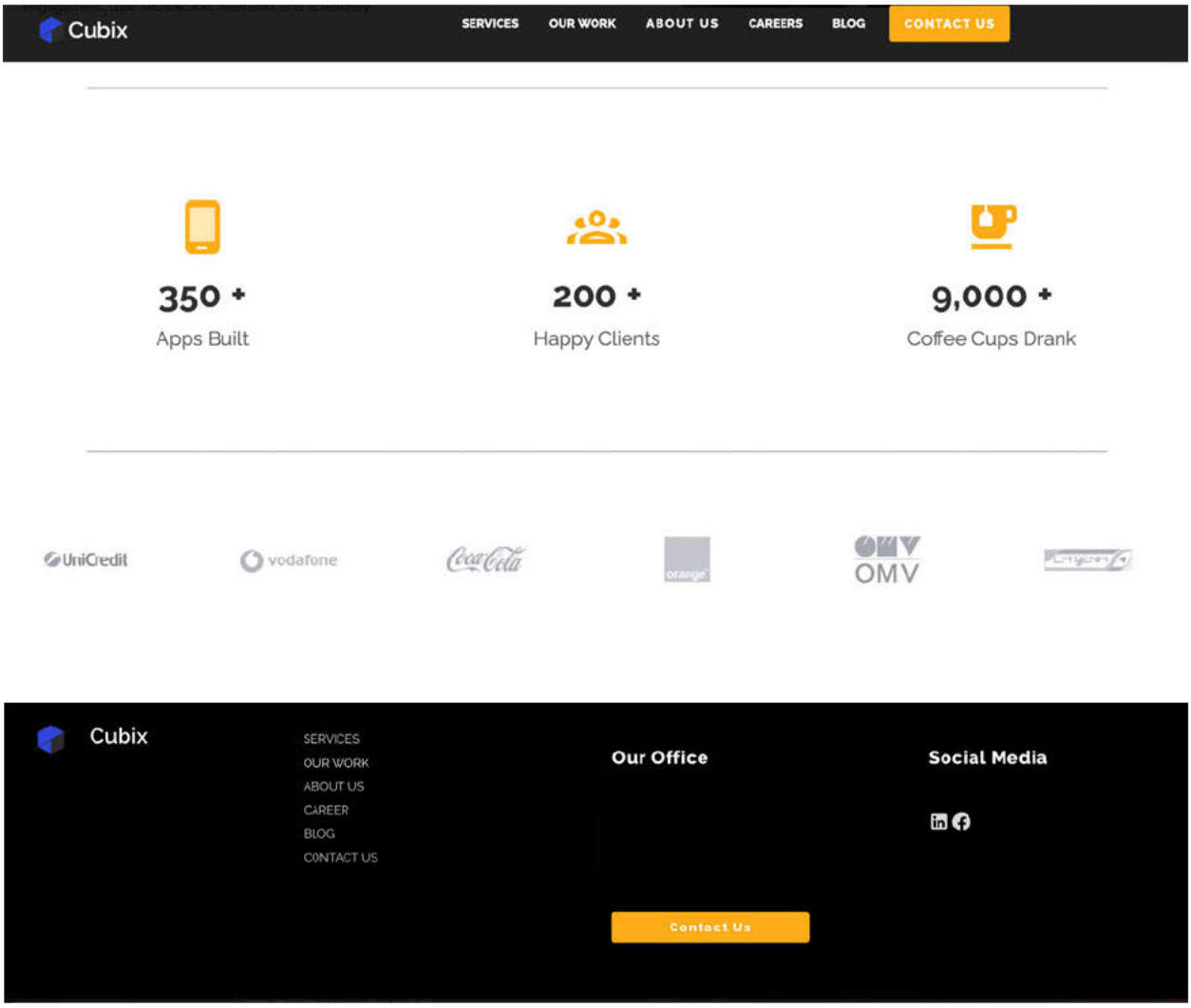

04
About Us
Who we are
We build web applications with 3D graphics.
Unique and dynamic web applications
BabyBox is your destination for web design, web development and SEO services. Our company is based in New York & Serbia
We make highly functional, user-friendly dynamic web applications, brand identities, and provide support. With well-shaped digital marketing, unique for every client, we provide more than a web platform.


Contact Us
Let's Talk
BabyBox

72. On or about November 17, 2023, I visited the website at the domain **cubixtechus.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

cubixtechus.com

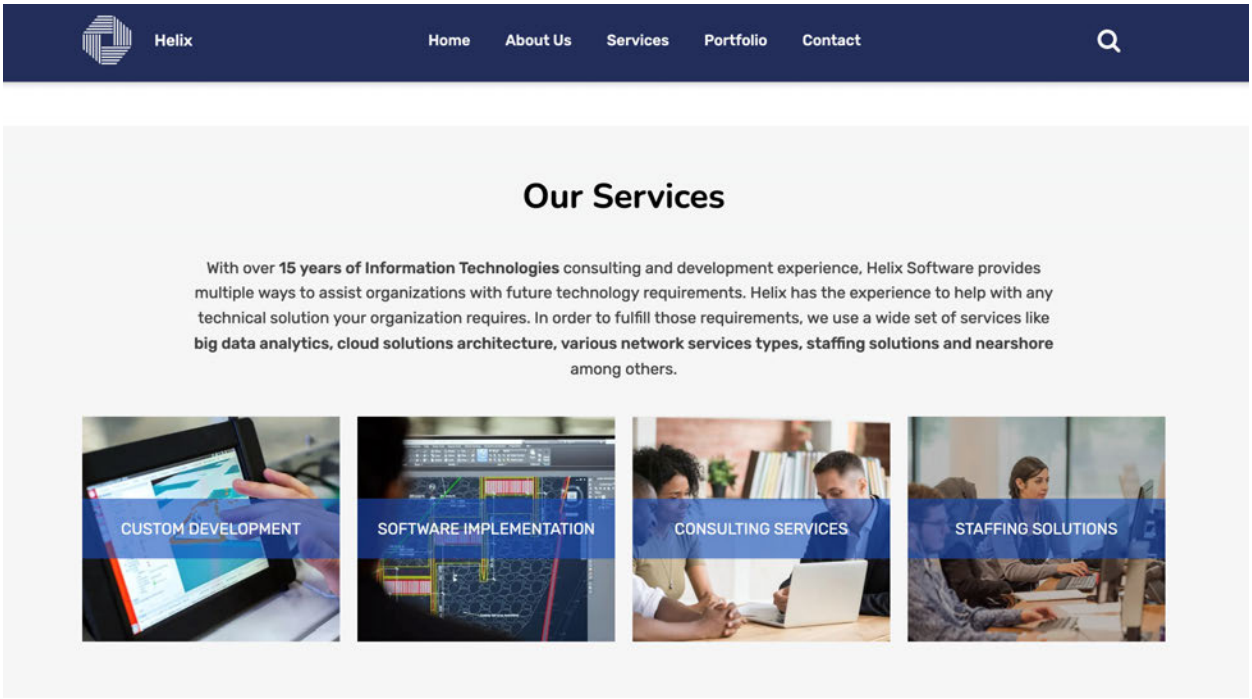


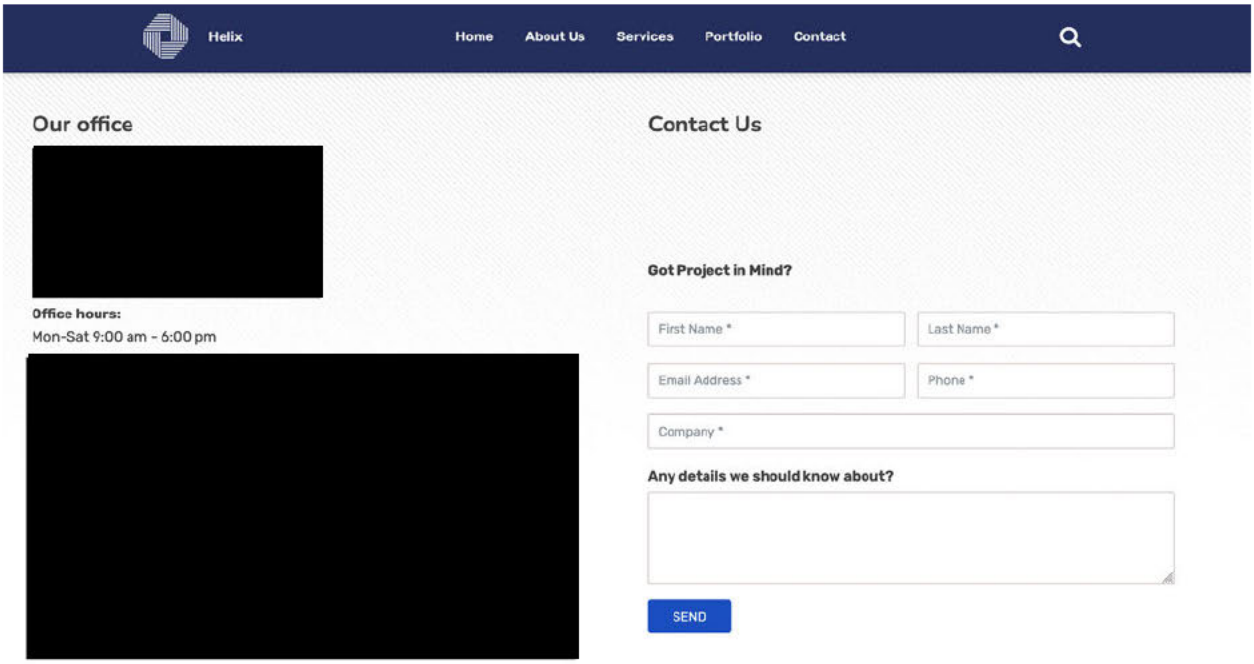


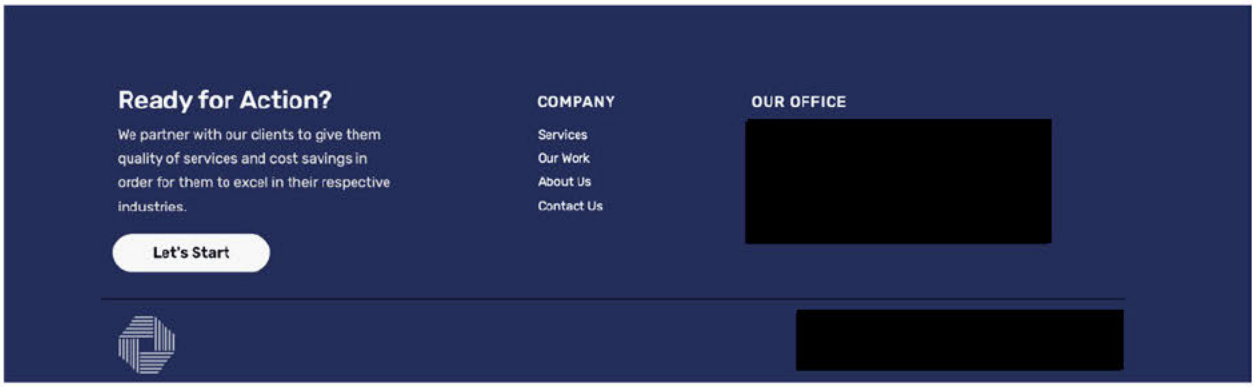
73. On or about November 17, 2023, I visited the website at the domain **helix-us.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

helix-us.com


Helix
Home
About Us
Services
Portfolio
Contact
SUCCESS YOUR BUSINESS
We Provide Best
Service for your Business

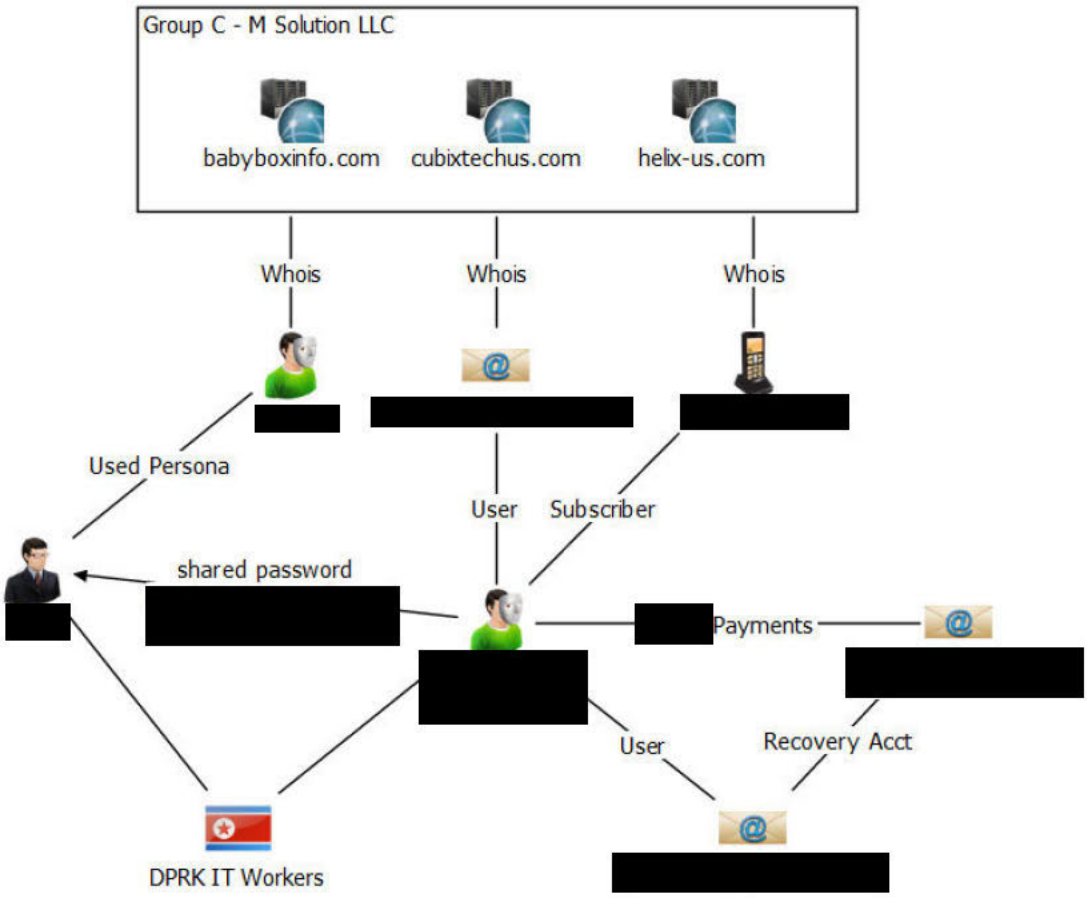

Helix
Home
About Us
Services
Portfolio
Contact
Our Services
With over 15 years of Information Technologies consulting and development experience, Helix Software provides multiple ways to assist organizations with future technology requirements. Helix has the experience to help with any technical solution your organization requires. In order to fulfill those requirements, we use a wide set of services like big data analytics, cloud solutions architecture, various network services types, staffing solutions and nearshore among others.
CUSTOM DEVELOPMENT
SOFTWARE IMPLEMENTATION
CONSULTING SERVICES
STAFFING SOLUTIONS





74. Below is a chart that summarizes the connections between the domains and the North Korean IT workers:

Chart for Group C – M Solution LLC



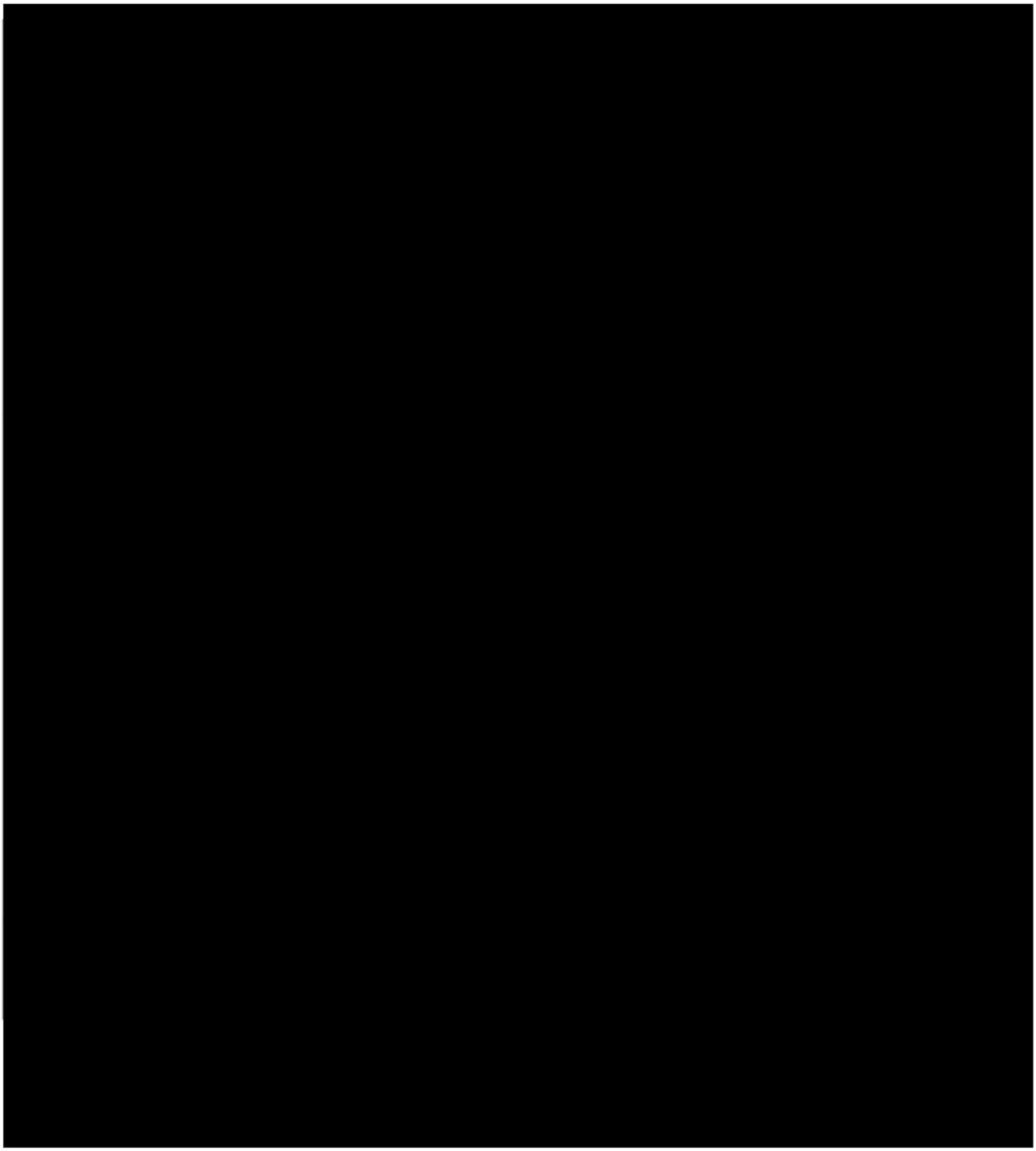
75. Based on the above, there is probable cause to believe that funds originating from a DPRK IT worker based outside the United States were sent into the United States in order to purchase **babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com** and that these domains were used with the intent of promoting a conspiracy to violate IEEPA. **Babyboxinfo.com**, **cubixtechus.com**, and **helix-us.com** are therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

D. Group D – Bynolt

Domain: bynolt.com

76. On or about November 17, 2023, I conducted open source research for information related to "Baby Box Tech" which was the named company associated with *babyboxtech.com*, one of the domains seized in October 2023 pursuant to the seizure warrant 4:23-MJ-9240-RHH. A [redacted] using the name "babyboxtech", which is the same name as the company "Baby Box Tech" and the domain, *babyboxtech.com*, was identified. Prior to the seizure of the domain babyboxtech.com, the group had the [redacted] "babybox." I observed that the "babyboxtech" [redacted] had changed its name to "BYNOLT," San Diego, CA, and advertised the domain **bynolt.com** and purported to be a software development company. According to the Bynolt [redacted], the HR Director for Bynolt was [redacted]. (name anonymized), who lived in Lahore, Punjab, Pakistan. [redacted]. was previously listed on the *babyboxtech.com* website as the HR Manager for "Baby Box Tech." Additionally, San Diego, CA, was the purported location for Baby Box Tech.

[redacted] – babyboxtech / Bynolt



77. On or about December 8, 2023, GoDaddy LLC ("GoDaddy"), the registrar for the domain **bynolt.com**, provided the WHOIS information for the domain as [redacted]. (the same [redacted]. as above), [redacted], with the email address

[redacted], and telephone number [redacted]. The domain was created on September 19, 2022, and expires on September 19, 2025. According to records from GoDaddy, payments were made using a credit card in the name of [redacted] (name anonymized) in the Pakistan Rupee (PKR) currency using the email address [redacted]. The credit card was issued by United Bank, LTD, Pakistan.

78. A review of open source information led me to conclude that the owner of the Miami, FL address is [redacted] (true name anonymized). A review of records from a Payment Service Provider 1 account associated with the email [redacted] owned by [redacted]., an identifier used by a North Korean IT worker known as [redacted]., showed that the [redacted] account made multiple payments to [redacted] between December 2021 and September 2022. Additionally, a Payment Service Provider 1 account owned by [redacted]. and associated with the email [redacted] (a North Korean IT worker email account used by [redacted]") showed the [redacted] account made multiple payments to [redacted]. between June 2022 and August 2022. I know from my training and experience that North Korean IT workers frequently use the identities of individuals who they have worked with previously, often times without their knowledge or permission. The use of a Pakistani credit card in the name of [redacted]., who resides in Miami, FL, supports this belief.

79. On or about December 8, 2023, I conducted open source research for [redacted] and identified a [redacted] from "HR Services" which listed a job for a "Lead Android Developers (remote)" at BABYBOXTECH. The contact information included the email address [redacted] and the website *babyboxtech.com*.

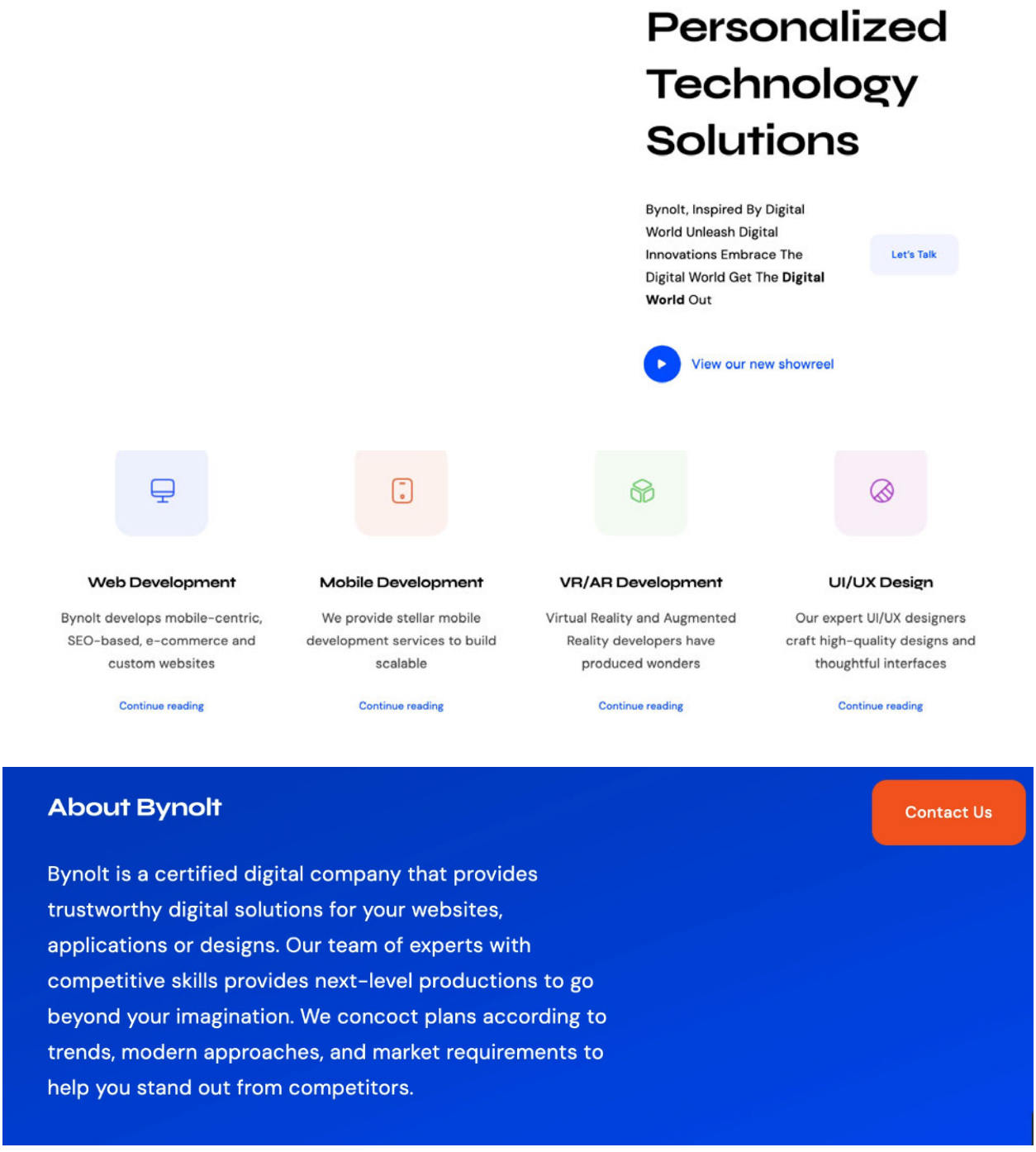
80. Further research on [redacted] identified additional employees at Bynolt, one of whom was located in Tennessee and purported to be a "Shipping and Receiving Specialist" for BABYBOXTECH (now Bynolt). The individual stated they were a "Remote Support Professional."

81. I know from my training and experience that North Korean IT workers recruit individuals to help them access the devices necessary to conduct their remote IT jobs. Those individuals will receive devices that they will then reship to another set of individuals. That second group will connect the devices to their home network and install remote desktop software. The remote software allows the North Korean IT workers to connect to the company's network and do their assigned IT work.

82. The FBI believes once the domain *babyboxtech.com* was seized, the North Korean IT worker changed the [redacted] to say "Bynolt". This was done to establish another front company and avoid references to "Baby Box Tech". Additionally, North Korean IT workers frequently recruit individuals in Pakistan and other countries to be the "face" of the company, while maintaining control of the finances and payments associated to their and others' development work.

83. On or about December 8, 2023, I visited the website at the domain **bynolt.com**. The following screen captures were obtained which indicated the domain was used to advertise IT work:

bynolt.com

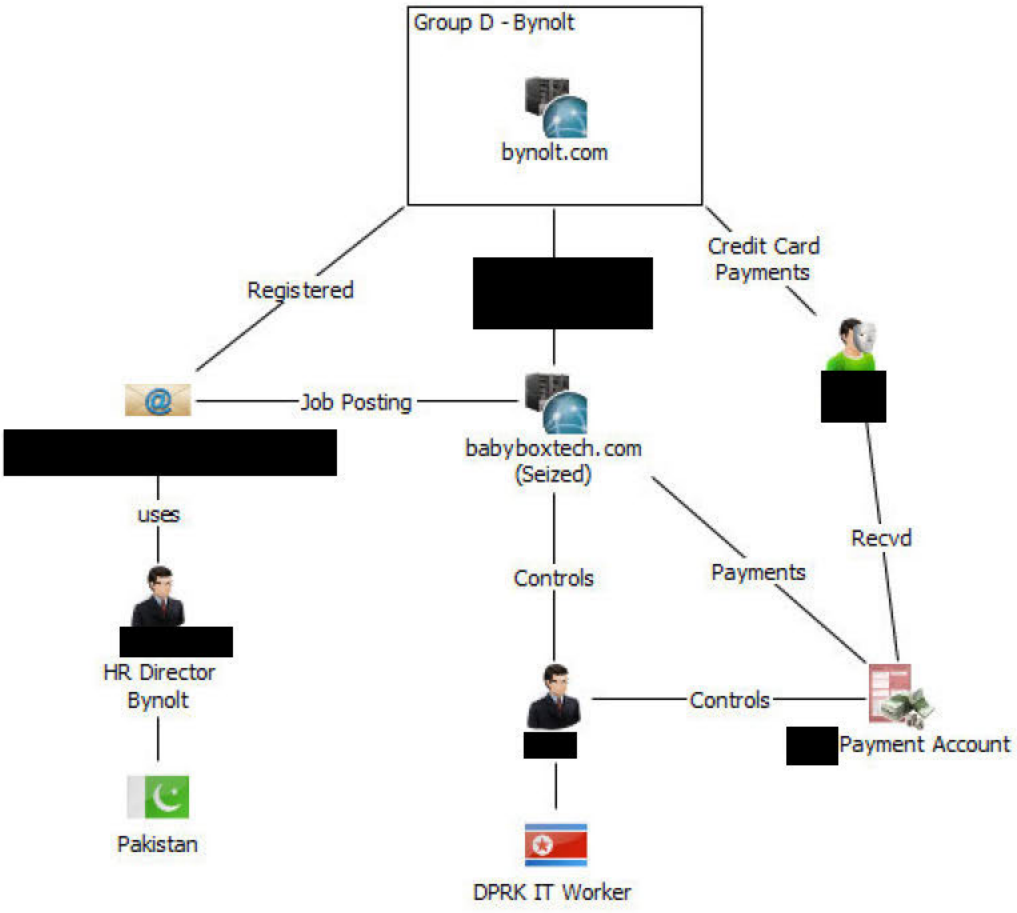


84. The website does not indicate the company is headquartered in San Diego, CA, which was listed on their [redacted], nor does it suggest that the company is associated with

developers in Pakistan. Additionally, the address in Miami, FL, which was used to register the domain by [redacted] is a condo and not associated to [redacted] or [redacted] North Korean IT workers frequently use multiple addresses and locations to further mask the company's association to North Korea.

85. Below is a chart that summarizes the connections between the domain and North Korean IT workers:

Chart for Group D - Bynolt



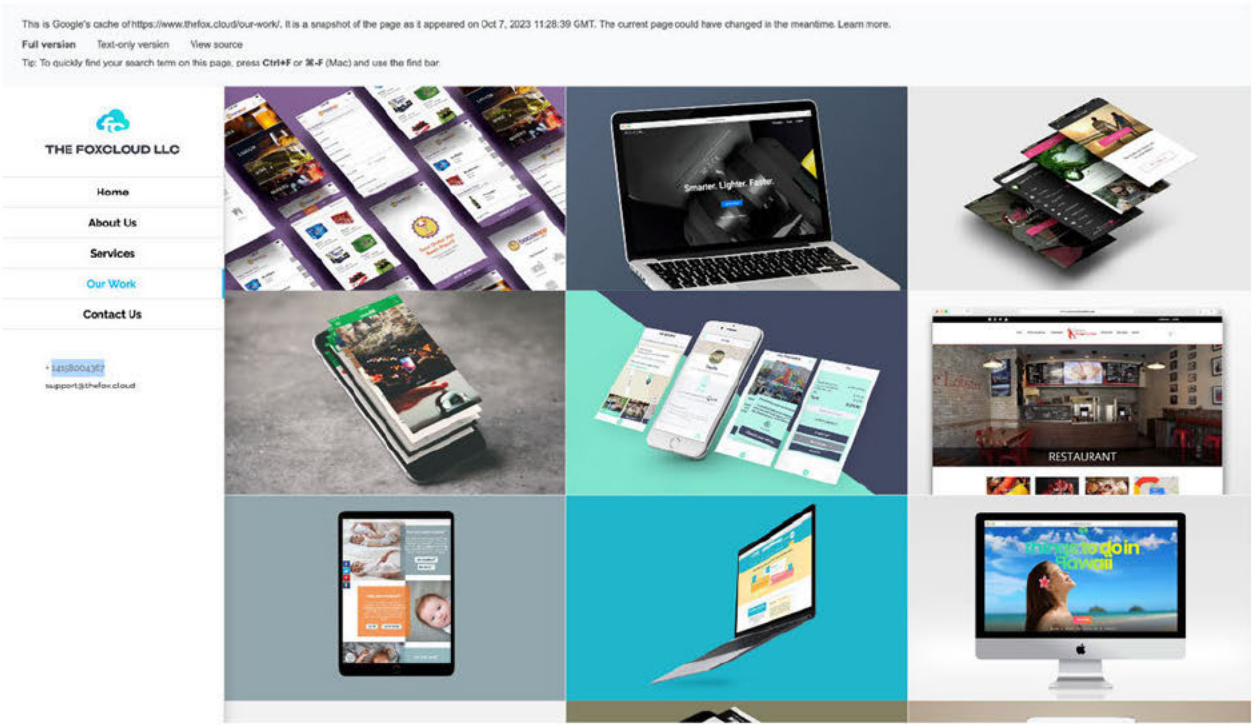
86. Based on the above, there is probable cause to believe that funds originating from a DPRK IT worker based outside the United States were sent into the United States in order to purchase **bynolt.com** and that this domain was used with the intent of promoting a conspiracy to violate IEEPA. **Bynolt.com** is therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

E. Group E – The FoxCloud, LLC

Domain: thefox.cloud

87. On or about November 1, 2023, I conducted open source research for telephone number [redacted], which was listed on a webpage as associated with the domains *foxysun.com* and *foxysunstudios.com*. Both of these domains were seized by the FBI on October 16, 2023 pursuant to seizure warrant 4:23-MJ-09240-RHH. A Google search result identified a cached page from October 7, 2023 for the domain **thefox.cloud** for the company "The FoxCloud LLC." The webpage was similar in appearance to *foxysun.com* and *foxysunstudios.com* used by Foxy Sun Studios and can be seen below:

Google Cache – thefox.cloud/our-work/



88. A WHOIS search for the domain **thefox.cloud** identified the first domain registrar as Google Domains, a company located in Mountain View California, and the present one as Squarespace, located in New York, New York. The domain was created on or about January 26, 2022, and expires on January 26, 2025.

89. On or about November 21, 2023, Google, the initial domain registrar for the domain **thefox.cloud**, provided the WHOIS information for the domain as [redacted], Fox Cloud LLC, [redacted], email address [redacted], telephone number [redacted]. The account settings identified an additional email address of [redacted] and email addresses [redacted] and [redacted].

90. On or about November 27, 2023, Squarespace provided the same WHOIS information for the domain **thefox.cloud** as [redacted], with the email address [redacted] and telephone number [redacted].

91. The email address [redacted] was previously used to register 12 domains, including those used by "Foxy Sun Studios LLC." All these domains are North Korean IT worker domains and were seized by the FBI on October 16, 2023, pursuant to 4:23-MJ-09240-RHH. Those domains, the email address [redacted], and telephone number [redacted], were controlled by an individual who used the name "[redacted]." The FBI believes this is an alias used by an unidentified North Korean IT worker.

92. On or about December 5, 2023, the FBI interviewed [redacted] who confirmed s/he did not control the email address [redacted] and had dissolved Foxy Sun Studios LLC in the United States. As noted above, North Korean IT workers frequently use the identities of individuals who they have worked with previously, often times without their knowledge or permission. Because the individual using the [redacted]" alias controlled the previously seized domains and information used to register **thefox.cloud**, I submit that I have probable cause to believe [redacted]'s identity was stolen by DPRK IT workers and the DPRK IT worker controlling the alias "[redacted]" actually registered and controls the domain **thefox.cloud**.

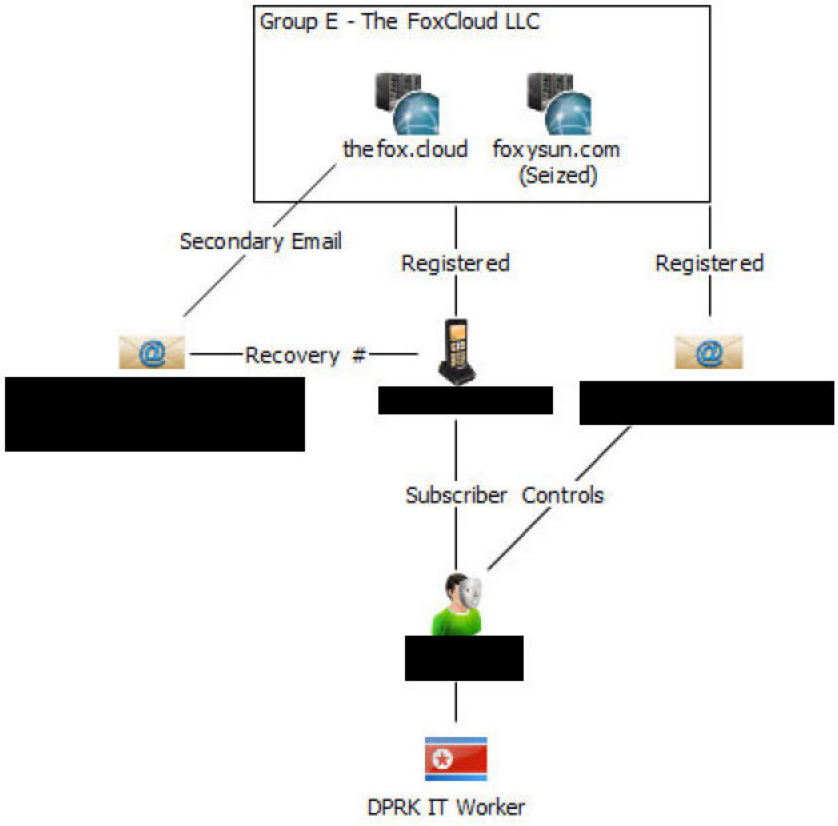
93. On or about November 30, 2023, Payment Service Provider 1 provided records for two accounts. The first was opened on September 4, 2023, and used the email [redacted] and the name "[redacted]." The second was opened on August 18, 2023, and used the email [redacted] and the name "[redacted]". According to Payment Service Provider 1's records, both [redacted] and [redacted] had the same date of birth and address in Hanoi, Vietnam. The company associated with both accounts was named "THE FOXCLOUD CO. LTD", and had the domain **www.thefox.cloud**. A review of the

deposits made into these accounts showed that they received funds from various companies for alleged IT work.

94. As of January 26, 2024, the website for the domain **thefox.cloud** was still under construction.

95. Below is a chart that summarizes the connections between the domains and North Korean IT workers:

Chart for Group E – The FoxCloud LLC



96. Based on the above, there is probable cause to believe that funds originating from a DPRK IT worker based outside the United States were sent into the United States in order to

purchase **thefox.cloud** and that this domain was used with the intent of promoting a conspiracy to violate IEEPA. **Thefox.cloud** is therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

THE SUBJECT DOMAIN NAMES

97. As described above, I submit that I have probable cause to believe that the **Subject Domain Names** were used by Yanbian Silverstar actors to facilitate the hiring of North Korean IT workers. As part of this scheme, these North Korean IT workers stole personally identifying information, including the identities of individuals located in the Eastern District of Missouri and elsewhere. They did this and registered the **Subject Domain Names** to evade detection by U.S. law enforcement.

98. Thus, I submit that there is probable cause to believe that funds originating outside the United States from DPRK IT workers were used to purchase and retain the **Subject Domain Names**, and that these domains were involved in an international money laundering offense (i.e. these funds travelled from/to a place outside the United States to/from/through a place inside the United States and were used to purchase the relevant domains with the intent of promoting the carrying on a conspiracy to violate IEEPA).

99. Based on the evidence discussed above, I have probable cause to believe DPRK IT workers used the **Subject Domain Names** to claim to prospective American employers that they could develop websites, as well as advertise their freelancer services to United States companies looking to complete web, application, and mobile development projects.

100. A search of publicly available WHOIS domain name registration records revealed that the **Subject Domain Names** were registered and maintained by one of the following

registrars:

a. GoDaddy.com, LLC, a company headquartered in Tempe, AZ;

b. NameCheap, Inc., a company headquartered in Phoenix, AZ;

c. Public Domain Registry, a company headquartered in Tempe, AZ;

d. Squarespace, Inc., a company headquartered in New York, NY; and

e. Tucows Inc., a company headquartered in Canada with an office in Bellevue, Washington.

101. The use of multiple registrars provides an opportunity to seize the **Subject Domain Names** from the top-level registry, instead of through five individual registrars.

102. The top-level domain for all the ".com" and ".net" domains in the **Subject Domain Names** is Verisign, Inc. (hereinafter "Verisign"). Verisign currently manages all ".com" and ".net" domains.

103. The top-level domain for the ".us" domain in the **Subject Domain Names** is GoDaddy.com, LLC, who manages all ".us" domains.

104. The only remaining domain which is not ".com", ".net", or ".us" in the **Subject Domain Names** is a ".cloud" domain registered at Squarespace, Inc. The top-level domain ".cloud" is managed by an organization not located in the United States, Aruba S.p.A. in Italy. However, Tucows, Inc. is the technical contact for the ".cloud" domains and can seize ".cloud" domains. Therefore, the **Subject Domain Names** seizure for the ".cloud" domain will be done at Tucows, Inc.

105. Lastly, the ".us" domain's registrar is Tucows, Inc., and since the ".cloud" domain will be seized at Tucows, Inc., the ".us" domain will be seized from Tucows, Inc., instead of the

top-level registry, GoDaddy.com, LLC.

106. Below is a chart summarizing the above seizure plan:

Domain	Registrar	TLD	TLD Registry	Serve Order
omegasoftware.us	Tucows, Inc.	.us	GoDaddy.com, LLC	Tucows, Inc.
thefox.cloud	Squarespace, Inc.	.cloud	Aruba S.p.A. – Tucows, Inc. (Technical Admin)	Tucows, Inc.
bynolt.com	GoDaddy.com, LLC	.com	Verisign	Verisign
logictech-us.com	NameCheap, Inc.	.com	Verisign	Verisign
cubixtechus.com	NameCheap, Inc.	.com	Verisign	Verisign
helix-us.com	NameCheap, Inc.	.com	Verisign	Verisign
babyboxinfo.com	NameCheap, Inc.	.com	Verisign	Verisign
blackishtech.com	Public Domain Registry	.com	Verisign	Verisign
purpleishtech.com	Tucows, Inc.	.com	Verisign	Verisign
culturebx.com	Tucows, Inc.	.com	Verisign	Verisign
nextnets.com	Tucows, Inc.	.com	Verisign	Verisign
illusionsoft.net	Tucows, Inc.	.net	Verisign	Verisign

SEIZURE PROCEDURE

107. As detailed in Attachments A-1 and A-2, upon execution of the seizure warrant, the registry for the ".com" and ".net" top-level domain, Verisign Inc., the registrar for the ".us" domain, Tucows, Inc., and the technical contact for the ".cloud" domain, Tucows, Inc., shall be directed to restrain and lock the **Subject Domain Names** pending transfer of all right, title, and interest in the **Subject Domain Names** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **Subject Domain Names** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.

108. In addition, upon seizure of the **Subject Domain Names** by the FBI, Verisign and Tucows, Inc. will be directed to associate the **Subject Domain Names** to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a

notice on the website to which the **Subject Domain Names** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

109. Based on the information contained in this affidavit, I submit that there is probable cause to believe that funds originating from outside the United States were transferred to/through the United States to purchase the **Subject Domain Names** and that these domains were used to promote the violation of IEEPA. Accordingly, the **Subject Domain Names** are therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1) and I respectfully request that the Court issue a seizure warrant for the **Subject Domain Names**

110. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **Subject Domain Names** for forfeiture. By seizing the **Subject Domain Names** and redirecting traffic to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the **Subject Domain Names** will prevent third parties from continuing to access these websites.

111. Because the warrant will be served on Verisign Inc. and Tucows, Inc., which control the **Subject Domain Names**, at a time convenient to them, and the registry or registrar will transfer control of the **Subject Domain Names** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

112. Finally, and in order to protect the ongoing investigation and in consideration that much of the information set forth above is not otherwise publicly available, I respectfully request that this Affidavit be filed and kept under seal until further order of this Court.

I state under the penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

[redacted]

[redacted]
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on May 3, 2024.

[redacted]

HONORABLE NOELLE C. COLLINS
United States Magistrate Court Judge

ATTACHMENT A-1

SUBJECT DOMAIN NAMES	
1	babyboxinfo.com
2	blackishtech.com
3	bynolt.com
4	cubixtechus.com
5	culturebx.com
6	helix-us.com
7	illusionsoft.net
8	logictech-us.com
9	nextnets.com
10	purpleishtech.com

With respect to domains listed above ("SUBJECT DOMAIN NAMES"), Verisign Inc., 12061 Bluemont Way, Reston, Virginia 20190, who is the domain registry for the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAMES:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation by associating the SUBJECT DOMAIN NAMES to the following authoritative name-server(s):

   (a) hans.ns.cloudflare.com;

   (b) surina.ns.cloudflare.com; and/or

   (c) Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registry.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the

SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued by the United States District Court for the Eastern District of Missouri as part of a law enforcement action against North Korean Information Technology (IT) Workers who used it as a software development and portfolio website to advertise and obtain remote IT freelancer jobs using fraudulent identities.

For additional information on North Korea's use of remote IT workers and how to identify them see the following advisories:

1) Guidance on the DPRK Information Technology Workers – Treasury.gov – Enter "North Korean IT Workers Advisory" into any search engine –
2) Additional Guidance on DPRK IT Workers – PSA at IC3.gov

>> Report suspicious IT workers to IC3.gov <<

ATTACHMENT A-2

SUBJECT DOMAIN NAMES	
1	omegasoftware.us
2	thefox.cloud

With respect to domains listed ("SUBJECT DOMAIN NAMES"), Tucows, Inc., 10400 NE 4th Street, 5th Floor, Suite 121, Bellevue, Washington 98004, who is the domain registrar for the ".us" domain and the technical contact for the ".cloud" domain, listed in the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAMES:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation by associating the SUBJECT DOMAIN NAMES to the following authoritative name-server(s):

   (a) hans.ns.cloudflare.com;

   (b) surina.ns.cloudflare.com; and/or

   (c) Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registrar.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain

Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued by the United States District Court for the Eastern District of Missouri as part of a law enforcement action against North Korean Information Technology (IT) Workers who used it as a software development and portfolio website to advertise and obtain remote IT freelancer jobs using fraudulent identities.

For additional information on North Korea's use of remote IT workers and how to identify them see the following advisories:

1) Guidance on the DPRK Information Technology Workers – Treasury.gov – Enter "North Korean IT Workers Advisory" into any search engine –
2) Additional Guidance on DPRK IT Workers – PSA at IC3.gov

>> Report suspicious IT workers to IC3.gov <<