

UNITED STATES DISTRICT COURT
for the

Eastern District of Missouri

In the Matter of the Seizure of
Twelve (12) ".Com" Domain Names, further
described in Attachment A-1

)
)
) Case No. 4:23MJ9240 RHH
)
)
)

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) ".Com" Domain Names, further described in Attachment A-1

which is

subject to forfeiture under Title 18, United States Code, Sections 981(a), 982(a), and 1028(b) and Title 28, United States Code, Section 2461(c), and therefore is subject to seizure under Title 18, United States Code, Sections 981(b) and 982(b), Title 21, United States Code, Sections 853(e)&(f) and Title 28, United States Code, Section 2461(c) concerning a violation of Title 18, United States Code, Sections 1028, 1343, 1349, 1956, 1957 and 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

October 5, 2023
Date and Time Issued

Honorable Rodney H. Holmes, U.S. Magistrate Judge
Name and Title of Judicial Officer

at St. Louis, Missouri

[REDACTED]
Signature of Judicial Officer

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

UNITED STATES OF AMERICA)
)
)
v.)
)
TWELVE (12) “.COM”;)
ONE (1) “.CLOUD”;)
ONE (1) “.INFO”;)
ONE (1) “.ASIA”;)
ONE (1) “.SERVICES”;)
ONE (1) “.TECH”)
DOMAIN NAMES)

Filed Under Seal

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 Federal Bureau of Investigation (“FBI”). I have been a Special Agent with the FBI since [REDACTED] 2007. Since April 5, 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. 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.

3. This affidavit does not contain all of the information known to me in regard to the investigation; however, it contains information establishing probable cause to seize multiple domains set forth in Attachment A-1 and A-2 (the “**Subject Domain Names**”).

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that unknown and known foreign persons have committed violations of 18 U.S.C. §§ 1028 (identity theft), 1343 (wire fraud), 1956 and 1957 (money laundering), 1349 (attempt and conspiracy to commit wire fraud), and 50 U.S.C. § 1701 et seq. (International Emergency Economic Powers Act, or “IEEPA”) (the “**Subject Offenses**”), including in connection with making online payments to obfuscate an individual’s location in order to violate U.S. sanctions and induce individuals online to hire the individual to perform freelancer work for them, as explained in more detail below. There also is probable cause to seize the Subject Domain Names as described in Attachment A-1 and A-2.

PURPOSE OF APPLICATION

5. I submit this application in support of seizure warrants for seventeen (17) domain names, as detailed in Attachments A-1 and A-2, hereafter referred to as **Subject Domain Names**, as property used or intended to be used to commit or to facilitate the commission of the Subject Offenses, and are therefore subject to seizure pursuant to 21 U.S.C. § 853(f) and 18 U.S.C. § 1028(g). The procedure by which the government will seize the **Subject Domain Names** are described in Attachments A-1 and A-2 hereto and below.

APPLICABLE STATUTES

International Emergency Economic Powers Act (IEEPA)

6. Under IEEPA, it is a crime to willfully violate or conspire to violate any license, order, regulation, or prohibition issued pursuant to IEEPA, including restrictions imposed by the Department of Treasury. 50 U.S.C. § 1705(a).

7. The Department of Treasury's Office of Foreign Asset Control (OFAC) has the authority to designate for sanctions entities or people determined to have violated the President's Executive Orders.

8. On September 13, 2018, OFAC designated for sanctions a North Korean information technology firm based in China named Yanbian Silverstar Network Technology Co., Ltd ("Yanbian Silverstar"), as well its Russia-based front company, Volasys Silver Star, for violating the President's Executive Orders. These entities exported workers from North Korea to generate revenue for the Government of North Korea (in violation of Executive Order 13722), and employed North Korean workers in the information technology industry (in violation of Executive Order 13810). The same OFAC designation also included 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 had 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.

Wire Fraud

10. 18 U.S.C. § 1343 (wire fraud) criminalizes devising or intending to devise a scheme to defraud (or performing specific fraudulent acts) through the use of an interstate telephone call or electronic communication. 18 U.S.C. § 1349 criminalizes attempt and conspiracy to commit, *inter alia*, wire fraud.

Money Laundering

11. 18 U.S.C. § 1956(h) criminalizes a conspiracy to commit money laundering.

12. 18 U.S.C. § 1956(a)(1)(B)(i) criminalizes conducting, or attempting to conduct, a financial transaction which involves the proceeds of specified unlawful activity, knowing that the property involved in such financial transaction represents the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of said specified unlawful activity.

13. 18 U.S.C. § 1957 (the money laundering spending statute) criminalizes knowingly engaging or attempting to engage in a monetary transaction in criminally derived property from a specified unlawful activity in an amount greater than \$10,000.

14. Under 18 U.S.C. § 1956(c)(7)(D), the term “specified unlawful activity” includes violations of IEEPA. The financial transactions described in this affidavit are overt acts in furtherance of a money laundering conspiracy to conceal IEEPA violations.

Identity Theft

15. Pursuant to Title 18, United States Code, Section 1028(b)(5), any personal property used or intended to be used to commit the offense of Identity Theft is subject to criminal forfeiture.

Forfeiture

16. The proceeds of wire fraud, and conspiracy to commit wire fraud, are subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, or conspiracy to commit wire fraud, is subject to civil forfeiture. In addition, 28 U.S.C. § 2461(c) provides that, “[i]f a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized,” then the government can obtain forfeiture of property “as part of the sentence in the criminal case.” Thus, pursuant to 28 U.S.C. § 2461(c) and 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud is subject to criminal forfeiture.

17. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property which constitutes or is derived from proceeds traceable to a violation of IEEPA, is subject to criminal and civil forfeiture.

18. Property involved in a money laundering offense is subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to civil forfeiture. In addition, pursuant to 18 U.S.C. § 982(a)(1), any property involved in a violation of 18 U.S.C. § 1956, or

any property traceable to such property, is subject to criminal forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property “involved in” the crime, which can include untainted funds that are comingled with tainted funds derived from illicit sources.

19. Pursuant to 18 U.S.C. § 981(b), property subject to civil forfeiture may be seized by a civil seizure 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. § 1335(b)(1)(A). As detailed below, acts in furtherance of the fraud and money laundering scheme under investigation occurred in the Eastern District of Missouri. The criminal forfeiture statute, 18 U.S.C. § 982(b)(1), incorporates the procedures in 21 U.S.C. § 853, which provides authority for the issuance of a seizure warrant for property subject to criminal forfeiture.

20. 18 U.S.C. § 984 allows the United States to seize for civil forfeiture identical substitute property found in the same place where the “guilty” property had been kept. For purposes of Section 984, this affidavit need not demonstrate that the funds now in the Target Accounts are the particular funds involved in the fraud and money laundering violations, so long as the forfeiture is sought for other funds on deposit in that same account. Section 984 applies to civil forfeiture actions commenced within one year from the date of the offense.

21. Based on the foregoing, the issuance of this seizure warrant is authorized under 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b)(1) for criminal forfeiture; and 18 U.S.C. §§ 981(b) and

984 for civil forfeiture. Notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, the issuance of this seizure warrant in this district is appropriate under 18 U.S.C. § 981(b)(3) and 28 U.S.C. § 1355(b)(1) because acts or omissions giving rise to the forfeiture occurred in the Eastern District of Missouri.

22. Based on the foregoing, the issuance of this seizure warrant is authorized under 21 U.S.C. § 853(f) and 18 U.S.C. § 1028(g) for criminal forfeiture.

23. 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 them 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 the **Subject Domain Names** and their corresponding websites in their present form.

24. As set forth below, there is probable cause to believe that the **Subject Domain Names** are subject to criminal forfeiture because they were used in the commission of violations of the SUBJECT OFFENSES. Specifically, the **Subject Domain Names** were used or intended to be used to commit IEEPA violations, acquired from identity theft, and facilitate money laundering of the group's freelancer revenue.

BACKGROUND REGARDING NORTH KOREAN INFORMATION TECHNOLOGY WORKERS

25. According to a May 16, 2022, report jointly issued by the U.S. Department of State, Department of 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.

26. Because this work violates U.S. sanctions, 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.

27. 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.

28. 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.

29. The North Korean IT workers are primarily 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 appear that they are connecting to online services from false locations.

BACKGROUND ON DOMAIN NAMES

30. 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 address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (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 at 12061 Bluemont Way, Reston, Virginia.

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 IP address resolves 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**

31. In August 2019, the FBI interviewed an individual located in the United States (“Individual 1”) who had an account at [REDACTED]. [REDACTED] is a global freelancing platform based in the United States, which serves as an online marketplace where businesses advertise for independent professionals or freelance workers, who in turn can find work in a variety of industries, including software development and information technology.

32. Individual 1 described communications with another individual who has been using a specific [REDACTED] account and telephone number ending in 4091. This second individual is referred to as [REDACTED].

33. Individual 1 allowed [REDACTED] to use Individual 1’s [REDACTED] account for freelance work. Individual 1 also agreed to purchase a laptop for [REDACTED] and keep it in Individual 1’s home in the United States. Individual 1 told the FBI that [REDACTED] used remote access software to use the computer located in Individual 1’s residence, and that the computer’s monitor showed that the remote user was using the computer for [REDACTED]. Individual 1 eventually had four laptops used by [REDACTED], with [REDACTED] paying Individual 1 \$100 per month per laptop.

34. [REDACTED] also requested that Individual 1 find other people with additional [REDACTED] accounts that [REDACTED] could use, but Individual 1 did not refer any people to [REDACTED].

35. For the work completed by [REDACTED] through Individual 1’s [REDACTED] account, the payments would be channeled through Individual 1’s [REDACTED] account and sent (minus a portion of the money kept by Individual 1) to [REDACTED] using his accounts at the payment platforms [REDACTED] and [REDACTED].

36. According to Microsoft, the [REDACTED] account used by [REDACTED] was registered with a specific email address through Yandex.com. Yandex.com is a Russian email provider.

37. According to [REDACTED] the account registered with the telephone number ending in [REDACTED] was registered using the email address [REDACTED]@gmail.com, and the answer to the security question is “[REDACTED].”

38. According to [REDACTED] the account used by [REDACTED] to receive payment from Individual 1 for freelance work was registered using the email address [REDACTED]@126.com (126.com is a Chinese email provider), and the answer to the security question was “[REDACTED]” which is Chinese for Silver Star. According to [REDACTED] this account used by [REDACTED] to receive payment from Individual 1 for freelance work received over \$85,000 between April 2018 and October 2019.

39. Based on my training and experience, the use of a Chinese email provider and security question, the similarity of the security question to the name of the sanctioned North Korean IT worker front company Yanbian Silverstar, the receipt of funds, and the use of an intermediary’s [REDACTED] account, multiple [REDACTED] accounts, multiple email accounts, and a U.S.-based laptop to conduct freelance IT work, I have probable cause to believe that [REDACTED] is a North Korean IT worker living in China and working at Yanbian Silverstar. [REDACTED] was subsequently identified as [REDACTED], a North Korean IT worker working for Yanbian Silverstar.

40. Through an approved undercover operation, the FBI utilized an online undercover employee (“OCE”) to communicate while in the Eastern District of Missouri via [REDACTED] with [REDACTED]. In August 2020, [REDACTED] explained his need for a U.S. [REDACTED] account and that he would pay 15% of the monthly earnings to the OCE for the use of the account. Also, [REDACTED] needed a laptop

so he could connect via a remote desktop-type application. This would provide [REDACTED] with the appearance of residing in the United States and the ability to avoid using a Virtual Private Network (“VPN”) IP address which might be blocked by [REDACTED]. On August 16, 2020, [REDACTED] agreed to provide \$75 to the OCE to purchase a laptop.¹ On August 17, 2020, OCE received the \$75 payment from a [REDACTED] account registered with email address [REDACTED]@126.com.

41. According to [REDACTED] the account used by [REDACTED] to receive payment from Individual 1 for freelance work logged on from IP address 36.97.143.26 (“IP Address 1”) from April 27, 2018, to October 13, 2019. Based on databases regularly relied upon by the FBI, IP Address 1 resolves to China Telecom, Jilin, China and was associated with a dedicated server during this time period. This means accounts accessed by IP Address 1 during this time period would have been working together, likely from the same location and for the same organization. As described below, records from [REDACTED] identified multiple accounts accessed from IP Address 1 were used by Yanbian Silverstar freelancers.

42. Based on my training and experience, and evidence of a North Korean IT worker living in China and working at Yanbian Silverstar using a Chinese dedicated server located at IP Address 1 to access [REDACTED] have probable cause to believe that others using IP Address 1 between April 27, 2018, to October 13, 2019, are also North Korean IT workers living in China and working at Yanbian Silverstar.

¹ The FBI purchased and provided remote access for [REDACTED] to access the laptop and conduct their IT work.

43. The FBI's review of the account information for these [REDACTED] accounts showed payments from freelancer platforms such as [REDACTED]. Many [REDACTED] accounts also listed multiple email addresses in their subscriber information (allowing the user to register numerous freelancer platform accounts with the same [REDACTED]). These characteristics corroborate the probable cause that these domains and accounts are used by North Korean IT workers living in China and working at Yanbian Silverstar.

44. In February and July, 2022, United States Magistrate Judges Shirley P. Mensah and John M. Bodenhausen in the Eastern District of Missouri signed federal search warrants for numerous Google and Microsoft for accounts associated to Yanbian Silverstar actors based on the information received from [REDACTED]. The communications from these Google and Microsoft accounts discussed using identities of third parties 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.

45. A review of the records from the Google and Microsoft search warrants identified additional email accounts, bank accounts, telephone numbers, fictitious company names, and stolen personally identifiable information (PII), such as SSN, date of birth, and address, used by the Yanbian Silverstar actors to create their online payment and freelancer platform accounts.

46. The email addresses and financial identifiers associated with Yanbian Silverstar, provided by [REDACTED] Microsoft, and Google, were in turn provided to [REDACTED]. [REDACTED] provided a list of accounts matching those identifiers. The general pattern of these accounts includes physical addresses in China, payments received from freelancer and payment platforms,

and withdrawals of funds to accounts at Chinese banks. I know from my training and experience that North Korean IT workers frequently use China-based banks to spend their freelancer revenue or else transmit it to North Korea.

47. During the course of the investigation multiple domains associated with North Korean IT workers were identified. The following outlines the probable cause associated with each of the **Subject Domain Names**:

A. **silverstarchina.com**

48. On or about November 4, 2019, [REDACTED] identified 64 [REDACTED] accounts that were created or accessed from IP Address 1 between April 27, 2018, to October 13, 2019. Many contained the name “Silver Star” in their subscriber information and indicated that the users’ location was in Jilin, China, corroborating that the accounts are used by North Korean IT workers living in China and working at Yanbian Silverstar. For example, one of these [REDACTED] accounts listed the business name “Yanbian Silver Star Network Technology Co., Ltd.” listed an address in Jilin, China, and used the email address [REDACTED]@silverstarchina.com. The [REDACTED] was restricted by [REDACTED] on September 18, 2018.

49. A review of open source information for **silverstarchina.com** identified the registrar and hosting provider was Bluehost.com, 1500 N Priest Drive, Suite 200, Tempe, AZ 85281. On or about August 15, 2023, [REDACTED] Bluehost provided the subscriber records for the domain, **silverstarchina.com**. The account was registered in the name [REDACTED] email address [REDACTED]@hotmail.com, Changbai Road, Yanji, China, and they have been a customer since November 12, 2015. Yanbian Silverstar has locations in Yanji,

China. The account had been paid by through [REDACTED] accounts with the email addresses [REDACTED]@hotmail.com, [REDACTED]@126.com, [REDACTED]126.com, [REDACTED]@126.com, [REDACTED]@126.com, and [REDACTED]@126.com. The most recent payment occurred from the [REDACTED] account, [REDACTED]@hotmail.com, on November 11, 2022, and renewed the domain silverstarchina.com for one year. The hosting plan at Bluehost was not renewed.

50. On or about March 7, 2022, [REDACTED], a review [REDACTED] records for the account associated to the email addresses [REDACTED]@hotmail.com and [REDACTED]@126.com identified payments to Bluehost.com totaling \$4,398.26 from November 10, 2014, to February 23, 2019.

51. Yanbian Silverstar actors have been observed using variations of email addresses with the name “eden” followed by [REDACTED] letters and the Chinese email provider 126.com. Furthermore, the email address [REDACTED]@126.com was identified from [REDACTED] records as being accessed from IP Address 1. Additionally, a [REDACTED] account using the email address [REDACTED]@126.com was identified as being used by North Korea and the remaining funds on the account were seized in response to a seizure warrant issued in the Eastern District of Missouri on October 25, 2022, as proceeds from North Korea IT workers.

52. On or about May 9, 2022, [REDACTED] provided records which identified a customer who on September 4, 2018, provided their freelancer website as “<http://www.silverstarchina.com>”. [REDACTED] requests some customers fill out a questionnaire called “Global Payment Services”. These questions were requested from the customer along with their answer:

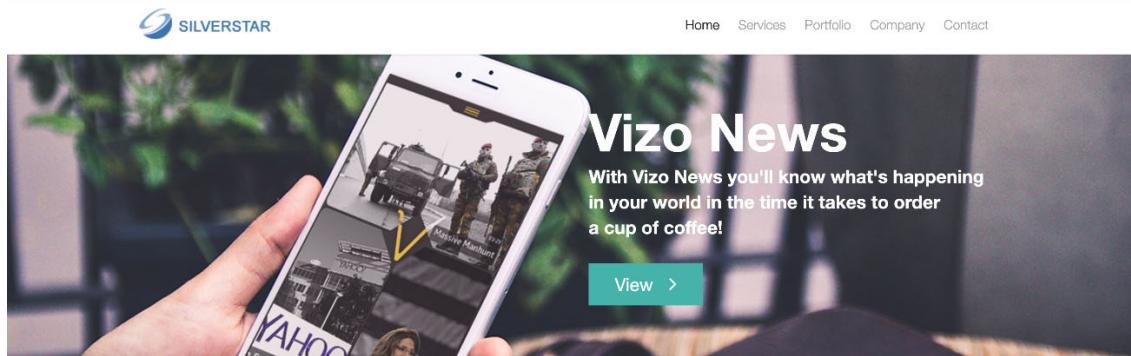
Question	Answer
----------	--------

Select your category	Software development
Provide a direct web link to your online store or website	http://www.silverstarchina.com
Please explain, in English, your source of income and/or business type	I develop mobile apps and websites for my clients.

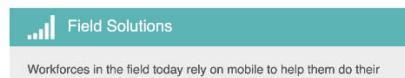
53. In response to the URL question, the customer provided the domain **silverstarchina.com**. The email address for the [REDACTED] account above was [REDACTED]@126.com. A review of Microsoft records in response to a search warrant issued in the Eastern District of Missouri on July 19, 2022, for an account controlled and used by [REDACTED] [REDACTED] Mission Representative for Yanbian Silverstar, located a document in Korean which listed the email address [REDACTED]@126.com. The document was in Korean and listed the address, [REDACTED] Yanji City, which is the same address associated to Silver Star China / China Silver Star / Yanbian Silverstar, and had the name “Chilsong Shiyong JV Co. LTD” stamped on the document.

54. On May 12, 2023, I reviewed the domain **silverstarchina.com** and it did not display any data. A review of the Internet Archive using the Wayback Machine, a website which captures websites on the internet, for **silverstarchina.com**, identified multiple captures were saved. A review of the snapshot from August 10, 2019, identified the website was used by Silver Star China as a portfolio website to advertise their IT development services. The website listed applications they supposedly developed. The site listed the contact address as Yanji, Jilin, CHANG BAI SHAN DONG LU, 20998B-26HAO, Yanji, Jilin 133000 China. This is the same address listed in the Department of Treasury OFAC sanctions for China Silver Star / Yanbian Silverstar.

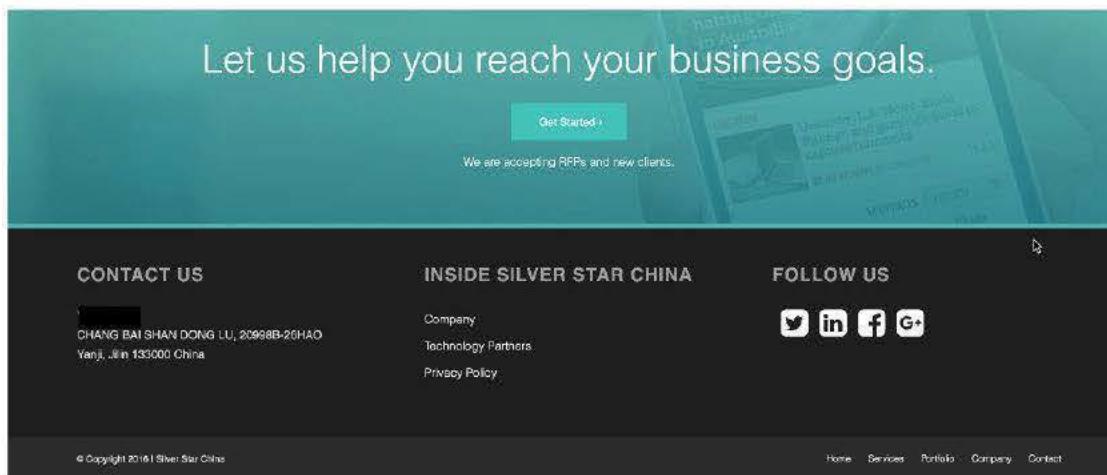
silverstarchina.com – Internet Archive



We Are Industry Leaders In



silverstarchina.com – Contact Us – Internet Archive



55. As discussed above, the domain **silverstarchina.com** is used and controlled by North Korean IT workers working for Yanbian Silverstar and is used to further their ability to obtain IT freelance work. In addition, there is probable cause to believe that criminal proceeds from the aforementioned fraud scheme and conspiracy to violate IEEPA were used to purchase and retain this domain, and that this domain was involved in a money laundering offense (i.e. criminal proceeds were used to purchase the domain in a financial transaction with the intent to promote the carrying on of the fraud scheme and the conspiracy to violate IEEPA).

B. edenprogram.com

56. A review of the [REDACTED] transactions for the [REDACTED]@126.com [REDACTED] account, who provided payment to the OCE for a laptop, identified a \$30 payment on August 6, 2020, to individual named [REDACTED] with the note “Skype – Eden Programming”. The FBI believes a North Korean IT worker paid an individual to setup a Skype account or do some type of work related to the company “Eden Programming.”

57. A review of open source information from October 30, 2020, and November 5, 2020, identified a website at **edenprogram.com** for “Eden Programming” which listed their

address as [REDACTED] Fremont, CA 94538 and two email addresses – info@edenprogram.com and [REDACTED] @gmail.com. The website contained a portfolio of applications and websites the company supposedly completed. A review of open source information for **edenprogram.com** identified the registrar was Tucows.com, 96 Mowat Avenue, Toronto, Ontario and the hosting provider was Google LLC (Google Cloud), 1600 Amphitheatre Parkway, Mountain View, CA 94043.

58. On or about November 13, 2020, [REDACTED] Tucows, the registrar for the domain **edenprogram.com**, provided the organization information for the domain **edenprogram.com** as [REDACTED], using email [REDACTED] @gmail.com, [REDACTED] Fremont, CA 94538, and telephone number [REDACTED]

59. On or about June 15, 2023, [REDACTED] Google provided the subscriber information for **edenprogram.com**. The hosting of the domain was created on July 23, 2020, and listed two contacts: [REDACTED] @edenprogram.com and [REDACTED] @gmail.com. The payment for the domain was a Mastercard in the name of [REDACTED] in Ukraine. Additional payments were in the names of [REDACTED] (United States), [REDACTED] (United States), and [REDACTED] (United States). The included services for the account was Gmail, Drive and Docs, Google Chat, and Google Meet.

60. The names [REDACTED] were both fraudulent identities created by and through a website called “[REDACTED],” which provides fraudulent, but verified [REDACTED] accounts. On or about May 3, 2022, in response a search warrant, Google provided records for the email address [REDACTED] @gmail.com who received emails from [REDACTED] for the [REDACTED] accounts [REDACTED] on January 20, 2021, and [REDACTED] on February 23, 2021. Therefore, the FBI

believes those payment methods used for the **edenprogram.com** domain at Google were fraudulent accounts.

61. On or about May 3, 2022, in response a search warrant, Google provided records for the email address [REDACTED]@gmail.com which was identified as being used by [REDACTED] [REDACTED] a group leader for Yanbian Silverstar. On or about December 19, 2017, an email was received from Google to [REDACTED]@gmail.com regarding the addition of a recovery account for the email address [REDACTED]@gmail.com. Additionally, on or about February 4, 2018, an email was sent by [REDACTED]@gmail.com to an individual who hired [REDACTED] for IT work. The email contained a non-disclosure agreement (NDA) addressed to and signed by [REDACTED]. The FBI believes [REDACTED] [REDACTED] used the persona [REDACTED] to obtain freelancer jobs and controlled the credit card in the name of [REDACTED] for the payments for the **edenprogram.com** domain.

62. Further open-source searches from October 30, 2020, to November 5, 2020, identified a [REDACTED] account, a freelancer website, for “Eden Programming Solutions” (URL was eden-programming-solutions). According to their profile, the group joined in October 2017 and generated \$422,000 in revenue.

63. On or about December 8, 2020, [REDACTED] [REDACTED] provided the following information regarding “eden-programming-solutions”. The name of the group was “Eden Programming Village” with the screen name of “Eden Programming Solutions” and used the name [REDACTED] Oakland, CA, and email address [REDACTED]@gmail.com. The [REDACTED] address is a large business skyscraper. The account had two [REDACTED] accounts: [REDACTED]@gmail.com and [REDACTED]@126.com [REDACTED] [REDACTED] – China) and one [REDACTED] account – [REDACTED]@126.com.

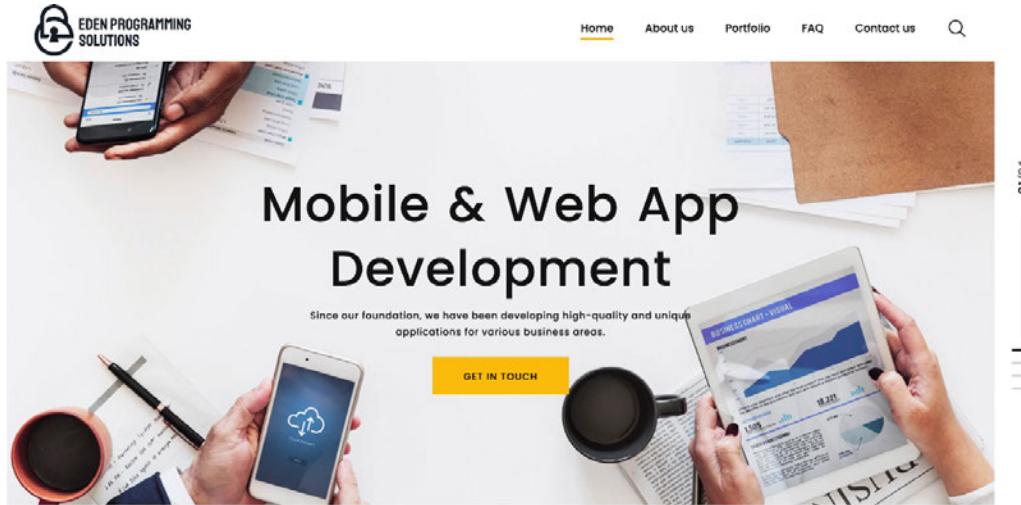
64. The [REDACTED] account [REDACTED]@126.com was previously observed sending money to Individual 1 for allowing the use of their home network and [REDACTED] account. Additionally, on September 2, 2020, the FBI observed on the undercover laptop, [REDACTED]@126.com had [REDACTED] transactions with the account [REDACTED]@gmail.com, which was a target account in a previous search warrant issued in the Eastern District of Missouri on December 17, 2020, and used [REDACTED]@gmail.com as a recovery account.

65. On or about March 16, 2022, in response to a search warrant issued in the Eastern District of Missouri on February 9, 2022, Google provided records for the email account [REDACTED]@gmail.com. The account, along with [REDACTED]@edenprogram.com was linked to [REDACTED]@gmail.com. A review of the [REDACTED]@gmail.com account identified documents containing username and passwords for multiple freelancer identities and email and communication accounts. The account had multiple Korean language documents and viewed locations around North Korea in Google Maps. The user of the account was identified as [REDACTED] group leader for Yanbian Silverstar. Additionally, the [REDACTED].mail.com was linked by cookies to the email addresses [REDACTED]@gmail.com and [REDACTED]@gmail.com.

66. On May 15, 2023, I reviewed the domain **edenprogram.com**. The website was used by Eden Programming Solutions as a portfolio website to advertise their IT development services. The website listed applications development by Eden Programming Solutions, provided a list of employees, who they state are all based in the United States, and the contact information as [REDACTED] Walnut Creek, CA 94596, email addresses *info@edenprogram.com* and [REDACTED]@gmail.com, and telephone numbers [REDACTED] A

review of open source identified the property management company for the [REDACTED] location. Their website listed [REDACTED] as available for lease as of May 12, 2023.

edenprogram.com - Home page



edenprogram.com - Developers

The screenshot shows the 'Main Developers' section of the website. It features a grid of eight developer profiles, each with a blacked-out face and a name tag at the bottom. The names and roles are:

- Lead Developer
- Mobile App Developer
- UI/UX Designer
- PHP/JS Developer
- Web Frontend Developer
- Unity, VB/AR Expert
- Full Stack Developer
- Unreal Engine Developer

A yellow navigation bar at the top includes links for Home, About us, Portfolio, FAQ, Contact us, and a search icon.

edenprogram.com – Contact Us

The contact form page has a dark background. On the left, there is a sidebar with icons for address, e-mail, and social media, along with a list of e-mails. The main form area has fields for Name, E-mail, and Message, followed by a yellow 'SEND MESSAGE' button. To the right, a sidebar lists services offered by the company.

What Do We Offer
iOS/MacOS Apps
Android Apps
Windows Desktop Apps
UI & UX Design
Web Apps
VR/AR Apps And Games
Mobile Games

67. The use of different names, addresses, and North Korean IT worker payment accounts for the domain **edenprogram.com** demonstrate it is used and controlled by North Korean IT workers working for Yanbian Silverstar and is used to further their ability to obtain IT freelance work. Based on the foregoing, there is probable cause to believe that criminal proceeds

from the aforementioned fraud scheme and conspiracy to violate IEEPA were used to purchase and host this domain, and that this domain was involved in a money laundering offense (i.e. criminal proceeds were used to purchase the false identities that were then used to host the domain in a financial transaction with the intent to promote the carrying on of the fraud scheme and the conspiracy to violate IEEPA). In addition, there is probable cause to believe that the domain was used or intended to be used to commit the offense of identity theft.

C. **xinlusoft.com and softdevsun.com**

68. On or about October 27, 2022, in response to a search warrant, Microsoft provided records for the [REDACTED] account [REDACTED] used by [REDACTED] Company President of Yanbian Silverstar. On or about May 31, 2021, [REDACTED] shared a picture of a China National ID card with the number [REDACTED] and DOB: [REDACTED], to another unknown North Korean IT worker.

69. On or about December 7, 2022, [REDACTED] provided records to accounts which had been opened using China National ID cards identified from Microsoft [REDACTED]. The China National ID [REDACTED], DOB: [REDACTED], was used to open three [REDACTED] accounts in the name of [REDACTED] using different email addresses. One of the accounts used the email address [REDACTED]@outlook.com. [REDACTED] requests some customers fill out a questionnaire called “Global Payment Services”. These questions were requested from the customer along with their answer:

Question	Answer
----------	--------

Select the category that best describes the goods or services that you'll be getting paid for.	Programming and technical support
What services do you provide?	Mobile apps and web
What is your connection to the web page or URL provided?	xinlusoft.com
Briefly describe your business. For example, who are your customers? What services or products do you provide?	As the CTO of a company, I have many developers.
Provide the URL to your business's website or your online store's web page.	xinlusoft.com

The above answers were provided by the customer on December 10, 2021, and included the URL **xinlusoft.com**. The user self-identified as the “CTO” (Chief Technology Officer) of the company.

70. A review of the documents provided by the customer to [REDACTED] identified an invoice dated March 9, 2022, from [REDACTED], Company: Xinlu Science & Technology, Xinggong Street, Dalian, Liaoning Unit 5, building 34, Dalian. The address is located in China. The invoice indicated they provided software engineering and consulting services for a company in the United States. Dalian, China is another location where North Korean IT workers work.

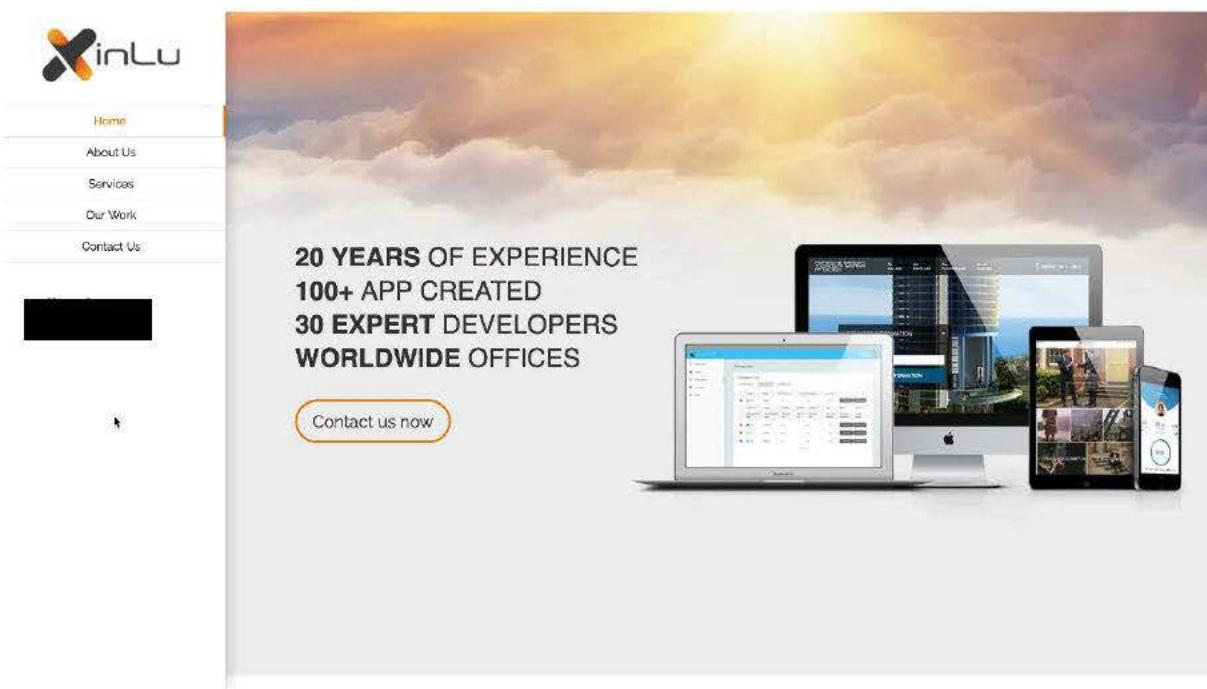
71. On or about January 24, [REDACTED] provided records which identified an account which used the email addresses [REDACTED]@163.[REDACTED] |@foxysun.com, [REDACTED]@gmail.com, [REDACTED]@gmail.com, and [REDACTED]@gmail.com. A review of the transactions identified multiple payments from August 2021 to June 2022 from the [REDACTED] account of the same U.S. company identified in the invoice provided to [REDACTED] as discussed above. Notes were included in the payments which indicated it was for [REDACTED].

72. On or about July 24, 2023, [REDACTED], GoDaddy.com provided records for **xinlusoft.com**. The domain was initially assigned to [REDACTED]”, [REDACTED].

[REDACTED] Kocaeli, Turkey, email address [REDACTED]@gmail.com, telephone number [REDACTED]. On or about June 22, 2023, the user requested the domain be transferred to the user [REDACTED].", email address [REDACTED]@outlook.com, [REDACTED], San Francisco, CA 94108, telephone number [REDACTED]

73. On May 12, 2023, I reviewed the domain **xinlusoft.com**. The website was used by Xinlu Science and Technology Co. Ltd. as a portfolio website to advertise their IT development services. The website listed the contact for the website was listed as *support@xinlusoft.com* and telephone number [REDACTED]. At the bottom of the "About Us" page it stated the website was powered by "Xinlu Science and Technology Co. Ltd" and there was a hyperlink to **foxysun.com**. The "Contact Us" page listed the email address *info@softdevsun.com* and listed their main office address as [REDACTED], Science and Technology Square, [REDACTED] Shahekou District, Dalian, China, telephone [REDACTED]. [REDACTED] Also, **xinlusoft.com** and **foxysun.com** listed several of the same projects, indicating they are the same team.

xinlusoft.com – Home Page



xinlusoft.com – Contact Us



We'd love To Meet You In Person Or Via The Web!

Main Office:

Shahekou District, Dalian, China

Email: info@softdevsun.com

xinlusoft.com – About Us

The screenshot shows the Xinlu company website. At the top right, a banner reads "Meet your new best friends, our gurus." Below the header, there's a navigation menu with links to Home, About Us, Services, Our Work, and Contact Us. The main content area features three profiles:

- Manager:** Shows a placeholder silhouette profile picture. Below it, a bio states: "Our well-experienced manager who is fully focused on technological and scientific issues within Xinlu company!" Three progress bars indicate skills: Product Management at 99%, Product Marketing at 99%, and Project Management at 99%.
- Creative Director:** Shows a placeholder profile picture. Below it, a bio states: "UI/UX design expert who works by aiming at the needs of the end user. She is comfortable in all aspects of UI design. Elana's experience helps to carry out an effective integration and delivery of target content, functionality, visuals and technology to make your project more successful." Three progress bars indicate skills: Mobile Design at 99%, Web Design at 99%, and Logo Design at 99%.
- CTO:** Shows a placeholder profile picture. Below it, a bio states: "An has rich experience in software development. He has a good sense of humor and rich experience in project management." Three progress bars indicate skills: Development at 99%, Management at 99%, and Finance at 89%.

74. A review of a United Nations Security Council report dated August 28, 2020, revealed the Panel investigated a company called “Dalian Xinlu Science and Technology Co. Ltd.”, which according to the report is run by a North Korean IT worker in Dalian, China, named [REDACTED]

75. A review of Microsoft records in response to a search warrant issued in the Eastern District of Missouri on July 19, 2022, for an account controlled and used by [REDACTED] [REDACTED] the company president of Yanbian Silverstar, identified a [REDACTED] on or about February 13, 2019, between [REDACTED] and another unidentified North Korean. In the [REDACTED] the unknown North Korean requests a telephone number from [REDACTED] who responds with [REDACTED]. As discussed previously, one of the [REDACTED] email addresses associated to payments received from freelancer work related to Xinlu Science & Technology was listed as [REDACTED] @163.com.

The sharing of the telephone number [REDACTED] further links Yanbian Silverstar to the **xinlusoft.com** domain.

76. The sharing of a China National ID Card and telephone number by [REDACTED] [REDACTED] the Yanbian Silverstar company president, demonstrates the domain **xinlusoft.com** is controlled by North Korean IT workers working for Yanbian Silverstar.

77. On May 12, 2023, I reviewed the domain **softdevsun.com**, which was identified on the **xinlusoft.com** website. A review of the Internet Archive using the Wayback Machine for **softdevsun.com** identified a capture from July 26, 2019. The website was used by Xinlu Science and Technology Co. Ltd. as a portfolio website to advertise their IT development services. The same projects were listed on the website as observed on **xinlusoft.com** and **foxysun.com**.

softdevsun.com – Contact Us – Internet Archive

The screenshot shows the Wayback Machine interface with the URL <http://softdevsun.com/contact-us/>. It displays 9 captures between 22 Jun 2019 and 21 Sep 2019. The page content includes a navigation menu with links to Home, About Us, Services, Our Work (with sub-links for All Projects, Web, Mobile, E-commerce, Animation), and Contact Us. Below the menu, there is an email address info@softdevsun.com and a placeholder text "Loading...".

78. On or about July 24, 2023, [REDACTED] GoDaddy.com provided records for **softdevsun.com**. The domain was registered by [REDACTED], [REDACTED]

[REDACTED] Kocaeli, Turkey, email address [REDACTED]@gmail.com, telephone number [REDACTED]. The domain expired on June 8, 2023, and as of July 10, 2023, was on hold at GoDaddy.com. As of August 26, 2023, the domain was registered at Hong Kong Juming Network Technology Co., and the current owner could not be verified.

79. On or about June 26, 2023, [REDACTED] provided records for the business account for FoxySun Studios LLC, foxysun.com, email accounts@foxysun.com, in the name of [REDACTED]. The account was opened on August 24, 2017, and had 34 additional email addresses in various names associated to the account, including [REDACTED]@gmail.com. A review of the transactions identified payments to GoDaddy.com for the following domains: **foxysun.com** (January 4, 2023 – Renewed for 8 years), **xinlusoft.com** (January 4, 2023 – 3 year registration), and **foxysunstudios.com** (March 29, 2022 – 3 year registration). Additionally, multiple payments were received for freelancer work. The use of multiple email addresses in different names and freelancer payments are consistent with North Korean IT worker activity. As further discussed below, the following domains had payments from the [REDACTED] account to GoDaddy.com:

- foxysun.com: January 4, 2023
- xinlusoft.com: January 4, 2023
- danielliu.info: November 25, 2022
- jinyang.asia and jinyang.services: September 7, 2022
- foxysunstudios.com: March 29, 2022
- foxyssunstudio.com: March 29, 2022
- thefoxesgroup.com: January 26, 2022
- thefoxcloud.com: January 26, 2022
- cloudfoxhub.com: November 24, 2021
- mycloudfox.com: November 24, 2021
- cloudbluefox.com: November 24, 2021
- danielliu.info: November 24, 2021

80. Based on the foregoing, there is probable cause to believe that criminal proceeds from the aforementioned fraud scheme and conspiracy to violate IEEPA were used to purchase and host these domains, and that these domains were involved in a money laundering offense (i.e. criminal proceeds were used to host the domain in a financial transaction with the intent to promote the carrying on of the fraud scheme and the conspiracy to violate IEEPA).

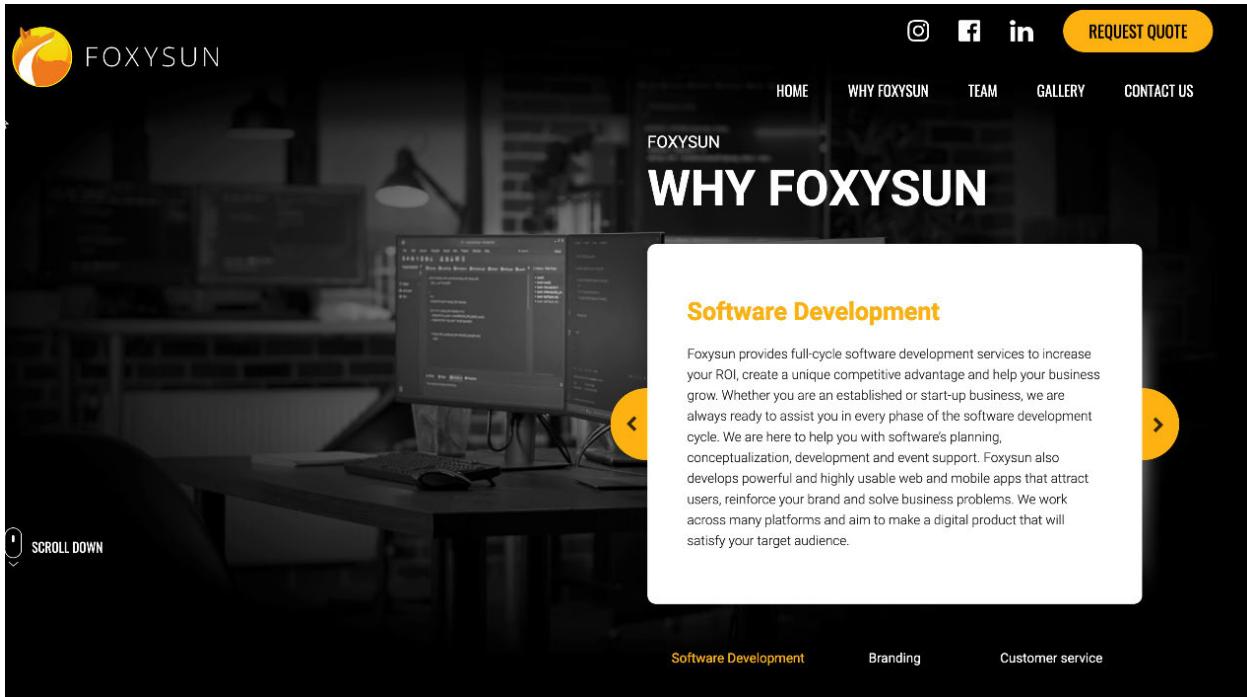
D. **foxysun.com, foxysunstudio.com, foxyssunstudios.com, cloudbluefox.com, cloudfoxhub.com, mycloudfox.com, thefoxcloud.com, thefoxesgroup.com, cloudfox.cloud, danielliu.info, jinyang.asia, and jinyang.services**

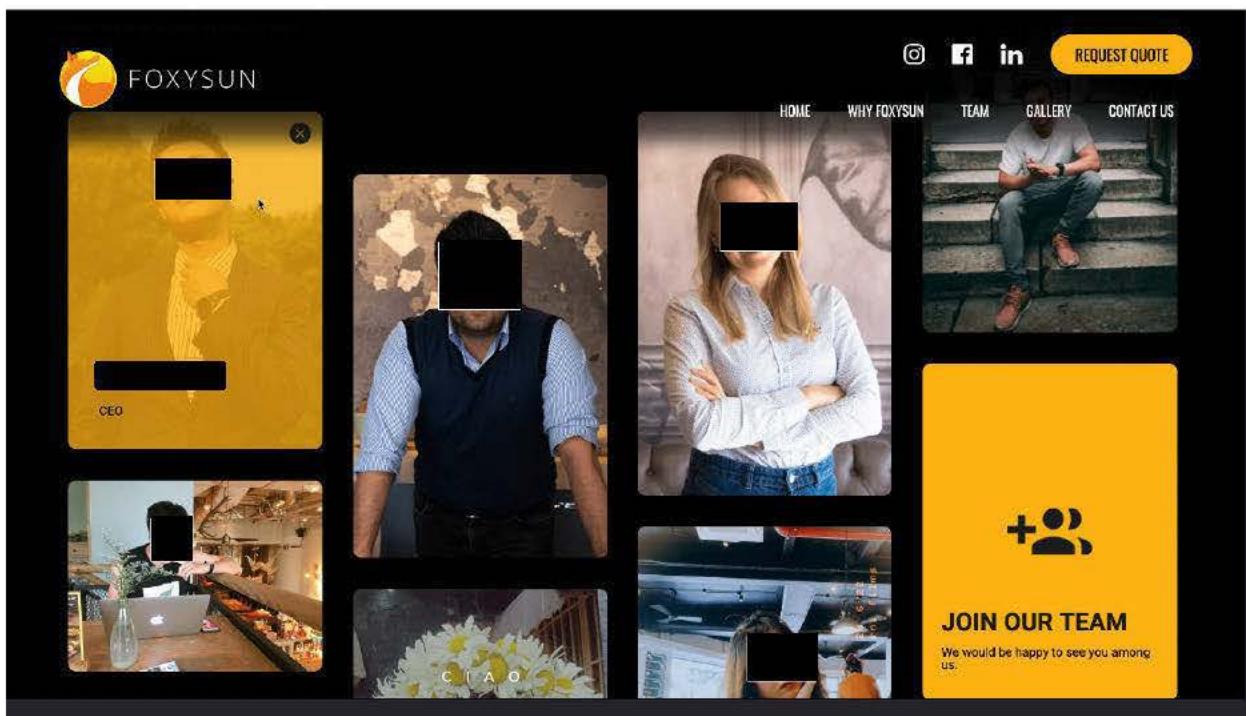
81. On or about December 13, 2019, the FBI's Internet Crime Complaint (IC3) received a complaint from an individual regarding FoxySun Studios LLC, [REDACTED] San Francisco, CA 94108, telephone number [REDACTED], website **foxysun.com** and **foxyssunstudio.com**. An individual named [REDACTED], whom complainant stated was in China, requested to use the complainant's [REDACTED] account and they would receive a 15% of all jobs they completed. Additionally, [REDACTED]. requested to get remote access of their computer. The request to use an individual's [REDACTED] account and network is indicative of North Korean IT workers.

82. On May 12 and 15, 2023, I reviewed the website at **foxysun.com** and it identified the company FoxySun Studios, LLC and [REDACTED] was listed as the CEO. The website was used as a portfolio website to advertise their IT development services. Their office was located in San Francisco and the telephone number [REDACTED]. A business search at the State of California Secretary of State website did not locate a registered LLC for FoxySun Studios. A business search at the State of Nevada Secretary of State website identified a company named Foxy Sun Studios, LLC. The entity was registered on April 5, 2017, and was dissolved as of May 30, 2023.

The officer/manager for the LLC was listed as [REDACTED] [REDACTED], San Francisco, CA 94108.

fooxysun.com – Home Page





83. On May 12, 2023, I reviewed the Internet Archive using the Wayback Machine for **foysun.com** and located a capture from July 4, 2020. The capture listed their address as [REDACTED]

[REDACTED] San Francisco, CA 94108.

foxysun.com – Internet Archive



84. On May 23, 2023, I visited the address of [REDACTED], San Francisco, CA and discovered the address did not exist. The address of [REDACTED] did exist, which was provided in the business registration for Foxy Sun Studios LLC. At the address there was a law firm named located in the building. [REDACTED]

[REDACTED]. Additionally, a review the domains **xinlusoft.com**, **foxysun.com**, **foxysunstudios.com** and **softdevsun.com** identified a testimonial from the same law firm which stated in part “Xinlu’s (or FoxySun’s) Development process made relaunching our Law Firm’s outdated Web-site simple, cost effective and painless.”

85. On or about May 12 and 13, 2023, I conducted a review of the page source, the code which the browser uses to display the website, and found the domains **xinlusoft.com** and **foxysun.com** shared the same Google Analytics ID – UA-116042295-1. On or about June 15, 2023, [REDACTED], Google provided the subscriber records for the Google Analytics ID UA-116042295-1 and the ID was created on March 20, 2018, and associated with the email address [REDACTED]@gmail.com.

86. [REDACTED] level of involvement is currently unknown, but North Korean IT workers frequently recruit individuals to assist with creating accounts and allowing their identities to be used. Sometimes these individuals have previously hired IT workers to complete a project. The North Korean IT worker will then request assistance from their client to help with account

creation, financial transactions, or the use of their identity, but the IT worker maintains control of the accounts. Therefore, the FBI believes the website **foxysun.com**, and other related websites discussed below, are used and controlled by North Korean IT workers, using the identity of [REDACTED].

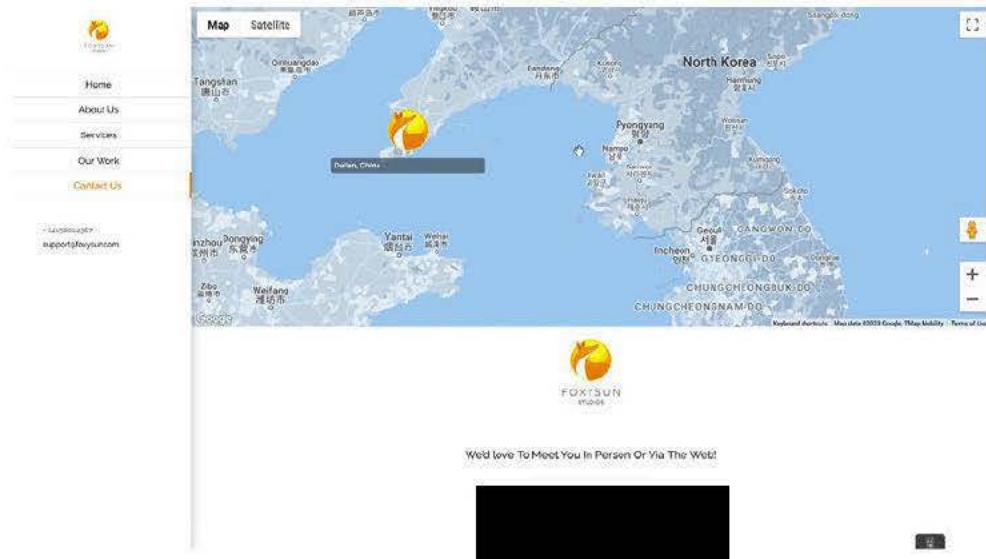
87. As discussed above, the [REDACTED] account for FoxySun Studios LLC, foxysun.com, email *accounts@foxysun.com*, in the name of [REDACTED], was used to purchase the domains **foxysun.com** (January 4, 2023 – Renewed for 8 years), **xinlusoft.com** (January 4, 2023 – 3 year registration), and **foxysunstudios.com** (March 29, 2022 – 3 year registration). In addition, the following domains had payments from that [REDACTED] account to GoDaddy.com:

- foxysun.com: January 4, 2023
- xinlusoft.com: January 4, 2023
- danielliu.info: November 25, 2022
- jinyang.asia and jinyang.services: September 7, 2022
- foxysunstudios.com: March 29, 2022
- foxysunstudio.com: March 29, 2022
- thefoxesgroup.com: January 26, 2022
- thefoxcloud.com: January 26, 2022
- cloudfoxhub.com: November 24, 2021
- mycloudfox.com: November 24, 2021
- cloudbluefox.com: November 24, 2021
- danielliu.info: November 24, 2021

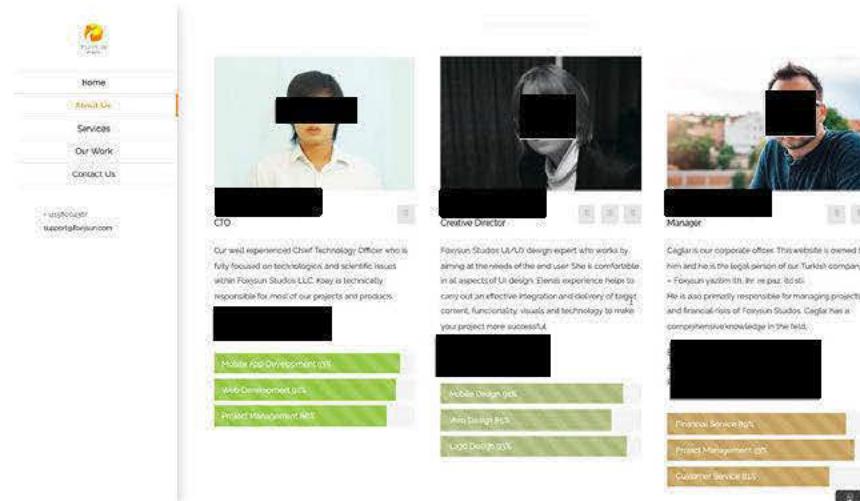
88. None of the above domains currently have a website associated to them but since the domains were paid from the same account as the **foxysun.com**, **xinlusoft.com**, and **foxysunstudios.com**, the FBI believes they are controlled by the same North Korean IT worker group and could be used to facilitate the group's IT work and were included in the **Subject Domain Names**.

89. On May 12, 2023, I reviewed open source information and identified an additional domain associated to FoxySun Studios, LLC. A website was identified at <https://foxysunstudios.com> which listed the contact information as telephone number [REDACTED] [REDACTED] and email address support@foxysun.com/info@foxysun.com. Additionally, the website shared the same WordPress Avada theme as the xinlusosft.com website and listed the same pictures of their employees as the foxysun.com, foxysunstudio.com, and xinlusoft.com website.

foxysunstudios.com – Home Page



foxysunstudios.com – About Us



90. On or about July 21, 2023, [REDACTED] Microsoft

provided subscriber information for [REDACTED] telephone number [REDACTED]. The telephone number was associated to two Microsoft accounts. One account used the telephone number as an alias, [REDACTED] @outlook.com with the name [REDACTED] and was created on June 29, 2016. The user provided their location as China. The other account, which was listed as the customer controlling the account was [REDACTED] user [REDACTED] email address [REDACTED] @gmail.com, and controlled the number as of February 19, 2019. The account used the [REDACTED] account, [REDACTED] @gmail.com, for the payment method. The email address [REDACTED] @gmail.com was also listed on the [REDACTED] @foxysun.com, [REDACTED] account discussed previously.

91. On or about July 5, 2023, [REDACTED], Google provided subscriber records for the email address [REDACTED] @gmail.com, the account associated to the Google Analytics ID shared between the domains **xinlusoft.com** and **foxysun.com**. According to

Google records, the email address [REDACTED]@outlook.com was listed as a recovery account for [REDACTED]@gmail.com and provided their location as Columbia, MD.

92. On or about January 24, 2023, [REDACTED]

provided records which identified an account which used the email addresses

[REDACTED]@163.com, [REDACTED]@fooxysun.com, [REDACTED]@gmail.com, [REDACTED]@gmail.com, and [REDACTED]@gmail.com. A review of the account's transactions identified the following transactions received from [REDACTED] 1 account "FoxySun Studios LLC":

Date	Gross	Note
09-Dec-22	\$1,600.00 USD	[REDACTED] - November 2022 (last)
05-Dec-22	\$5,500.00 USD	[REDACTED] - November 2022 (3)
22-Nov-22	\$3,000.00 USD	[REDACTED] - CN office - November 2022 (2)
09-Nov-22	\$4,800.00 USD	[REDACTED] - CN office - November 2022 (1)
04-Nov-22	\$3,500.00 USD	[REDACTED] - CN Office - October 2022 (4)
25-Oct-22	\$3,000.00 USD	CN Office - [REDACTED] - October 2022 (1)
06-Oct-22	\$5,000.00 USD	[REDACTED] - CN office - Sep 2022 (3)
02-Sep-22	\$5,000.00 USD	[REDACTED] - CN (3)
08-Aug-22	\$3,800.00 USD	- CN office - July 2022
28-Jun-22	\$4,000.00 USD	- CN office - June 2022 (1)
26-Nov-21	\$10,000.00 USD	[REDACTED] - November (1)
30-Jul-21	\$4,500.00 USD	[REDACTED] Xinlu - July(2)
21-Jul-21	\$4,500.00 USD	[REDACTED] Xinlu - July(1)

93. The total amount received from FoxySun Studios was \$63,200.00. The notes identified the payment was either for or sent by [REDACTED] "Xinlu" from the "CN office". The FBI believe [REDACTED] refers to China and "Xinlu" relates to the Xinlu Science & Technology discussed in the **xinlusoft.com** domain section above. Additionally, the use of an email address with the **fooxysun.com** domain indicates the [REDACTED] account which received the payments from FoxySun Studios is connected to Xinlu. IT workers have been observed sending money to accounts they control in order to pay other teams for their expenses or further launder their proceeds.

94. On or about July 24, 2023, [REDACTED], GoDaddy.com provided records related to **foxysun.com**. The domain was initially registered by [REDACTED] [REDACTED] San Francisco, CA 94118, telephone number [REDACTED] email address [REDACTED]. On or about March 13, 2019, the domains **foxysun.com** and **foxysunstudio.com** were transferred to [REDACTED] [REDACTED] Kocaeli, Turkey, email address [REDACTED] @gmail.com, telephone number [REDACTED]. Additionally, the [REDACTED], [REDACTED] @gmail.com, GoDaddy.com account controlled/registered the following additional domains:

<u>Domain</u>	<u>Created</u>	<u>Expires</u>
foxysun.com	3/8/2017	3/8/2031
softdevsun.com	6/8/2018	6/8/2023
cloudbluefox.com	11/24/2021	11/24/2023
mycloudfox.com	11/24/2021	11/24/2023
cloudfoxhub.com	11/24/2021	11/24/2023
danielliu.info	11/24/2021	11/24/2023
cloudfox.cloud	11/24/2021	11/24/2023
thefoxcloud.com	1/26/2022	1/26/2027
thefoxesgroup.com	1/26/2022	1/26/2027
foxysunstudio.com	3/29/2022	3/29/2027
foxysunstudios.com	3/29/2022	3/29/2025
jinyang.services	9/7/2022	9/7/2027
jinyang.asia	9/7/2022	9/7/2027

95. On July 25, 2023, the domains **cloudbluefox.com**, **mycloudfox.com**, **cloudfoxhub.com**, **danielliu.info**, **cloudfox.cloud**, **thefoxcloud.com**, **thefoxesgroup.com**, **jinyang.services**, and **jinyang.asia** were reviewed. None of them had a website associated to them. Based on the use of the word "fox" and [REDACTED]., the FBI believes these domains are placeholders for possible future use by North Korean IT workers. The use of a name [REDACTED] in a

domain indicates another possible persona used by North Korean IT workers to mask their true identity.

96. On July 25, 2023, I reviewed open source information for the domain **foxsunstudio.com**. The website appeared to be similar in content to **foxsun.com** and **foxsunstudios.com**.

foxsunstudio.com – Home Page

The screenshot shows the homepage of foxsunstudio.com. At the top, there is a navigation bar with links for Home, Who we are, Services, Our work, Get in touch, and Blog. To the right of the navigation bar is a large black rectangular redaction box. Below the navigation bar, the text "We develop Technology Solutions." is displayed next to a trophy icon indicating 300,000 satisfied users. To the right of this text is a decorative image of a palm leaf. The page then features three main service sections: "Mobile Applications" (showing several smartphones), "Web Applications" (showing a desktop monitor and a smartphone), and "E-commerce" (showing a hand holding a smartphone displaying an e-commerce interface). Each service section includes a brief description and a "START YOUR PROJECT" button at the bottom.

We develop Technology Solutions.

300 000 satisfied users

Mobile Applications

We develop scalable interfaces and a robust user experience, which enables you to optimize your ROI.

Web Applications

We build, manage and promote websites for businesses. High-quality web presence guaranteed.

E-commerce

We create outstanding online shops for startup to large-scale businesses. Start cashing in.

START YOUR PROJECT

Meet your new best friends, our gurus.

We a team of over 14 specialists in a wide range of platforms and technologies, whatever your requirements are. We guarantee delivery within your time deadlines and budget.



CEO



Lead Designer



Co-founder



Project Manager

[LEARN MORE ABOUT US HERE](#)

foxysunstudio.com – Get in Touch



Home

Who we are

Services

Our work

Get in touch

Blog



We'd love To Meet You In Person Or Via The Web!

Corporate offices in San Francisco and Los Angeles



97. On or about June 15, 2023, [REDACTED], Google

provided records related to the domain **foxysun.com**. A review of the Google Pay contact

information identified the contact email address was [REDACTED]@foxysun.com, telephone number [REDACTED]-[REDACTED], and the name [REDACTED], Miami Beach, FL 33139. The billing address was listed as [REDACTED] San Francisco, CA 94108 and [REDACTED] Turkey. A review of the Google Pay billing records identified multiple payment contacts. One contact was [REDACTED] using the [REDACTED] email address [REDACTED]@gmail.com. The following names were listed along with credit cards used for payment: [REDACTED] (Great Britain), [REDACTED] (United States), and [REDACTED].

98. On or about June 15, 2023, [REDACTED] Google provided records related to [REDACTED]@gmail.com. The email address in the name of [REDACTED], created on June 29, 2007, and had the recovery email address [REDACTED]0@gmail.com. The account used Google Pay and the [REDACTED] account [REDACTED]@gmail.com.

99. On or about June 29, 2023, [REDACTED] provided records related to [REDACTED]@gmail.com. The name on the account was [REDACTED] and was registered on November 3, 2017. There were two bank accounts on the account, one at [REDACTED], the other was a Chinese bank, Agricultural Dev Bank of China. Multiple payments were received from [REDACTED], a freelancer website, in the name of [REDACTED]. I know from my training and experience that North Korean IT workers frequently use China-based banks to spend their freelancer revenue or else transmit it to North Korea.

100. The name [REDACTED] appears on the **foxysun.com** website as a “manager” but the names [REDACTED] and [REDACTED] do not. Additionally, there were multiple addresses associated to the Foxy Sun accounts. Additionally, the same picture was used for [REDACTED] between the **foxysunstudios.com** and **foxysunstudio.com** websites. This further demonstrates the fraudulent activities of the domains. The use of multiple names, addresses, and payment methods across the

accounts associated with Foxy Sun Studios are indicative of fraudulent activity and is a tactic used by North Korean IT workers to mask their true identity.

101. Based on the foregoing, there is probable cause to believe that criminal proceeds from the aforementioned fraud scheme and conspiracy to violate IEEPA were used to purchase and host these domains, and that these domains were involved in a money laundering offense (i.e. criminal proceeds were used to host the domain in a financial transaction with the intent to promote the carrying on of the fraud scheme and the conspiracy to violate IEEPA).

E. **babyboxtech.com**

102. On or about October 27, 2022, [REDACTED] Microsoft provided records for the [REDACTED] accounts [REDACTED] both used by [REDACTED] [REDACTED] Company President of Yanbian Silverstar. On or about January 7, 2022, [REDACTED] [REDACTED] shared the email [REDACTED] @126.com and its password to himself.

103. On or about November 23, 2022, [REDACTED] [REDACTED] provided records for the [REDACTED] with the email account [REDACTED] @126.com. The account used the name [REDACTED] and provided an address in Yanji, China. A review of the “Global Payment Services” questionnaire identified the following:

Question	Answer
What services do you provide?	Mobile apps and web
What is your connection to the web page or URL provided?	finance manager
Briefly describe your business. For example, who are your customers? What services or products do you provide?	Web & Mobile App Development support
Provide the URL to your business's website or your online store's web page.	https://babyboxtech.com/

The above answers were provided by the customer on December 18, 2021, and included the URL **babyboxtech.com**. The user self-identified as the finance manager.

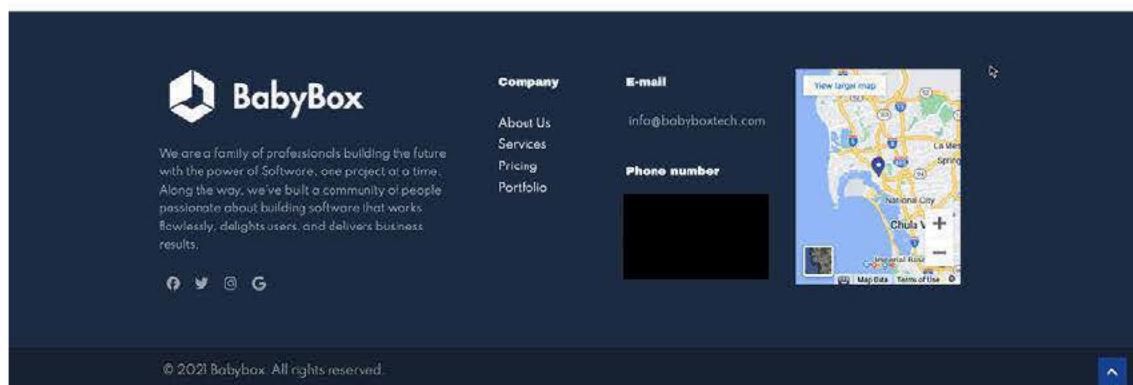
104. On May 12, 2023, I reviewed the domain **babyboxtech.com** identified the website was used by Babybox Technology as a portfolio website to advertise their IT development services and stated they were a “certified software development studio”. The website listed the following contact information, email: *info@babyboxtech.com*, phone number [REDACTED], CN [REDACTED].

babyboxtech.com – Home Page



OUR SERVICES

babyboxtech.com – Contact Us



105. On or about March 17, 2022, [REDACTED] Microsoft provided records for the [REDACTED] account [REDACTED] used by [REDACTED] a North Korean IT worker for Yanbian Silverstar. On or about March 18, 2021, [REDACTED] a North Korean IT worker for Yanbian Silverstar and the user of [REDACTED] sent a screenshot of an account recovery for an Apple ID and it requested the trusted phone ending in 61. [REDACTED] then sent [REDACTED] the number “[REDACTED]” and subsequently sent two six digit codes to [REDACTED]. Based on the codes the FBI believes those were verification codes provided to [REDACTED] at telephone number [REDACTED] and were used by [REDACTED] to access an Apple account associated to the same telephone number.

106. On or about January 24, 2023, [REDACTED] [REDACTED] provided records for the account associated to [REDACTED]. with the email addresses [REDACTED]@hotmail.com and [REDACTED]@gmail.com. On April 26, 2023, [REDACTED] was interviewed and confirmed they had allowed an individual, whom they thought resided in the United States, to use their [REDACTED] account for in their freelancer business as well as remotely access a laptop on their network. At the unknown individual’s direction, [REDACTED] created a company called “Bluesky IT” to manage the freelancer payments and activity associated with the assisting the unknown individual. A review of the [REDACTED] transactions for [REDACTED] account identified a payment to NameCheap on December 29, 2021, for the domain renewal and SSL renewal for **babyboxtech.com**.

107. The email address [REDACTED]@gmail.com was identified as being used and controlled by [REDACTED] a North Korean IT worker for Yanbian Silverstar, who also uses variations of the name “bluesky” in their communication accounts.

108. On or about June 5, 2023, [REDACTED] NameCheap

provided records for the domain **babyboxtech.com**. The domain's Whois information was provided as [REDACTED], Babybox, Team Leader (Title). [REDACTED] Atlanta, GA, telephone [REDACTED]
[REDACTED] email address [REDACTED] @gmail.com. On or about August 26, 2022, the email address for the account was changed to [REDACTED] @gmail.com. A review of the payments identified three [REDACTED] payments using the email address identified above, [REDACTED] @hotmail.com, and one payment from [REDACTED] @gmail.com.

109. On June 15, 2023, [REDACTED] Google provided records for telephone number [REDACTED]. The name on the account was [REDACTED], email address [REDACTED] @gmail.com, and was registered on June 11, 2020.

110. On or about January 24, 2023, [REDACTED] [REDACTED] records for account [REDACTED] @126.com, the email address used to pay the FBI's OCE to purchase the laptop remotely accessed by [REDACTED] the email address [REDACTED] @gmail.com was listed as another verified and active email address on the same account.

111. The email address [REDACTED] @gmail.com has been associated to [REDACTED] [REDACTED] who received the two factor verification code discussed above. Additionally, Microsoft records in response to a search warrant issued by the EDMO on July 19, 2022, for an account controlled and used by [REDACTED] a group leader of Yanbian Silverstar, identified a [REDACTED] on or about October 11, 2020, between [REDACTED] where [REDACTED] the email address [REDACTED] @gmail.com was a new email. [REDACTED] subsequently sent a link to [REDACTED] to confirm an email address. A review of [REDACTED] for the [REDACTED] @126.com

account confirmed the email address [REDACTED]@gmail.com was added on October 11, 2020. The FBI believes [REDACTED] had access to the [REDACTED]@gmail.com and received a link to verify the account from [REDACTED] and provided the link to [REDACTED] to verify the email address on the [REDACTED]@126.com [REDACTED] account.

112. The above shows the domain, **babyboxtech.com**, is controlled by North Korean IT workers working for Yanbian Silverstar.

113. Based on the foregoing, there is probable cause to believe that criminal proceeds from the aforementioned fraud scheme and conspiracy to violate IEEPA were used to purchase and host this domain, and that this domain was involved in a money laundering offense (i.e. criminal proceeds were used to host the domain in a financial transaction with the intent to promote the carrying on of the fraud scheme and the conspiracy to violate IEEPA). In addition, there is probable cause to believe that the domain was used or intended to be used to commit the offense of identity theft.

F. **ktsolution.tech**

114. On or about February 25, 2022, in response to a search warrant, Google provided records related to the email account [REDACTED]@gmail.com, used by North Korean IT worker [REDACTED] who works for Yanbian Silverstar. A review of account identified the user searched for cities in North Korea and review North Korean state-controlled news sites. Additionally, the email account received an email regarding the creation of a Google Workspace for the domain **ktsolution.tech**.

115. On or about July 24, 2023, [REDACTED] GoDaddy.com provided records related to **ktsolution.tech**. The domain was registered on May 5, 2021, and

expires on May 5, 2024. The user for the account was listed as [REDACTED] with a Tennessee address, telephone number [REDACTED] email address [REDACTED]@gmail.com. The name [REDACTED] appeared in a spreadsheet containing stolen PII (name, SSN, DOB, and addresses) used by [REDACTED] [REDACTED] and North Korean IT workers to create accounts to further their ability to fraudulently obtain freelancer jobs and open financial accounts.

116. On July 25, 2023, I reviewed open source information for the domain **ktsolution.tech** and the domain did not have a website.

117. Based on the foregoing, there is probable cause to believe that the domain was used or intended to be used to commit the offense of identity theft.

THE SUBJECT DOMAIN NAMES

118. As described above, the **Subject Domain Names** were used by Yanbian Silverstar actors to facilitate the hiring of North Korean IT workers including the use of stolen PII, including an individual's identity who is located in the Eastern District of Missouri and elsewhere, in order to evade detection from law enforcement throughout the United States.

119. In addition, there is probable cause to believe that criminal proceeds from the aforementioned fraud scheme and conspiracy to violate IEEPA were used to purchase and host the **Subject Domain Names**, and that the **Subject Domain Names** were involved in money laundering offenses (i.e. criminal proceeds were used to host the **Subject Domain Names** in financial transactions with the intent to promote the carrying on of the fraud scheme and the conspiracy to violate IEEPA). In addition, there is probable cause to believe that several of the **Subject Domain Names** were used or intended to be used to commit the offense of identity theft.

120. The **Subject Domain Names** were or could be utilized for portfolio websites and to recruit other developers and companies to use their freelancer services for web, application, and mobile development projects.

121. A search of publicly available WHOIS domain name registration records revealed that the **Subject Domain Names** were registered by one of the following registrars:

- a. Bluehost, Inc., a company headquartered in Jacksonville, FL,
- b. NameCheap, Inc., a company headquartered in Phoenix, AZ,
- c. Tucows Domains Inc., a company headquartered in Canada, and
- d. GoDaddy.com, LLC, a company headquartered in Tempe, AZ.

122. The use of registrars outside of the United States requires the seizure of the **Subject Domain Names** from the top-level registry, not the individual registrars.

123. The top-level domain for all the .com domains in the **Subject Domain Names** is Verisign, Inc. (hereinafter “Verisign”). Verisign currently manages all “.com” domains.

124. The remaining domains that are not “.com” domains in the **Subject Domain Names** were registered at GoDaddy.com, LLC. Those top-level domains (.cloud, .info, .asia, .services, and .tech) are managed by various organizations, some of whom are not located in the United States. The following is the listing of the other top-level registries:

- a. .cloud – Aruba S.p.A., Italy
- b. .info – Identity Digital, Inc., Bellevue, WA
- c. .asia – DotAsia Organisation Ltd., Hong Kong
 - a. .services – Identity Digital, Inc., Bellevue, WA
 - b. .tech – Radix FZC DMCC, Dubai, UAE

125. Since there are multiple different top-level domains, the **Subject Domain Names** seizure for those top-level domains will be done at the registrar, GoDaddy.com, LLC.

SEIZURE PROCEDURE

126. As detailed in Attachments A-1 and A-2, upon execution of the seizure warrant, the registry for the “.com” top-level domain, Verisign Inc., and the registrar for the domains “.cloud”, “.info”, “.asia”, “.services”, and “.tech”, GoDaddy.com, LLC, 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.

127. In addition, upon seizure of the **Subject Domain Names** by the FBI, Verisign and GoDaddy.com 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

128. Based on the information contained in this affidavit, I submit that there is probable cause to believe that criminal proceeds from the fraud scheme and conspiracy to violate IEEPA were used to purchase and retain the **Subject Domain Names**; that the **Subject Domain Names** were involved in money laundering offenses; and/or were used in and/or intended to be used in facilitating and/or committing identity theft. Accordingly, the **Subject Domain Names** are subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (c),

982(a)(1) and (2), and 1028(b)(5); and 28 U.S.C. § 2461, and, and I respectfully request that the Court issue a seizure warrant for the **Subject Domain Names**.

129. 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 it 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.

130. Because the warrant will be served on Verisign Inc. and GoDaddy.com, LLC, which controls the **Subject Domain Names**, at a time convenient to it, the registry 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.

131. 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 October 5, 2023.

[REDACTED]

HONORABLE RODNEY H. HOLMES
United States Magistrate Court Judge

ATTACHMENT A-1

SUBJECT DOMAIN NAMES	
1	silverstarchina.com
2	edenprogram.com
3	xinlusoft.com
4	foxysun.com
5	foxysunstudio.com
6	foxysunstudios.com
7	cloudbluefox.com
8	cloudfoxhub.com
9	mycloudfox.com
10	thefoxcloud.com
11	thefoxesgroup.com
12	babyboxtech.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 company or portfolio website to obtain remote IT freelancer jobs using fraudulent identities.

For additional information on North Korea's use of remote IT workers review the advisory:

“Guidance on the Democratic People’s Republic of Korea Information Technology Workers”

<https://ofac.treasury.gov/sanctions-programs-and-country-information/north-korea-sanctions>

ATTACHMENT A-2

SUBJECT DOMAIN NAMES	
1	cloudfox.cloud
2	danielliu.info
3	jinyang.asia
4	jinyang.services
5	ktsolution.tech

With respect to domains listed (“SUBJECT DOMAIN NAMES”), GoDaddy.com, LLC, 2155 E. GoDaddy Way, Tempe AZ 85284, who is the domain registrar 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 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 company or portfolio website to obtain remote IT freelancer jobs using fraudulent identities.

For additional information on North Korea's use of remote IT workers review the advisory:

"Guidance on the Democratic People's Republic of Korea Information Technology Workers"

<https://ofac.treasury.gov/sanctions-programs-and-country-information/north-korea-sanctions>