



U.S. Department of JUSTICE

The Department of Justice is posting this court document as a courtesy to the public. An official copy of this court document can be obtained (irrespective of any markings that may indicate that the document was filed under seal or otherwise marked as not available for public dissemination) on the Public Access to Court Electronic Records website at <https://pacer.uscourts.gov>. In some cases, the Department may have edited the document to redact personally identifiable information (PII) such as addresses, phone numbers, bank account numbers, or similar information, and to make the document accessible under Section 508 of the Rehabilitation Act of 1973, which requires federal agencies to make electronic information accessible to people with disabilities.

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

FILED

10/6/2026

IN THE MATTER OF THE SEIZURE OF
INTERNET DOMAIN NAMES:

C0CC.CC
98AIBLOG.COM
98AICAI.COM
98AICODE.COM
OUTLOOK3650.COM
YOUTUBECARD.COM
LINKEDINNS.NET

Magistrate No. 26-1564
[UNDER SEAL]

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

**AFFIDAVIT BY TELEPHONIC OR OTHER RELIABLE ELECTRONIC MEANS
IN SUPPORT OF AN APPLICATION FOR SEIZURE WARRANTS**

I, Special Agent Adam James, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for seizure warrants for the property described in the Attachments, specifically, the domain names **c0cc.cc**, **98aiblog.com**, **98aica.com**, **98aicode.com**, **outlook3650.com**, **youtubecard.com**, and **linkedinns.net** (the "TARGET DOMAIN NAMES").

2. I am a Special Agent with the FBI. I am currently assigned to the San Diego Cyber National Security squad. In this capacity, I investigate possible violations of federal criminal law, including those involving computer crimes, and am familiar with the means and methods used to commit these offenses.

3. The facts set forth in this affidavit are based on my personal observations, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals (including other law enforcement personnel), and information gained through my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this

matter. I have not, however, excluded any information known to me that would undermine a determination of probable cause.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that the TARGET DOMAIN NAMES are property used or intended to be used to commit or to facilitate the commission of violations of 18 U.S.C. § 1030(a)(2)(C) (unauthorized access to a protected computer to obtain information) and 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage to a protected computer without authorization), as well as conspiracy to commit these same offenses, in violation of 18 U.S.C. § 371. Thus, I believe they are subject to seizure and criminal forfeiture pursuant to Rule 41(b), 18 U.S.C. § 1030(i) and 21 U.S.C. § 853(f).

5. Additionally, there is probable cause to believe that the TARGET DOMAIN NAMES are property involved in a money laundering conspiracy (18 U.S.C. § 1956(h)) to transfer money from outside the United States to a place within the United States, with the intent to promote the carrying on of a specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(2)(A), specifically to damage protected computers (a violation of 18 U.S.C. § 1030(a)(5)(A)) and obtain information from them without authorization (18 U.S.C. § 1030(a)(2)(C)). Thus, I believe they are subject to seizure and civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1)(C), and seizure and criminal forfeiture pursuant to 18 U.S.C. §§ 982(a)(1) and 982(b)(1).

6. Domain Registrar 1 is the registrar that controls **98aiblog.com**, **98aical.com**, **98aicode.com**, **outlook3650.com**, **youtubecard.com**, and **linkedinn.net**. Domain Registrar 2 is the registrar that controls **c0cc.cc**. Both Domain Registrar 1 and Domain Registrar 2 are headquartered in Phoenix, Arizona.

7. This application is for a seizure warrant that can be served on Verisign Inc. (“Verisign”) which is the domain registry for .cc, .net, and .com, and is headquartered at 12061 Bluemont Way, Reston, Virginia.

STATUTORY AUTHORITY

8. 18 U.S.C. §1030(a)(2)(C) makes it a crime, in relevant part, to intentionally access a computer without authorization and thereby obtain information from any protected computer.

9. 18 U.S.C. §1030(a)(5)(A) makes it a crime to knowingly cause the transmission of a program, information, code, or command, and, as a result of that conduct, intentionally cause damage without authorization, to a protected computer.

10. 18 U.S.C. § 371 provides that “[i]f two or more persons conspire either to commit any offense against the United States . . . and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.”

11. 18 U.S.C. § 1956(a)(2)(A) (international promotional money laundering) prohibits, in relevant part, the transportation, transmission, or transfer of funds or monetary instruments from or through a place *outside* the United States to a place *within* the United States, with the intent to promote the carrying on of specified unlawful activity. Under 18 U.S.C. § 1956(c)(7)(D), specified unlawful activity includes violations of 18 U.S.C. § 1030. Under 18 U.S.C. § 1956(h), any person who “conspires to commit any offense defined in [§ 1956]” shall also be subject to criminal prosecution.

12. Pursuant to 18 U.S.C. §§ 1030(i) and (j), a court, in imposing a sentence on any person convicted under 18 U.S.C. § 1030, shall order the defendant to forfeit any interest in any personal property that was used or intended to be used to commit or to facilitate the commission

of the violation of the statute.

13. 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 (Money Laundering) is subject to civil forfeiture.

14. Pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in a violation of Title 18, United States Code, Section 1956 (Money Laundering) is subject to criminal forfeiture.

15. This application seeks a seizure warrant under both civil and criminal authority, because the property to be seized could easily be placed beyond legal process if not seized by warrant, as domains are fungible and can be destroyed quickly by authorized users.

16. 18 U.S.C. § 981(b) states that property subject to forfeiture under Section 981 may be seized via 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. 18 U.S.C. §§ 982(b)(1) and 1030(i)(2) incorporate the procedures in 21 U.S.C. § 853 (other than subsection (d)) for all stages of a criminal forfeiture proceeding. Section 853 permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture. Seizures are appropriate from this district, because at least one of the predicate acts giving rise to forfeiture occurred in the Western District of Pennsylvania, as described below.

BACKGROUND ON DOMAIN NAMES AND MALWARE

17. I use the following terms in this affidavit:

a. IP address: An IP address is a unique numeric address used by devices on the internet. Every device attached to the internet must be assigned a public IP address so that

internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address – it enables devices connected to the internet to properly route traffic to each other.

b. Domain name: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., “justice.gov”). Domain names are composed of one or more parts, separated by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the “top-level domain” (e.g., “.com” or “.gov”). To the left of the top-level domain is the “second-level domain,” which is often thought of as the “name” of the domain. The second-level domain may be preceded by a “third-level domain,” or “subdomain,” which often provides additional information about various functions of a server or delimits areas under the same domain.

c. Domain name system: The domain name system (“DNS”) is the way that internet domain names are translated into IP addresses. The DNS system functions like a phonebook for the internet, allowing users to find websites and other resources by their domain names while translating them into IP addresses that their computers need to locate them.

d. Registrar: A registrar is a company that sells domain names to the public. For example, the registrar for the domain **98aiblog.com** is Domain Registrar 1.

e. Registry: A registry is an organization that manages top-level domains. For example, the registry for the “.com” top-level domain is VeriSign.

f. Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Malware has been developed for many different types of internet-connected devices, including computers, routers, IP cameras, DVRs, and NAS devices.

g. Command and control server (C2): A server used by cyber threat actors to launch and control cyber-attacks. Cyber threat actors use C2 servers to, for example, distribute malicious programs, command their malware, and receive stolen data.

h. Web vulnerability scanner: A web vulnerability scanner is an automated security tool that inspects websites for security flaws, code errors, and misconfigurations. It tests the website by sending specific inputs and analyzing the response to find vulnerabilities that an attack could use to exploit the website.

i. Reverse Proxy: A reverse proxy is an intermediary server or set of servers that receives incoming requests from clients on the internet and forwards the requests to the appropriate web server. A reverse proxy can provide enhanced security by hiding from clients or other remote users the real IP address of web servers.

BACKGROUND ON THE BOTNET MALWARE

18. The FBI is investigating a botnet¹ that used a variant of Mirai malware, a type of malware that targets internet-of-things computer devices and gives unauthorized users control over them.² This variant of Mirai malware links infected devices with other similarly infected devices to form a network of infected devices, also known as a “botnet.” Infected devices in a botnet,

¹ A botnet is a network of internet-connected devices infected with malware and controlled remotely by cyber threat actors to conduct a variety of malicious cyber activities.

² The internet of things (“IoT”) describes physical computer devices having software and other technologies that connect them to the internet as a way of increasing their efficiency and functionality. Examples of IoT devices include small-office/home-office routers, internet protocol (“IP”) cameras, and digital video recorders. Certain botnets are designed to exploit specific vulnerabilities in IoT devices.

known as “bots,” are controlled by one or more command-and-control (“C2”) servers. This botnet was in use from at least on or about July 23, 2021, until on or about September 13, 2024.

19. Hackers can use a botnet to transmit malware, launch cyber-attacks, and obfuscate the hackers’ true IP address, identity, and physical location. For example, overseas hackers may access a U.S. victim’s network through a botnet’s U.S.-located bot. To the victim’s network, the malicious traffic appears to come from the IP address of the U.S.-located bot, when, in fact, the malicious traffic originated outside the United States.

20. In or around May 2024, the FBI analyzed samples of a specific variant of Mirai malware that one or more private sector entities uploaded to an online service that collects suspicious files. The FBI identified several domains used by C2 servers to receive and send communications to devices in the botnet, including subdomains of w8510.com. The FBI determined that the Mirai variant programmed bots to communicate with subdomains of w8510.com, and that virtual private servers (“VPSs”) acted as C2 servers to host those subdomains.

21. In or around July 2024, using open-source information, the FBI identified IP addresses of dozens of botnet C2 servers – including U.S.-based botnet C2 servers – that were hosting various subdomains of w8510.com. By analyzing the network traffic to and from these IP addresses, collected pursuant to a court order authorizing use of a pen register and trap and trace device (“PRTT”), the FBI confirmed that these botnet C2 servers were managing and controlling thousands of bots worldwide that had been infected with this variant of Mirai malware.

22. Multiple botnet C2 servers associated with the botnet were registered to an account at VPS Provider 1, a provider of VPSs headquartered in West Palm Beach, Florida whose identity is known to your affiant. The servers registered at VPS Provider 1 had a consistent naming

convention which included the Chinese term “kehu.” “Kehu” is a Romanization of the Chinese word 客户 that translates to “customer” or “client.” The servers registered with the VPS Provider 1 account also had different numbers after the name “kehu.” The subscriber used variations of the term “kehu1036” to name VPS Provider 1 servers associated with the w8510.com domain. Based on my training and experience, I believe this meant that “kehu1036” or “client 1036” was a customer number for the botnet-related servers.

23. The subscriber used this naming convention after sending funds from the People’s Republic of China (“PRC”) to the United States to lease the following botnet C2 servers from VPS Provider 1, identified by their IP addresses and name: 202.182.109.151 (named “kehu1036jp4”), 207.148.68.131 (named “kehu1036spgs1”), 139.180.137.219 (named “kehu1036spgs2”), 207.148.122.69 (named “kehu1036spgs3”), 45.77.231.209 (named “kehu1036uks1”), 78.141.238.97 (named “kehu1036uks2”), 149.248.51.22 (named “kehu1036cas1”), 108.61.177.81 (named “kehu1036frs1”), 65.20.97.251 (named “kehu1036ess1”), 149.28.137.29 (originally named “kehu1036spg3”) and 207.148.73.238 (named “149.28.137.29”).³ The FBI searched these botnet servers pursuant to warrants issued by the Honorable Kezia O. L. Taylor, *see* Magistrate Number 24-962, and the Honorable Patrica L. Dodge, *see* Magistrate Number 24-1228. All the servers contained evidence consistent with the botnet the FBI was investigating.

24. A search of the botnet C2 server assigned IP addresses 202.182.109.151 (named “kehu1036jp4”) revealed that it contained C2 software that controlled bots infected with the Mirai malware. This analysis also confirmed that this botnet C2 server was an “upstream management

³ The IP address 149.28.137.29 was associated with a server at VPS Provider 1. Between March 25, 2023, and June 19, 2023, the IP address 149.28.137.29 was named “kehu1036spg3.”

server” which sent commands to the other C2 servers controlling the infected devices making up the botnet. Specifically, the server assigned IP address 202.182.109.151 hosted an application named “Sparrow.” The hackers used the Sparrow application to manage and control the botnet. The Sparrow application used a database stored on the server that contained a table of information about each of the infected victim devices. As of approximately June 5, 2024, the database on the server assigned IP address 202.182.109.151 contained records of over 1.2 million infected devices, including over 385,000 unique U.S. victim devices. According to the database records, over 260,000 of these devices, including approximately 126,000 U.S. devices, were actively infected as of approximately June 5, 2024.

25. The U.S.-based devices infected with this variant of Mirai malware are “protected computers” within the meaning of 18 U.S.C. § 1030(e)(2)(B) because they are connected to the Internet and affect interstate communications. They have been “damaged” within the meaning of 18 U.S.C. § 1030(e)(8) because the installation of unauthorized malware has impaired the integrity of the devices. Each infection of a U.S.-based device is the unauthorized intrusion and damage of a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A).

26. The FBI investigated the geographic locations of the U.S.-based devices infected with this variant of Mirai malware and confirmed that there is probable cause to believe that violations of 18 U.S.C. §§ 1030(a)(2)(C) and (5)(A) have been committed in the Western District of Pennsylvania. Specifically, the FBI has identified two such victims devices located in the Western District of Pennsylvania.

27. On or about September 11, 2024, the FBI seized the domain name w8510.com pursuant to a warrant obtained in the Western District of Pennsylvania. Also, on or about September 11, 2024, pursuant to a warrant from the Western District of Pennsylvania, the FBI

logged into the botnet C2 servers leased by VPS Provider 1, changed the system settings to prevent the botnet administrators from accessing the botnet C2 servers and issuing commands, and issued a command to terminate the communication channel between the botnet's C2 servers and any infected devices, thus disrupting the botnet.

C0CC.CC, THE BOTNET AND THE MICROSCAN TOOL

28. The C2 server at IP address 202.182.109.151 (named "kehu1036jp4") contained multiple copies of the source code for the Sparrow application and a file containing a user guide for the Sparrow application. The first line of the user guide stated that "KRLab" would provide 10 real world nodes for testing. The Sparrow application's source code also used files that contained the name "KRLab." The FBI's investigation uncovered integritytech.com[.]cn. This website included the public facing website for KRLab – which was a sub-division of a Chinese hacking and cyber security firm named Integrity Technology Group ("Integrity Tech."). Certain U.S.-based private sector cyber security firms refer to Integrity Tech's hacking tools and activity (including hacking activity associated with the Mirai Botnet described above) using the Advanced Persistent Threat ("APT") name "Flax Typhoon." Integrity Tech has contracts with the PRC government.

29. The FBI's investigation and search of certain servers named with variations of "kehu1036" revealed that they controlled the botnet which was used to execute scans for vulnerable victim networks as commanded by a server assigned IP address 198.13.53.226. The server assigned IP address 198.13.53.226 hosted and operated a tool created by Flax Typhoon named "Microscan" that scanned victim networks for vulnerabilities. Search returns for Flax Typhoon servers executing Microscan scans revealed that they sometimes used Flax Typhoon's Mirai botnet to hide the origin of scans.

30. FBI open-source research on or about September 9, 2026, showed that the subdomain x.c0cc.cc (c0cc.cc being one of the TARGET DOMAINS) still hosted the Microscan tool that I originally found on 198.13.53.226 when I searched that IP address. Meaning anyone on the internet could go to the x.c0cc.cc domain and see the Microscan tool's login page. The login page for the Microscan tool found at x.c0cc.cc was exactly the same as the login page I found during the search of 198.13.53.226. Records provided by Cloudflare on or about July 13, 2025, and VPS Provider 1 on or about June 3, 2026, revealed that x.c0cc.cc received internet traffic destined for the IP address 198.13.53.226. Additionally, the Cloudflare records revealed that other subdomains of c0cc.cc resolved to servers leased by the same account that leased the server assigned IP address 198.13.53.226. I therefore believe that the c0cc.cc and all of its subdomains are controlled by the same actors.

31. Flax Typhoon actors conducted successful computer intrusions against multiple victim entities which had been scanned using the Microscan tool. One such victim ("VICTIM 1") was a university located in Hsinchu, Taiwan. Flax Typhoon actors scanned VICTIM 1's network with Microscan on or about March 21, 2023, and compromised it soon after. Another victim ("VICTIM 2") was a second university, located in Puli Township, Taiwan. Flax Typhoon actors scanned VICTIM 2's network with Microscan on or about August 7, 2022, and compromised it soon after.

32. Search returns for the server assigned IP address 198.13.53.226 revealed that between on or about April 26, 2022, and on or about December 29, 2022, Flax Typhoon actors also used the Microscan tool to scan for vulnerabilities on the networks of a U.S. power company based in South Carolina, a multi-national Non-Governmental Organization, Japanese and Polish airports, and at least two Taiwanese critical infrastructure companies in the natural gas and power

sectors.

33. In summary, based on my training and experience, I believe probable cause exists to conclude the domain **c0cc.cc** was used to access a proprietary web vulnerability scanning tool owned by Flax Typhoon and that tool was used in furtherance of violations of 18 U.S.C. §§ 1030(a)(2)(C) and (5)(A) because the vulnerability scanning tool was linked to a botnet and used to steal data from or damage devices owned by VICTIM 1 and VICTIM 2.

THE VICTIM 1 AND VICTIM 2 INTRUSIONS AND THE REMAINING TARGET DOMAINS

34. Search returns for a server assigned IP address 108.61.181.104 and purchased by Flax Typhoon revealed that, as of no later than approximately August 12, 2024, Flax Typhoon actors successfully accessed VICTIM 1's network without authorization and installed SoftEther – a remote administration software. That software used a subdomain of **98aiblog.com**, one of the TARGET DOMAINS, to cause the VICTIM 1 server to connect to the IP address 108.61.181.104. Search returns further revealed that, on or about August 19, 2024, the SoftEther software used the same subdomain of **98aiblog.com** to cause a VICTIM 2 server to connect to IP address 108.61.181.104. According to Domain Registrar 1's records, on or about September 9, 2026, the domain **98aiblog.com** was registered to the same Domain Registrar 1 account (username asdown3389) which created it on March 13, 2024.

35. Search returns for a server assigned IP address 207.148.92.220 and purchased by Flax Typhoon revealed that, as of March 2026, it hosted a tool named FishHub. The FishHub tool found on 207.148.92.220 used the domains **98aical.com**, **98aicode.com**, **outlook3650.com**, **youtubecard.com**, and **linkedinns.net**, five of the TARGET DOMAINS, to facilitate computer intrusions. Based on my training and experience I believe the tool was named FishHub because it facilitated phishing activity.

36. Search returns for the server assigned IP address 207.148.92.220 included the source code for the FishHub tool. The FishHub tool source code contained code similar to the following:

```
DownloadFile('https://fym.[98aica.com, 98aicode.com, outlook3650.com,  
youtubecard.com, or linkedinns.net]/dshnmpmbxwylismvb/  
shnmpmbxwylismvb.txt', '%temp%\shnmpmbxwylismvb.vbe').
```

Based on my analysis of the FishHub tool and code, I believe that the FishHub tool downloaded this file to phishing victims, and the file then used these five domain names to download additional malicious programs and code to the victims' systems. Based on the FBI's analysis of the FishHub tool and code, these additional malicious programs and code were designed to: 1) create a file listing; 2) search for specific files; 3) compress documents; and then 4) exfiltrate the selected files to the server assigned IP address 207.148.92.220. In other words, the domains **98aica.com**, **98aicode.com**, **outlook3650.com**, **youtubecard.com**, and **linkedinns.net** functioned to facilitate the downloading and execution of a file on a victim's network, which would give Flax Typhoon actors remote access to a victim's networks. Flax Typhoon actors would use that access to exfiltrate selected files to the server assigned IP address 207.148.92.220.

37. Search returns for the server assigned IP address 207.148.92.220 revealed data and files from more than 20 different entities. Commands from the server assigned IP address 207.148.92.220 also showed that six of the targeted entities were Universities located in Taiwan. Because the FishHub tool was designed to exfiltrate files to this server, I believe based on my training and experience that Flax Typhoon actors stole the files using the FishHub tool.

38. The domains **98aica.com**, **98aicode.com**, **outlook3650.com**, **youtubecard.com**, and **linkedinns.net** were registered by two Domain Registrar 1 accounts. One Domain Registrar 1 account, username asdown3389 (described above), registered **98aica.com** and **98aicode.com**.

The other, username d527a8, registered **outlook3650.com**, **youtubecard.com**, and **linkedinns.net**. Both Domain Registrar 1 accounts were repeatedly accessed by the IP address 66.42.60.242 at approximately the same time. On or about February 10, 2026, the IP address 66.42.60.242 was used to access both Domain Registrar 1 accounts and renew the five domains (**98aica.com**, **98aicode.com**, **outlook3650.com**, **youtubecard.com**, and **linkedinns.net**) with funds from AliPay – a PRC-based financial services provider. Additionally, the same account with VPS Provider 1 leased servers with the assigned IP addresses 66.42.60.242 and 108.61.181.104.⁴ I, therefore, believe that all five domains are controlled by the same actors.

39. For these reasons, I believe that there is probable cause to conclude that the domains are property used to operate a computer intrusion tool in order to steal information from and damage protected computers – in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (a)(5)(A).

INTERNATIONAL PROMOTIONAL MONEY LAUNDERING

40. According to Domain Registrar 1's records, the domains **98aiblog.com**, **98aica.com**, and **98aicode.com** – three of the TARGET DOMAIN NAMES – and two additional domains, 98aivip.com and 98aiday.com, were purchased on or about March 13, 2024, by the Domain Registrar 1 account with the username asdown3389, using IP address 141.11.87.76. According to Domain Registrar 1's records, a \$139.50 payment was made for these five domain names on or about March 13, 2024, using Financial Services Provider 1. This Domain Registrar 1 account's registration address is "712 Tin Ha Road, Hung Shui Kiu, Yuen Long, Hong Kong

⁴ The FBI learned about Customer Account 2 because a Threat Intelligence Team ("IT-1") of a significant software company identified other IPs owned by Customer Account 2 as operating on behalf of Flax Typhoon. The FBI later confirmed IT-1's assessment by searching the IP addresses IT-1 originally identified.

999077,” and, as described above, was repeatedly accessed using the IP address 66.42.60.242.

41. According to Financial Services Provider 1’s records, the Financial Services Provider 1 account used to pay for the five domains is registered to Lin Kunzhong (林坤仲), who provided a billing address and telephone number in Hong Kong. According to Financial Services Provider 1’s records, the funds for the March 13, 2024, payment to Domain Registrar 1 were provided by a Hong Kong credit card. Also, according to Financial Services Provider 1’s records, this customer used IP address 141.11.87.76 to send funds to Domain Registrar 1 on or about March 13, 2024; as noted above, this same IP address was used to register the domains **98aiblog.com**, **98aicai.com**, **98aicode.com**, **98aivip.com**, and **98aiday.com** at Domain Registrar 1 on or about March 13, 2024. IP address 141.11.87.76 geolocates to Taipei, Taiwan, further supporting this customer’s location and the payment’s origin to be outside of the United States.

42. The domains **outlook3650.com**, **youtubecard.com**, and **linkedinns.net** were originally registered with a second Domain Registrar 1 account (username d527a8) on or about February 18, 2025. The registration address for this account is: “130 Yee Kuk Street, Cheung Sha Wan, Sham Shui Po District, Hong Kong, 85014.”

43. Around February 2026, the Domain Registrar 1 registration for **98aiblog.com**, **98aicai.com**, **98aicode.com**, **outlook3650.com**, **youtubecard.com**, and **linkedinns.net** was renewed using funds from a PRC-based account at AliPay and IP address 66.42.60.242.

44. Additionally, records from Domain Registrar 2 revealed that the domain **c0cc.cc** was first registered on or about November 7, 2018, and renewed on or about August 31, 2024. Both the purchase and renewal were made using Chinese Yuan and an Alipay account with the name: “Yuxin Ling;” and the address: “Beijing, 11 1000000000 CN.”

45. Based on these records and my training and experience, I have probable cause to believe the funds used to purchase and/or renew the TARGET DOMAIN NAMES originated from outside of the United States and were transferred into the United States with the intent to promote the violations of 18 U.S.C. § 1030, in violation of 18 U.S.C. § 1956(a)(2).

CONCLUSION AND SEIZURE PROCEDURE

46. As described above, the TARGET DOMAIN NAMES are being used to host, manage, and operate tools used in computer intrusion activities and are being used to commit violations of 18 U.S.C. §§ 1030(a)(2)(C) and (5)(A). Based on my training and experience, I have probable cause to believe the TARGET DOMAIN NAMES are therefore subject to seizure and criminal forfeiture pursuant to Rule 41(b), 18 U.S.C. § 1030(i) and 21 U.S.C. § 853(f). In addition, I have probable cause to believe that the TARGET DOMAIN NAMES were purchased by moving funds originated outside of the United States into and through the United States to promote a specified unlawful activity in violation of 18 U.S.C. § 1956(a)(2). Based on my training and experience, I have probable cause to believe the TARGET DOMAIN NAMES are therefore subject to seizure and civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1)(C), and seizure and criminal forfeiture pursuant to 18 U.S.C. §§ 982(a)(1) and 982(b)(1). Accordingly, I respectfully request that the Court issue seizure warrants for the TARGET DOMAIN NAMES.

47. As detailed in the Attachments, upon execution of the seizure warrants, the registrar for each of the TARGET DOMAIN NAMES shall be directed to restrain and lock the TARGET DOMAIN NAMES, pending transfer to the United States upon completion of forfeiture proceedings to ensure that changes to the TARGET DOMAIN NAMES cannot be made without prior consultation with the FBI or DOJ.

48. In addition, upon seizure of the TARGET DOMAIN NAMES by the FBI, the registrar and/or the registry for each of the TARGET DOMAIN NAMES will be directed to associate the TARGET DOMAIN NAMES to new servers as designated by the FBI.

49. Because the warrants are directed to the registrar and/or the registry for each of the TARGET DOMAIN NAMES, which will subsequently transfer control of the TARGET DOMAIN NAMES to the government, there exists reasonable cause to permit the execution of the requested warrants at any time in the day or night.

50. Finally, it is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrants. Your Affiant believes that sealing this document is necessary because the items and information to be seized are relevant to an ongoing criminal investigation that is neither public nor known to all the targets of the investigation..

51. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates or otherwise seriously jeopardize the investigation.

The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

s/Adam James

Adam James

Special Agent

Federal Bureau of Investigation

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 6th day of October, 2026.

**This matter shall remain under seal until further
order of the Court.**



HONORABLE MAUREEN P. KELLY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

With respect to the domain names **c0cc.cc, 98aiblog.com, 98aical.com, 98aicode.com, outlook3650.com, youtubecard.com, and linkedinns.net** subdomains (collectively in this Attachment as “**TARGET DOMAIN NAMES**”), Verisign, Inc. (Verisign), headquartered at 12061 Bluemont Way, Reston, VA 20190, which is the registry for the domain name, shall take the following actions to effectuate the seizure of the **TARGET DOMAIN NAMES**:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation (FBI), by associating the domain names **TARGET DOMAIN NAMES** to the following authoritative name-server(s):
 - a. ns1.fbi.seized.gov
 - b. ns2.fbi.seized.gov
 - c. Any new authoritative name servers or IP addresses to be designated by a law enforcement agent in writing, including e-mail, to Verisign.
2. Prevent any further modification to, or transfer of, the domain name **TARGET DOMAIN NAMES** pending transfer of all right, title, and interest in the domain name to the United States upon completion of forfeiture proceedings, to ensure that changes to the domain name **TARGET 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.
5. The Government will display a notice on the website to which **TARGET DOMAIN NAMES** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This website has been seized. This effort addresses cyber threat actors known as Integrity Technology Group (永信至诚科技集团股份有限公司). This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant pursuant to violations of 1030(a)(5)(A) (damage to a protected computer), issued by the United States District Court for the Western District of Pennsylvania as part of law enforcement operation and action by: The United States Attorney's Office for the Western District of Pennsylvania and the Federal Bureau of Investigation. For more information, visit www.justice.gov. Report cybercrime at www.ic3.gov.