U.S. Department of
JUSTICE

AFFIDAVIT IN SUPPORT OF

APPLICATIONS FOR SEIZURE WARRANTS

I, Special Agent [redacted], being first duly sworn, hereby depose and state:

INTRODUCTION

1. I make this affidavit in support of applications for seizure warrants for the property described in Attachments A-1, A-2, and A-3, specifically, the domain names:

   a. **qtproxy.xyz,**

   b. **qt-proxy.org**, and

   c. **qt-team.com**

collectively, the **Target Domain Names**.

2. 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 involved in violations of 18 U.S.C. §§ 1956(h) (conspiracy to launder money), 1956(a)(2)(A) (international promotional money laundering), and 1030(a)(5)(A) (damage to a protected computer).

3. In particular, the investigation has revealed that the **Target Domain Names** have been used to operate a scanning and exploit platform named QScan and an obfuscation network named QTRouter. These **Target Domain Names** were paid for using international monetary transactions into the United States.

4. Because the **Target Domain Names** are properties involved in a scheme to violate U.S. money laundering laws, they are subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1)(C).

5. The **Target Domain Names** were registered through Namecheap Inc. (Namecheap) and NameSilo LLC (NameSilo), the recipients of the international monetary transactions into the United States. Namecheap is headquartered at 4600 East Washington Street, Suite 305, Phoenix, AZ 85034. NameSilo is headquartered at 1300 E Missouri Ave, Suite A-110, Phoenix, AZ 85014.

6. Namecheap and NameSilo are domain registrars, which reserve and register domain names on behalf of their customers with the various domain registries. Seizure warrants will be served on the domain registries (.xyz, .org, and .com), which are operated by XYZ.COM LLC. (XYZ.COM), Public Interest Registry, and Verisign, Inc. (Verisign), respectively. XYZ.COM is headquartered at 2121 E. Tropicana Ave, Suite 2, Las Vegas, NV 89119. Public Interest Registry is headquartered at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, VA 20190. Verisign is headquartered at 12061 Bluemont Way, Reston, VA 20190.

STATUTORY AUTHORITY

7. 18 U.S.C. § 981(a)(1)(A) provides that any property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 (money laundering) or conspiracy to commit such an offense, or property traceable to such property, is subject to civil forfeiture. Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed.

8. 18 U.S.C. § 982(a)(1) provides that any property involved in a violation of 18 U.S.C. § 1956 or conspiracy to commit such an offense, or property traceable to such property, is subject to criminal forfeiture. Section 982(b)(1) authorizes the issuance of a criminal seizure warrant under 21 U.S.C. § 853(f), which provides that a criminal seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued, and that a court shall issue a criminal seizure warrant if it determines that the property would be subject to forfeiture in the event of a conviction, and that a restraining order would be inadequate to assure the availability of the property for forfeiture. Here, neither a restraining order nor an injunction is sufficient to guarantee the availability of the **Target Domain Names** for forfeiture, nor prevent criminals from continuing to access them and using them to commit additional crimes.

9. 18 U.S.C. § 981(h) provides that, in the case of property of a defendant charged with a criminal violation that is the basis for forfeiture of the property, venue for civil forfeiture lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought.

10. 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 § 1956(c)(7)(D), specified unlawful activity includes violations of § 1030(a)(5)(A) (damage to a protected computer). Under § 1956(h), any person who "conspires to commit any offense defined in [§ 1956]" shall also be subject to criminal prosecution.

EXPERIENCE & TRAINING

11. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since January 2010. After my new agent training my entire career has been spent on San Diego's Cyber National Security squad. I have received training in conducting cyber-based investigations, as well as training covering, among other things, hacker techniques, incident responses, computer forensics, and cyber security. Prior to employment with the FBI, I worked 10 years in the Information Technology (IT) field with various job functions including Systems Administrator and Software Developer. I have a Bachelor of Science in Computer Science. This training and experience form the basis for opinions I express below.

BACKGROUND ON DOMAN NAMES

12. I use the following terms in this affidavit:

a. *Botnet*: A botnet is a network of internet-connected devices ("bots") infected with malicious software and controlled remotely by malicious cyber actors, without the knowledge or consent of the device owners.

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, or "labels," delimited 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. For example, in "www.justice.gov," the top-level domain is ".gov," the second-level domain is "justice," and the subdomain is "www," which indicates that the domain points to a web server.

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

d. *Internet Scanning*: A process used to identify devices, open ports, and vulnerabilities on devices on the Internet

e. *IoT Device*: An internet of things (IoT) device is any computing device accessible on the Internet. It can include home routers, security cameras, smart TV devices, smart appliances, etc.

f. *IP address*: An internet protocol address (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

g. *Obfuscation network*: A network of connected devices on the Internet deployed for the purpose of reducing the traceability of computer network exploitation activities.

h. *Zero-day exploit*: This term refers to a vulnerability in a computer or software's security that hackers can exploit. One of the defining features of a zero-day exploit is that only the hackers who found and/or use it know about the vulnerability and the means of exploiting it. Consequently, if the same zero-day exploit is used to attack different targets at or around the same time, that typically indicates that the same hacker or group of hackers are responsible for those attacks.

EVIDENCE ESTABLISHING PROBABLE CAUSE

Background

13. The FBI has been investigating a group of malicious cyber threat actors located in the People's Republic of China (PRC). They use the acronyms QTFY, QT, and QTCYBER for themselves and their tools, and will hereafter be referred to as "QTFY actors." They work for a private PRC company called Nanjing Xinjiuwei Network Technology Co (南京鑫玖维网络科技有限公司) (Nanjing Xinjiuwei). Payments from the PRC's Ministry of State Security (MSS) to Nanjing Xinjiuwei, for example, indicate that the company conducts malicious cyber activities on behalf of the PRC Government.

14. QTFY actors include former members of the PRC's People's Liberation Army (PLA), and they use their PLA relationships to obtain contracts and subcontracts supporting offensive cyber operations. Since at least 2018, QTFY computer infrastructure has been used to compromise critical infrastructure and other sensitive networks in the United States and worldwide. Targeted U.S. federal government networks include those of the National Aeronautics and Space Administration (NASA), Federal Reserve, Department of Energy (DOE), Department of Justice, Department of Health and Human Services (HHS), National Institutes of Health (NIH), and, in 2026, the Senate. Other targeted networks include those operated by hospitals, telecommunications providers, power companies, financial institutions, and defense contractors.

15. QTFY actors have developed products that include a vulnerability scanning and exploitation platform named "QScan," an obfuscation network named "QTRouter," and botnets of compromised IoT devices. Not only do QTFY actors use these products

themselves, but they also sell access to QScan and QTRouter to others. These products work in conjunction. QTFY actors and their customers can use QScan to automatically scan and exploit thousands of vulnerable IoT devices worldwide, which QTFY actors can then add as botnet nodes in the QTRouter obfuscation network. QTFY actors and their customers use QTRouter to obfuscate their identities. For example, by routing their malicious internet traffic through IoT devices (compromised by QScan) local to their victims, these Chinese hackers can blend in with legitimate users and remain undetected when scanning and attacking critical infrastructure and other targets.

16. In 2019, the FBI investigated QTFY's attempted computer intrusion at NASA. On or around August 10 and 12, 2019, cyber actors operating from IP address 104.168.166.42 attempted to exploit the Pulse Secure Virtual Private Network (VPN) vulnerability, identified as CVE-2019-11510, to gain unauthorized access to NASA's server.[1] A Pulse Secure VPN grants a legitimate user remote access to a protected network.

17. The Pulse Secure vulnerability, CVE-2019-11510, was a critical flaw in Pulse Secure appliances, which allowed malicious cyber actors to learn legitimate users' usernames and passwords, effectively granting malign actors unauthorized access to protected networks. Pulse Secure issued a patch for the vulnerability in April 2019.

18. Subscriber records for IP address 104.168.166.42 revealed that during August 2019 it was leased by an account registered to Lou Zhongrang of Changsha, China, and that email address qtfy100@gmail.com, email address jklpoi9966@gmail.com, and telephone number +86-16651613389 were associated with the account. Eighty-six is the country calling code for the PRC.

19. In November 2020 and January 2021, search warrants were obtained for Google accounts jklpoi9966@gmail.com, qtfy100@gmail.com, caiwenbai18@gmail.com,

---

[1] CVE stands for "Common Vulnerabilities and Exposures." A catalog of known vulnerabilities is maintained by the MITRE corporation and sponsored by the U.S. Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency (CISA). They bring awareness of known vulnerabilities to help network defenders prevent computer intrusions. Each known vulnerability is assigned a unique CVE number. Because NASA had applied a security patch to address this vulnerability prior to the attempted exploitation, the attempt was not successful.

dannelccc@gmail.com, and songjun2020.sm@gmail.com. The search warrant returns revealed that all the accounts were linked together. For example, jklpoi9966@gmail.com was a recovery email account for qtfy100@gmail.com, and jklpoi9966@gmail.com and dannelccc@gmail.com shared a recovery email account, 466197084@qq.com. The search returns also revealed that qtfy100@gmail.com, caiwenbai18@gmail.com, and songjun2020.sm@gmail.com shared Google tracking cookies, which indicate the same user logged into all three accounts.

20. Review of the email accounts showed the threat actors purchased a large amount of Internet infrastructure such as virtual private servers, IP addresses, and domain names. Infrastructure being obtained by the accounts was often reported being used for malicious purposes, such as Internet vulnerability scanning, exploit attempts, and hosting malware.

21. Because this affidavit is submitted for the limited purpose of obtaining a domain seizure warrant, only a select few of those abuse complaints are discussed in the subsequent paragraphs. The below paragraphs document four particular victims: Medical Center 1 of Ohio, Financial Group 1 of South Korea, Financial Group 2 of Michigan, and Insurance Agency 1 of Missouri. QTFY actors targeted all four victims using virtual private servers leased from Hostwinds, a United States based virtual private server hosting company, by a QTFY actor who used the qtfy100@gmail.com email address to register the Hostwinds account that leased those servers.

22. In an email dated on or around August 13, 2020, Hostwinds sent an abuse complaint to qtfy100@gmail.com, relaying information provided by the victim, Medical Center 1 of Ohio. The abuse complaint stated that Hostwinds IP address 192.236.192.6, which was subleased to qtfy100@gmail.com, was targeting Medical Center 1's Pulse Secure VPN vulnerability, CVE-2019-11510, the same vulnerability targeted in the August 2019 attack at NASA. Medical Center 1 included an additional comment in their communication to Hostwinds, which Hostwinds relayed to qtfy100@gmail.com. The additional message was "Attacking healthcare in a pandemic is just wrong. Please enforce

your AUP/TOS." Based on my training and experience, the acronyms AUP and TOS refer to Acceptable Use Policy and Terms of Service, respectively, and Medical Center 1 was requesting that Hostwinds enforce these policies against qtfy100@gmail.com.

23. In emails dated on or around November 29, 2019 and May 31, 2020, Hostwinds sent abuse complaints to qtfy100@gmail.com, relaying information provided by the victim, Financial Group 1 of South Korea. In its complaints, Financial Group 1 reported that IPs leased to qtfy100@gmail.com were scanning IP addresses owned by Financial Group 1. Based on my training and experience, hackers often scan IP addresses in order to find services exposed to the Internet in order to target those services. Financial Group 1 included the following additional language in its communication to Hostwinds, which was relayed to qtfy100@gmail.com: "The infrastructure of Financial Group 1 is classified as 'National Security Objective Facility - class A' and unauthorized access to this facility is strictly prohibited by related laws and regulations. Therefore, this access trial will be regarded as an illegal attack against foreign nation's critical infrastructure."

24. In an email dated on or around February 6, 2020, Hostwinds sent an abuse complaint to qtfy100@gmail.com, relaying information provided by the victim, Financial Group 2 of Michigan. In the email, Financial Group 2 listed eight Hostwinds IP addresses leased to qtfy100@gmail.com, that were attacking Financial Group 2 during the time period of December 19, 2019 to January 13, 2020.

25. In an email dated on or around January 15, 2020, Hostwinds sent an abuse complaint to qtfy100@gmail.com, relaying information provided by the victim, Insurance Agency 1 of Missouri. They indicated that IP address 142.11.212.111, which was leased by qtfy100@gmail.com, was targeting Insurance Agency 1, attempting to exploit the device using a different vulnerability: CVE-2019-19781. CVE-2019-19781 was a vulnerability in Citrix networking equipment. While technically different from CVE-2019-11510, CVE-2019-19781 was similar to the Pulse Secure vulnerability in that a successful exploitation would effectively grant the attacker remote access to a protected network.

26. A review of the abuse complaints received in the email accounts from the

search warrant returns as well as reporting on the Internet confirmed that numerous other IP addresses purchased by the users of the email accounts were used in malicious Internet vulnerability scans, botnet activity, and exploit attempts against known vulnerabilities.

27. In September 2024, QTFY actors conducted computer intrusions at three DOE National Laboratories, NIH, an HHS agency, and a U.S. security device manufacturer. These entities were victims of a zero-day attack against Ivanti Cloud Services Appliance (CSA). Ivanti CSA is an Internet appliance that provides secure communication and functionality over the Internet.

28. The QTFY actors used IP address 156.234.193.18 to remotely access all six victims. On or around October 17, 2024, domain www.**qtproxy.xyz** resolved to IP address 156.234.193.18. Between on or around December 3, 2023, and November 22, 2024, domain serverbks.xyz resolved to this same IP address, 156.234.193.18. Between on or around October 15, 2024, and November 25, 2024, domain docker-hub.**qt-team.com** also resolved to 156.234.193.18. Two of these, **qtproxy.xyz** and **qt-team.com**, are the **Target Domain Names**. All three domains are controlled by the QTFY actors:

a. Domain **qt-team.com** was registered on or about February 25, 2022 at domain registrar Namecheap with email account qkwl.yj@gmail.com, using the username "qtfy" and name "qt". Email account qkwl.yj@gmail.com is a recovery email account for the previously searched QTFY account songjun2020.sm@gmail.com.

b. Domain **qtproxy.xyz** was registered at domain registrar Namecheap with email account KNHLZN@proton.me, phone number +86-13076318234, payment method of PayPal account 120204803@qq.com. Domain **qtproxy.xyz** was also registered at Cloudflare with email account newtimebiz@outlook.com, which is the recovery email account for the previously searched QTFY account caiwenbai18@gmail.com.

c. Domain serverbks.xyz was also registered at Namecheap with the same phone number (+86-13076318234) and payment method (PayPal account

120204803@qq.com) as domain **qtproxy.xyz**. Additionally, QTFY actors logged into the Namecheap accounts for domains serverbks.xyz and **qtproxy.xyz** from the same IP address (38.46.221.154) on or around June 12, 2024.

29. Accordingly, there is evidence that the QTFY threat actors controlled 156.234.193.18 and were involved in the September 2024 cyber-attacks against the six victim entities.

*Use of the **Target Domain Names** in Computer Intrusions*

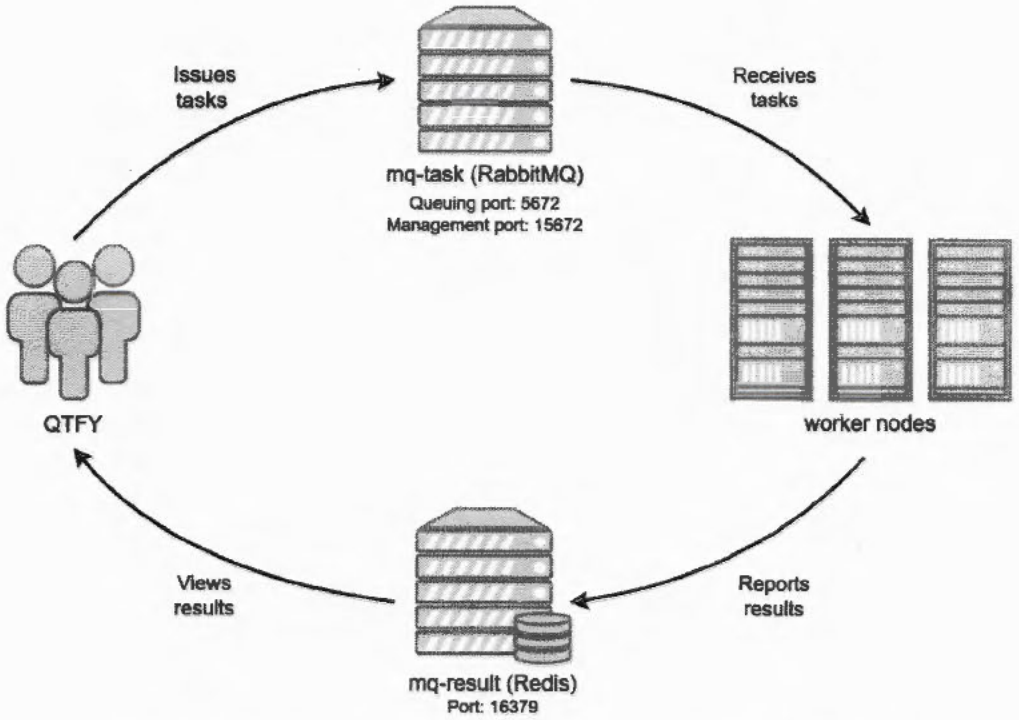
Use Involving QScan

30. Between October 2024 and May 2026, the FBI obtained Pen Register Trap and Trace (PRTT) orders and search warrants for four IP addresses (64.32.22.203, 148.135.90.22, 154.64.238.222, and 154.64.238.247). QTFY actors used servers assigned these IP addresses to operate QScan; servers operating QScan are referred to here as QScan servers.. From May 2022 to December 2025, mq-task.**qt-team.com** and mq-result.**qt-team.com** were the domains that resolved to the QScan server IP addresses. Between May 2024 and May 2025 mq-result.**qt-team.com** resolved to 64.32.22.203. Between May 2025 and December 2025 mq-result.**qt-team.com** resolved to 154.64.238.247. Between July 2024 and June 2025 mq-task.**qt-team.com** resolved to 148.135.90.22. Between June 2025 and December 2025 mq-task.**qt-team.com** resolved to 154.64.238.222.

31. From December 2025 to present, the QScan servers transitioned over to domains mq-result.**qt-proxy.org** and mq-task.**qt-proxy.org**. From December 2025 to present mq-result.**qt-proxy.org** resolved to 154.64.238.247. From December 2025 to present mq-task.**qt-proxy.org** resolved to 154.64.238.222. T**arget Domain Name qt-proxy.org** was registered at NameSilo from December 2025 to December 2026 with username "qtteam," email account vmdk001@proton.me, and Chinese cell phone number +86-15125550187.

32. Domains mq-task.**qt-team.com,** mq-result.**qt-team.com,** mq-task.**qt-proxy.org, and** mq-result.**qt-proxy.org** resolved to servers at IP addresses that hosted

respective components of QScan. The "mq-task" servers hosted RabbitMQ, an open-source "message broker" application used for sending communications ("messages") from one computer to another. In the case of QScan, the messages are scanning/exploit tasks submitted by QTFY actors and are executed by a pool of worker nodes, which typically were leased servers located outside of China. Finally, the "mq-result" server received completed tasks with Redis, a common database application.



33. QScan processed a variety of task queues, including webpage scraping, Trasport Layer Security (TLS) certificate [2] collection, subdomain enumeration, and penetration testing. Included with web scraping was a task queue dedicated to detecting the presence of certain potentially vulnerable plugins installed with content management systems. For penetration testing, QScan included a database of over 200 proof-of-concept exploits written in Python, and it was designed for large scale deployment. On a single day

[2] A TLS Certificate is a digital file issued by a trusted third party that verifies a website's identity and enables secure, encrypted communication. TLS certificates can provide an attacker information on the software or device type behind an IP address.

in 2024 for example, QScan processed over two million scanning/exploit tasks.

34. QScan log files and exfiltrated victim data obtained in a search warrant on 64.32.22.203 showed QTFY actors successfully exploited CVE-2024-24919, a vulnerability in Check Point Quantum Gateway, several days after the CVE was published in May 2024. The exploit provided access to files on the victim systems. Leveraging the exploit, QTFY actors stole sensitive information including server configuration files and user account details from over 300 organizations in the United States. Based on registered IP addresses and geolocation data, three of the victims were located in the Southern District of California.

Use Involving QTRouter

35. Between October 2024 and July 2026, the FBI obtained PRTT orders on domain **qtproxy.xyz**, and a server image on the resolution IP addresses for www.**qtproxy.xyz**.

36. The servers hosting domain **qtproxy.xyz** and its subdomains www.**qtproxy.xyz** and securelink.**qtproxy.xyz** are management servers for the QTRouter obfuscation network. These servers manage the QTRouter devices by maintaining lists of QTRouter devices, authenticating them onto the obfuscation network, providing them with lists of obfuscation network IP addresses, and logging QTRouter device activity. QTRouter hides a user's true IP address by routing the user's network traffic through various IP addresses, the various IP addresses in the network are called "nodes." Node types observed include commercial proxy service IP addresses (e.g., a proxy service called Fastlink was often utilized), Virtual Private Server (VPS) IPs, and compromised IoT devices. By mixing their malicious traffic with non-malicious users on commercial proxy services and compromising IoT devices and routing through IP addresses that geo-locate to locations of legitimate users of victim networks, QTRouter makes it difficult to identify and track malicious activity. The QTRouter obfuscation network consists of multiple integrated components:

a. QTRouter devices: Physical routers devices with custom software. Users of the obfuscation network have a QTRouter device issued to them and interact with an interface on the device. It provides functionality to view nodes, select nodes, and chain them together

b. Proxy Node Management System (代理节点管理系统): The name of the servers hosted at **qtproxy.xyz.** It authenticates QTRouter devices onto the obfuscation network and provides nodes lists to the QTRouter devices. It manages commercial proxy service node lists and VPS node lists. Node lists for compromised IoT devices are housed here so they can be provided to QTRouter users, however they are managed on the other systems listed below.

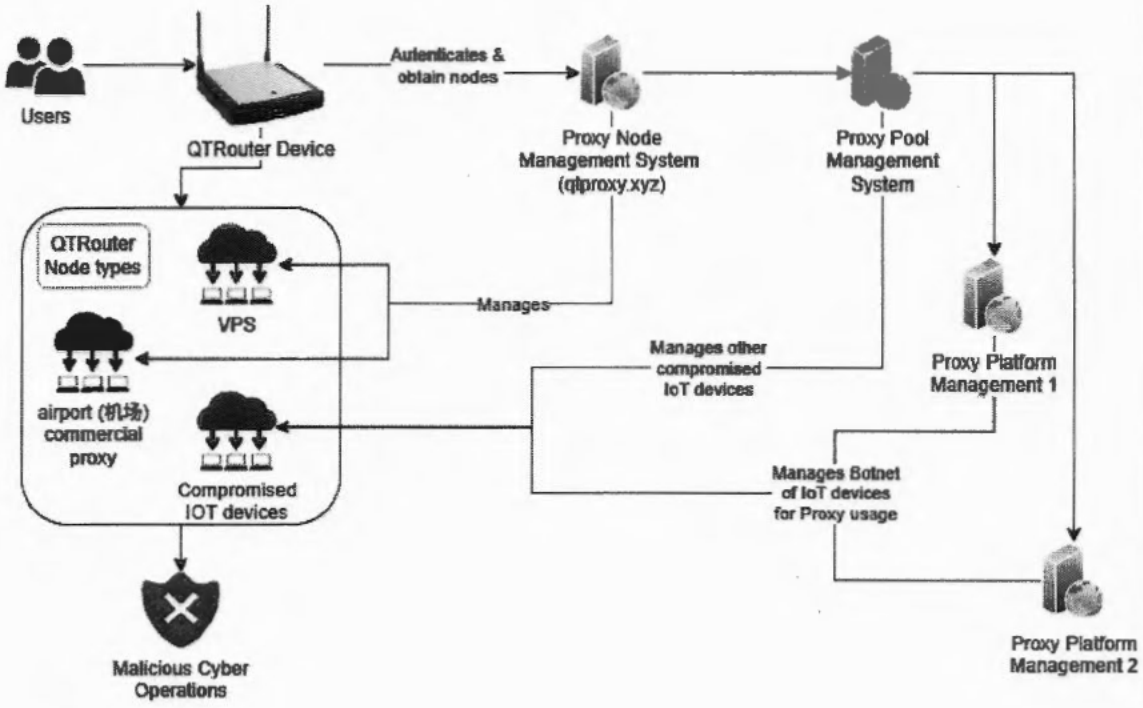
c. Proxy Pool Management System" (代理池管理系统): This was hosted at IP address 206.119.167.207. It is an aggregator of compromised IoT devices and hosted tools to compromise IoT devices. It hosted a database of exploits and a database of server fingerprints to quickly identify systems to target when a new exploit is discovered or when new proxy nodes are needed. It contained lists of multiple categories of compromised IoT devices along with access details (e.g., passwords). Categories included botnet SOCKS5 proxies, MikroTik RouterOS devices, and PPTP devices.

d. Proxy Platform Management (代理平台管理): This product manages a botnet of compromised devices, including IoT devices. Its primary function is to manage botnet nodes and to configure SOCKS5 proxy software on those devices. Three components of the platform were identified and hosted on open web directories: a "client," an "agent," and a "server." The threat actor interacts with a web interface on the management "server"; the "agent" is the C2 server and handles communication between the "client" and the management "server." Multiple separate Proxy Platform Management botnets are observed. Following is infrastructure attributed to this botnet:

//

	First Seen	Last Seen
23.95.220[.]192	2026-03-12	2026-05-12
103.201.131[.]121	2026-03-16	2026-05-16
109.236.48[.]121	2026-03-09	2026-03-11
install.anticonstitutionally[.]sbs	2026-03-03	Active
mail.fastsecurey[.]info	2026-03-30	Active
www.fastsecurey[.]info	2026-03-30	Active

e. Diagram of QTRouter Obfuscation Network:



International Transactions in Money Laundering Conspiracy

37. On or about February 25, 2022, QTFY controlled email account qkwl.yj@gmail.com, with username "qtfy" registered domain **qt-team.com** at Namecheap. Namecheap collects payments in the United States. The user paid $85.70 for the registration using a PayPal account registered to qkwl.yj@gmail.com, the payment was made from IP address 49.90.189.174, a China Telecom IP address located in Jiangsu, China. PayPal account records document the payment was made using an Agricultural Bank of China debit

card. The PayPal account that made the payment also utilized a Chinese cellular phone number, Chinese address, and a name in Chinese characters. Based on my training, experience, and this investigation, the payment for **qt-team.com** originated from China and traveled into the United States.

38. On or about November 10, 2022, QTFY controlled email account "KNHLZN@proton.me" registered domain **qtproxy.xyz** at Namecheap. The user paid $43.83 for the registration using a PayPal account registered to 120204803@qq.com. The payment was made from IP address 103.156.184.81 located in Taiwan. The Namecheap subscriber information included a Chinese cellular phone number and an address in China. PayPal account records document the payment was made using an Agricultural Bank of China debit card. The PayPal account that made the payment also had a Chinese cellular phone number, Chinese address, and a name in Chinese characters. Based on my training, experience, and this investigation, the payment for **qtproxy.xyz** originated from China and traveled into the United States.

39. On or about December 14, 2025, domain **qt-proxy.org** was registered at NameSilo. The payment was made from an IP address in Hong Kong and the user paid with Alipay. Alipay is a mobile and online payment platform based in China and owned by the Alibaba Group. NameSilo received the Alipay payment through a payment gateway named Pockyt, aka Yuansfer, headquartered in New York City, New York. NameSilo provided the Gateway Order ID for the payment they received, this ID was presented to Pockyt and they identified the Alipay account making the payment was a user with a Chinese phone number. Based on my training, experience, and this investigation, the payment for **qt-proxy.org** originated from China and traveled into the United States.

40. As described above, the **Target Domain Names** are property used as part of a scheme to commit violations of 18 U.S.C. §§ 1956(h) (conspiracy to launder money), 1956(a)(2)(A) (international promotional money laundering), and 18 U.S.C. § 1030(a)(5)(A).

SEIZURE PROCEDURE

41. As detailed in Attachment A-1, upon execution of the seizure warrant, the registry for .xyz domains, XYZ.COM, shall be directed to restrain and lock **qtproxy.xyz** pending transfer to the United States upon completion of forfeiture proceedings, to ensure that changes to those domains cannot be made without prior consultation with the FBI or DOJ.

42. As detailed in Attachment A-2, upon execution of the seizure warrant, the registry for .org domains, , Public Interest Registry, shall be directed to restrain and lock **qt-proxy.org** pending transfer to the United States upon completion of forfeiture proceedings, to ensure that changes to that domain cannot be made without prior consultation with the FBI or DOJ.

43. As detailed in Attachment A-3, upon execution of the seizure warrant, the registry for .com domains, Verisign, shall be directed to restrain and lock **qt-team.com** pending transfer to the United States upon completion of forfeiture proceedings, to ensure that changes to that domain cannot be made without prior consultation with the FBI or DOJ.

44. Upon seizure of the **Target Domain Names** by the FBI, XYZ.COM, Public Interest Registry, and Verisign will be directed to associate some or all of the **Target Domain Names** to new servers as designated by the FBI.

45. In addition, as detailed in Attachment A-1, A-2, and A-3, the FBI will post a notice on the seized **Target Domain Names** that will consist of law enforcement emblems and text, explaining that the domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Southern District of California as part of a coordinated international law enforcement action taken against QTFY for computer hacking activity.

CONCLUSION

46. As set forth above, there is probable cause to believe that the **Target Domain Names** are subject to civil and criminal forfeiture because they were used in a conspiracy to violate 18 U.S.C. §§ 1956(h) (conspiracy to launder money) and 1956(a)(2)(A)

(international promotional money laundering). Accordingly, the **Target Domain Names** are subject to forfeiture to the United States, and I respectfully request that the Court issue seizure warrants for the **Target Domain Names.**

47. Because the warrants will be served on XYZ.COM, Public Interest Registry, and Verisign, which control the **Target Domain Names**, and XYZ.COM, Public Interest Registry, and Verisign, thereafter, at a time convenient to it, will transfer control of the **Target 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.

48. Finally, and in order to protect the ongoing covert 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.

[redacted]

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 24th day of August, 2026.

[redacted]

U.S. MAGISTRATE JUDGE