

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
Routers Infected with 5socks and Anyproxy Malware

Case No. 25mj-374-CD**FILED UNDER SEAL**

FILED
 MAY 02 2025
 Heidi D. Campbell, Clerk
 U.S. DISTRICT COURT

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in Multiple Federal Judicial Districts, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

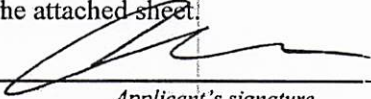
18 U.S.C. § 371
 18 U.S.C. § 1030(a)(5)(A)

Conspiracy
 Damage to a Protected Computer

The application is based on these facts:

See Affidavit of Camron Borders, attached hereto.

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

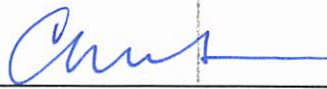

 Applicant's signature

SA Camron Borders, FBI
 Printed name and title

Subscribed and sworn to by phone.

Date: May 2, 2025

City and state: Tulsa, Oklahoma


 Judge's signature

Christine D. Little, U.S. Magistrate Judge
 Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Routers Infected with the 5socks and
Anyproxy Malware**

Case No. _____

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF RULE 41(b)(6)(B) WARRANT

I, Camron Ellis Borders, being duly sworn, hereby declare as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41(b)(6)(B) to use remote access techniques to search infected internet routers that are located in the United States, described in Attachment A, and to seize or copy electronically stored data related to the 5socks and Anyproxy malware and proxy services, further described in Attachment B, which are the evidence and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy) and 18 U.S.C. § 1030(a)(5)(A) (Damage to a Protected Computer).

2. The proposed warrant does not authorize the collection of the content of communications from infected routers, nor does it authorize law enforcement officers to alter the operating systems, files, or software on the infected routers except as expressly provided in this affidavit.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been employed by the FBI since January 2024. I am currently assigned to the Oklahoma City Division, Cyber Squad. In this capacity, I am charged with investigating violations of federal criminal law to include computer intrusions, cyber-criminal infrastructure and other crimes involving the use of computers. I have participated in the execution of multiple federal warrants.

STATEMENT OF PROBABLE CAUSE

A. *Background into the 5socks and Anyproxy criminal proxy services*

5. Since July 2024, the FBI has been investigating the proxy services¹ 5socks, located at "5socks.net," and Anyproxy, located at "Anyproxy.net," being advertised on online criminal discussion forums.

6. Based on my training and experience, criminals utilize proxy services to gain anonymity and obfuscation from law enforcement by routing their internet traffic through the proxy server. Proxy services can also circumvent firewalls of targeted computers that attempt to filter out-of-state or foreign internet traffic. Although

¹ A proxy service or specifically a proxy server, is a system or router that provides a gateway between users and the internet. It acts as a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online. See www.fortinet.com/resources/cyberglossary/proxy-server.

legitimate proxy services exist for lawful purposes, criminal proxy services typically do not comply with legal process or record any information on their users so that the users of the proxy servers can remain fully anonymous from police intervention. Additionally, criminal proxy services often use compromised computers infected with malware without the computer owner's knowledge. These include methods such as, installing viruses or backdoors on users' computers, tablets, or cellular phones through various means, including but not limited to, illegitimate VPNs, app store applications, and other methods.²

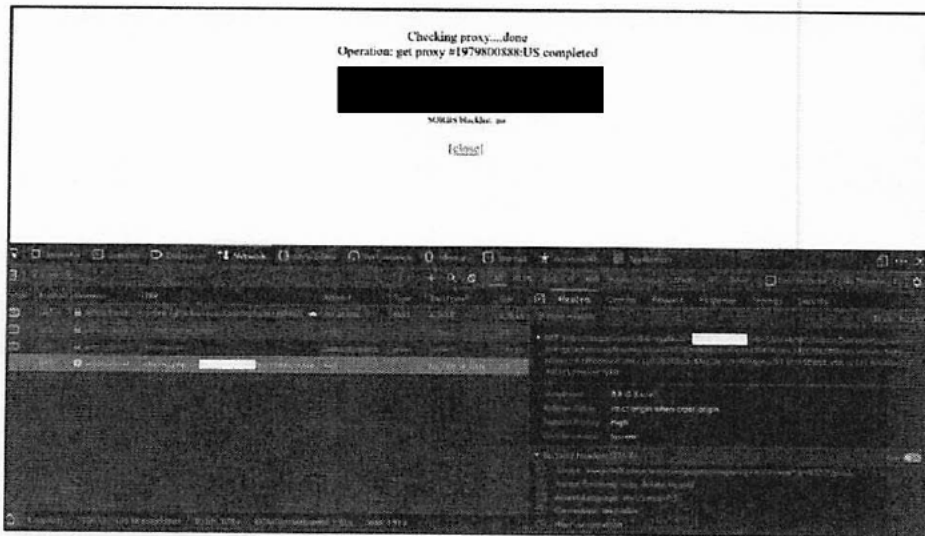
7. In particular, the 5socks and Anyproxy proxy services have been used by cyber actors to facilitate criminal activity, such as ransomware attacks, cryptocurrency heists, and other computer intrusions affecting victims in the United States and elsewhere.

8. 5socks.net's website advertises for sale over 7,000 anonymous proxies available in locations across the world, including in the United States. Customers can either purchase a preset number of proxies that expire daily or a preset number of proxies that expire monthly. Both of these plans are paid on a monthly subscription basis, with prices ranging from \$9.95 to \$110 per month. Additionally, the website's slogan "Working since 2004!" indicates this service has been operational for 20 years.

² 911 S5 Residential Proxy Service was a large residential proxy service that was taken down by U.S. law enforcement that used illegitimate VPNs to facilitate the proxy network. See www.ic3.gov/PSA/2024/PSA240529.

9. During the course of this investigation, the FBI determined that 5socks is a re-seller of proxies originally offered for sale by the older proxy service Anyproxy. On the 5socks.net administrative portal, there is a tool called "Check IP v.1.0" that allows users to see their current IP address and other networking related information. At the bottom of this tool, there is a "2004 anyproxy.net" copyright stamp.

10. The FBI was also able to publicly see an internet network GET request³ being sent to the Anyproxy.net server when purchasing a proxy from the 5socks.net SOCKS portal. Although this request failed to return a proper response, it was the same GET request as another GET request sent at the exact same time to the 5socks.net server.



11. In addition, the FBI was able to determine, based on internet network traffic, WHOIS records, and information provided by the Dutch National Police, that

³ A GET request is an HTTP request when a website asks a server for information. The server will return the requested information or an error message if the request does not complete properly. See <https://en.wikipedia.org/wiki/HTTP>.

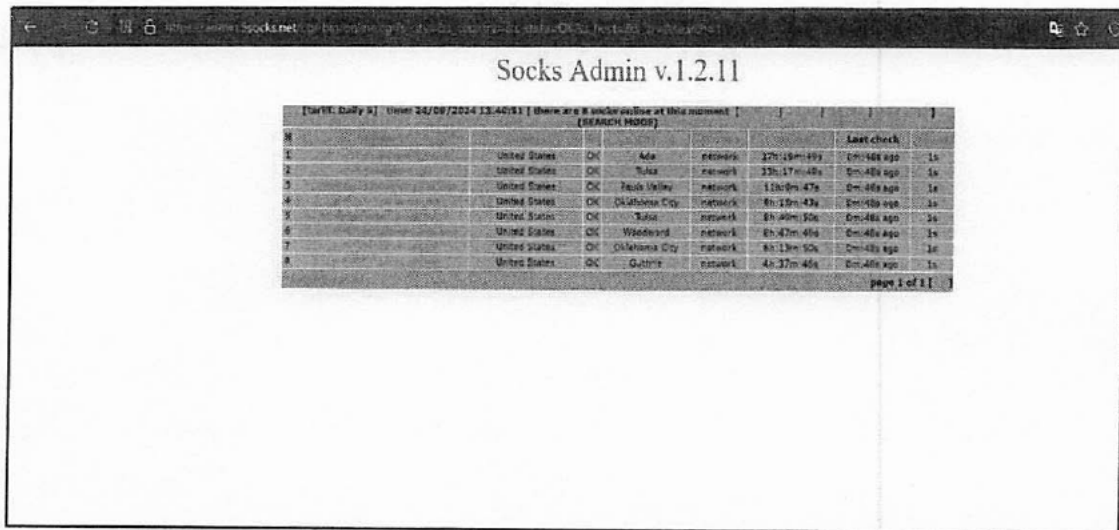
0.00323987 Bitcoin, excluding fees,⁴ into several cryptocurrency wallets created by the FBI. The OCE then registered for an account with 5socks.net's website, selected the option to purchase five daily proxies, and agreed to send payment using Bitcoin.

14. The OCE received an email from reg@5socks.net with a username and password for login. Upon logging in, the OCE was directed to "pay by Perfect Money."⁵ The OCE used Perfect Money to deposit 0.0006 Bitcoins, excluding fees, into a wallet designated by 5socks.net.

15. On September 24, 2024, the OCE logged back into 5socks.net and was presented with a message stating the account was successfully funded. The OCE navigated to the main menu and was presented with a list of proxies available for purchase. The OCE filtered the list of available proxies down to those located in the State of Oklahoma. This list returned eight Oklahoma-based proxies available for purchase.

⁴ A user pays a small transaction fee to process the transfer of Bitcoin.

⁵ Perfect Money is an online payment system, similar to PayPal, allowing users to send and receive funds through various national currencies. Perfect Money is popular in Russia and Eastern Europe.



16. The OCE then proceeded to purchase the following five Oklahoma proxies and identified their subscribers:

Location	ISP	IP & Port Address	Owner
Oklahoma City	Cox	[REDACTED]	Commercial real estate
Oklahoma City	Cox		Residential home builder
Tulsa	AT&T		Unknown
Tulsa	Encore		Sports & fitness magazine
Guthrie	Cox		Convenience store

17. Law Enforcement interviewed the owners of the Oklahoma City commercial real estate company ("Business 1") and the Tulsa sport and fitness magazine ("Business 4"). Both owners stated they were unaware of any issues with their internet services, but they both disclosed that they used Cisco Linksys E1200 wireless routers to supply their internet service.

18. The E1200 router is a popular older-model router that features remote access connectivity, allowing users who do not have physical control of the router to nevertheless reconfigure it. However, this router has known vulnerabilities in its remote access connection protocols that allow skilled computer hackers to hijack the device for their own purposes.⁶

19. The FBI also identified and contacted the owner of the router listed as the Oklahoma-based "Pauls Valley" proxy on 5socks.net, a car wash business located in Tuttle, Oklahoma ("Business 6"), which agreed to allow the FBI to successfully extract a copy of the malware from their infected router.

20. Based on my training and experience, Business 1, Business 4, and Business 6 are victims of 5socks. The proxy servers being sold via 5socks and Anyproxy are compromised residential⁷ internet networks. This is a common tactic of criminal proxy services, to compromise individuals or small businesses, then to sell

⁶ Home and office routers are frequent targets of hackers seeking to use the equipment in further crimes. See, e.g., Jessica Lyons, *Someone is Slipping a Hidden Backdoor into Juniper Routers Across the Globe*, THE REGISTER (Jan. 25, 2025), https://www.theregister.com/2025/01/25/mysterious_backdoor_juniper_routers/; Dan Goodin, *Thousands of Hacked TP-Link Routers Used In Yearslong Account Takeover Attacks*, ARS TECHNICA (Nov. 1, 2024), <https://arstechnica.com/information-technology/2024/11/microsoft-warns-of-8000-strong-botnet-used-in-password-spraying-attacks/>; Dan Goodin, *Bizarre Attack Infects Linksys Routers With Self-Replicating Malware*, ARS TECHNICA (Feb. 13, 2024), <https://arstechnica.com/information-technology/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/>

⁷ The term "residential" is used by these services to relay to potential customers that the services being offered are not data-center proxies but are individuals or businesses, which can lead to greater anonymity for the customer.

access to those networks to utilize as a proxy server which will provide anonymity to the criminals and make it appear their internet traffic is coming from the victim's networks. Customers of 5socks and Anyproxy who access these and other victim routers are essentially using the internet services belonging to the rightful owners of the victim routers.

C. Remote Access, Searches, and Seizures

21. The Dutch National Police, based on their access to 5socks and Anyproxy C2 infrastructure located in the Netherlands, have obtained, and provided U.S. authorities with, a list of victim router IP addresses. The 5socks and Anyproxy C2 infrastructure located in the Netherlands has transmitted proxy traffic through these victim router IP addresses during the past sixty days. In order to do so, they must be infected with the 5socks and Anyproxy malware.

22. Based on an analysis of the victim router IP addresses, FBI has determined that approximately eight hundred to nine hundred routers appear to be both currently infected with 5socks and Anyproxy malware and also located in the United States.

23. These hundreds of infected routers with IP addresses that are geolocated in the United States appear to be located in at least five or more judicial districts, including, but not limited to the following: Northern District of Oklahoma, Western District of Oklahoma, Eastern District of Virginia, Southern District of West Virginia, and Central District of California.

24. Infected routers located in the United States constitute “protected computers” within the meaning of Rule 41(b)(6)(B) and 18 U.S.C. § 1030(e)(2)(B) because they are used in or affecting interstate or foreign commerce or communication, based on their connection to the internet. The infected routers have been damaged within the meaning of Rule 41(b)(6)(B) and 18 U.S.C. § 1030(e)(8) because the 5socks and Anyproxy malware has impaired the integrity and availability of data, programs, systems, and information on the infected routers.

25. The FBI has partially reverse engineered the malware that was installed onto a victim device. Analysis of the reverse engineered malware revealed that the malware operates from the router’s short-term memory, which would be wiped off the device if it were to shut off or lose power for any reason. To re-establish control over the victim router in these circumstances, a different portion of the C2 infrastructure located in Turkey attempts to contact the compromised devices every 60 seconds to determine if the malware is still running. If it is not, the C2 infrastructure located in Turkey will attempt to re-exploit the victim router and re-install the malware. This will bring the victim router back under the control of Anyproxy and 5socks to again be sold to their customers.

26. Through its investigation, the FBI has gained a comprehensive understanding of the structure and function of the 5socks and Anyproxy proxy services. Based on that knowledge, the FBI has developed a means to identify infected routers, disconnect them from the proxy services, and prevent the administrators from

further communicating with those infected routers. This warrant would authorize certain aspects of that identification and search process as described below:

27. First, the FBI will identify the IP addresses of the victim routers, which are infected with 5socks and Anyproxy malware and are part of the 5socks and Anyproxy proxy services. FBI will do so based on information obtained from Dutch authorities, including the proxy leasing page obtained from the C2 server located in the Netherlands. This information includes a list of IP addresses and port numbers used by each infected router. Only routers that are part of the proxy network, or have communicated with the C2 infrastructure in the past sixty days, would be on this list.

28. Second, the FBI, from an FBI-controlled computer located in the United States, will connect to each of those routers using known vulnerabilities. FBI will issue a remote command to reboot the router, which will clear the router's volatile memory, including the malware. FBI will then close the vulnerability used by the administrators of the proxy services by disabling internet-facing remote management of the router. Disabling remote access will not interfere with the victims' internet access, and remote management will still be accessible through the router's Local Area Network. FBI will commit that change to the router's non-volatile memory. These actions will have the effect of removing the router from the proxy network and preventing the router from being vulnerable to reinfection.

29. The proposed warrant would authorize the FBI to restart the routers and disable remote access. The proposed warrant also authorizes law enforcement officers to seize or copy from the infected routers any electronically stored information,

including encryption keys and access logs used by the 5socks and Anyproxy administrators to communicate with computers that are part of the proxy service infrastructure, as well as IP addresses and routing information, necessary to determine whether the infected router continues to be controlled by the 5socks and Anyproxy proxy services.

30. The FBI will not collect content from the infected routers, nor will FBI alter the functionality of the infected routers' operating systems, files, or software, except as expressly provided in this affidavit. The owners of the victim routers will be able to reverse the FBI's changes by re-enabling remote management. The actions authorized by this warrant are designed to prevent the routers from being used as proxies and to prevent additional malware from being installed on the routers, by removing the victim routers from the proxy services and disabling remote access. The FBI has tested these actions to ensure that they operate properly and do not impact any other files or services on the infected routers.

TIME AND MANNER OF EXECUTION

31. I request, pursuant to Rule 41(e)(2), that the Court authorize the execution of this warrant for a period of fourteen days, beginning on May 2, 2025, and ending on May 16, 2025.

32. Because FBI intends to minimize the impact of restarting the routers, which only takes a matter of minutes, good cause exists to permit the execution of the requested warrant at any time in the day or night.

DELAYED NOTIFICATION

33. I request, pursuant to Rule 41(f)(3) and 18 U.S.C. § 3103a(b), that the Court authorize the officers executing this warrant to delay notice until thirty days after the collection authorized by the warrant has been completed, including extensions. There is reason to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the infected routers would seriously jeopardize the ongoing investigation, as such a disclosure would likely become known to the proxy service administrators and would give them an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1). The proposed search warrant does not authorize the seizure of any tangible property. See 18 U.S.C. § 3103a(b)(2). Further, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. See id.

34. In the event that providing notice to the subscriber or user of the infected computer no longer seriously jeopardizes the ongoing investigation, U.S. authorities will take steps to provide such notification earlier than thirty days after the collection authorized by the warrant has been completed, including extensions.

CONCLUSION

35. For all the reasons described above, there is probable cause for a warrant to use remote access to search electronic storage media described in Attachment A and to seize or copy electronically stored information described in Attachment B.

Respectfully submitted,



Camron Ellis Borders
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn to by phone on May 2nd, 2025.



CHRISTINE D. LITTLE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to the electronic storage media contained in victim routers located in the United States onto which malicious cyber actors have installed, without authorization, malware, and which routers have communicated with the 5socks and Anyproxy proxy service infrastructure.

ATTACHMENT B

ITEMS TO BE SEIZED

This warrant authorizes the search of the electronic storage media identified in Attachment A and the seizure or copying of electronically stored information that constitutes evidence and/or instrumentalities of the 5socks and Anyproxy conspiracy and computer fraud in violation of 18 U.S.C. § 371 (Conspiracy) and 18 U.S.C. § 1030(a)(5)(A) (Damage to a Protected Computer). This warrant authorizes the government to remotely access and search the victim routers identified in Attachment A by issuing commands to:

1. Seize or copy from those routers any electronically stored information, such as encryption keys and server lists, used by the administrators of the 5socks and Anyproxy proxy services to communicate with computers that are part of the proxy services infrastructure;
2. Seize or copy from those routers any electronically stored information, such as IP addresses and routing information, necessary to determine whether any router identified in Attachment A continues to be controlled by the 5socks and Anyproxy administrators after the seizure or copying of the electronically stored information identified in Paragraph 1;
3. Reboot the router; and
4. Disable the internet-facing remote management of the router.

This warrant does not authorize the seizure of any tangible property. Except as provided above, this warrant does not authorize the seizure or copying of any content

from the electronic storage media identified in Attachment A or the alteration of the functionality of the electronic storage media identified in Attachment A.