

UNITED STATES DISTRICT COURT

for the

Western District of Pennsylvania

In the Matter of the Search of)

(Briefly describe the property to be searched)
or identify the person by name and address))

INFECTED DEVICES AND COMMAND-AND-CONTROL)
SERVERS IN THE UNITED STATES THAT ARE PART)
OF A MIRAI BOTNET)

Case No. 24-1484

[UNDER SEAL]

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Pennsylvania
(identify the person or describe the property to be searched and give its location):

Please see Attachment A, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see Attachment B, incorporated herein.

YOU ARE COMMANDED to execute this warrant on or before September 23, 2024 (not to exceed 14 days)

in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to [REDACTED]

(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for 30 days (not to exceed 30) until, the facts justifying, the later specific date of [REDACTED]

Date and time issued: 09/09/2024 12:45 pm

City and state: Pittsburgh, Pennsylvania

Printed name and title

Return

Case No.:
24-1484

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH AND
SEIZURE OF INFECTED DEVICES AND
COMMAND-AND-CONTROL SERVERS IN
THE UNITED STATES THAT ARE PART OF
A MIRAI BOTNET

Magistrate No. 24-1484
[UNDER SEAL]

**AFFIDAVIT BY TELEPHONIC OR OTHER RELIABLE ELECTRONIC MEANS
IN SUPPORT OF AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT**

I, Special Agent [REDACTED] being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. The Federal Bureau of Investigation (FBI) is investigating Chinese hackers, known to the private sector as “Flax Typhoon,” who have installed a specific variant of malware on thousands of internet-connected devices, including small-office/home-office (SOHO) routers, internet protocol (IP) cameras, digital video recorders (DVRs), and network-attached storage (NAS) devices. These infected devices currently exist in the Western District of Pennsylvania, and throughout the United States and in numerous foreign countries. This specific variant of malware links the infected devices with other similarly infected devices to form a network of connected devices, also known as a “botnet,” which the Flax Typhoon hackers use to commit additional computer intrusions against other U.S. and foreign victims.

2. The FBI will identify U.S.-based devices infected with this malware, as well as the malware’s U.S.-based command-and-control (C2) servers, as described in Attachment A. The FBI seeks authorization under Federal Rule of Criminal Procedure 41(b)(6)(B) to remotely search those devices and seize the evidence and instrumentalities of the hackers’ criminal offenses, as described in Attachment B. As part of this search and seizure, the FBI will seize and send commands to and

through the botnet's C2 servers, remove the C2s from the botnet, and disable the malware on the infected devices.

AGENT BACKGROUND

3. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7); that is, an officer of the United States who is empowered to conduct investigations and make arrests for the offenses alleged in this affidavit.

4. I am a Special Agent with the FBI and am currently assigned to the San Diego Cyber National Security Squad. In this capacity, I investigate possible violations of federal criminal law, specifically computer intrusions by sophisticated cyber actors, and I am familiar with the means and methods used to commit these offenses.

5. 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 warrant and does not set forth all my knowledge about this matter. I have not, however, excluded any information known to me that would undermine a determination of probable cause.

LEGAL AUTHORITY

6. Federal Rule of Criminal Procedure 41(b)(6) provides that "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without

authorization and are located in five or more districts.”

7. 18 U.S.C. § 1030(a)(5)(A) provides that whoever “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished[.]” Section 1030(e)(2)(B) defines a “protected computer” as a computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]” Section 1030(e)(8) defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information[.]”

8. 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.”

9. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy) have been committed in the Western District of Pennsylvania and elsewhere. There is also probable cause to send commands to and through the U.S.-based C2 servers identified in Attachment A, and search U.S.-based C2 servers and infected U.S.-based devices, and seize evidence and instrumentalities of these crimes, as described in Attachments A and B.

THE MIRAI MALWARE VARIANT

10. Infected devices in a botnet, known as a “bots,” are controlled by one or more C2 servers. Through C2 servers, hackers can control and use a botnet for their illegal purposes like

transmitting malware, conducting cyber attacks, and obfuscating the hackers' true IP address, identity, and physical location. For example, when an overseas hacker accesses a U.S. victim's network through a U.S.-located bot, it will appear that the hacker's computer is located in the United States at the location to which IP addresses of the infected device (bot) resolves, and thereby deceptively blend into the local internet traffic of the hacking victim.

11. Mirai is a type of malware capable of infecting internet-connected devices without their owners' consent and creating a botnet that receives commands from C2 servers. Variants of Mirai malware have been used by a variety of malicious hacking groups to conduct computer intrusions targeting victims within the United States and in foreign countries.

12. In May 2024, the FBI analyzed samples of a particular variant of Mirai malware that had been uploaded to an online service that collects suspicious files in an effort to analyze them and detect malware and other malicious files. This variant was used to infect internet-connected devices such as SOHO routers, IP cameras, DVRs, and NAS devices, and was embedded with encoded domain names that resolved to C2 servers.¹ This variant was designed to run on x86, MIPS, ARM, PPC, and SH4 processor architectures.² The FBI identified several C2 domains used by this variant, including subdomains of w8510.com (*e.g.*, testate.w8510.com).³

13. In July 2024, [REDACTED] the FBI identified IP addresses of dozens of C2 servers – including U.S.-based C2 servers – that were hosting various subdomains

¹ Once a person, or registrant, registers a domain name, the registrant can decide which IP address and server the domain name will resolve to.

² A processor architecture describes the design and organization of a computer's central processing unit (CPU).

³ Domain names are composed of one or more parts separated by periods. The right-most label is the top-level domain. Taking testate.w8510.com as an example, the top-level domain is ".com." The second-level domain is then "w8510," and "testate" is the third-level domain. The example testate.w8510.com, containing a third-level domain, is often called a subdomain.

of w8510.com, and continued to identify additional C2 servers as they were incorporated into the botnet. [REDACTED]

[REDACTED] the FBI confirmed that these C2 servers were managing and controlling thousands of bots worldwide that had been infected with this variant of Mirai malware. The FBI also confirmed that these C2 servers were themselves controlled by other servers (“upstream management servers”), consistently communicating with them over a particular uncommon port number, Transmission Control Protocol (TCP) port 34125.⁴

14. The FBI has identified and reviewed data from multiple upstream management servers. Upon review of data from one of these servers on June 5, 2024, the FBI found that it hosted a MySQL⁵ database, which stored information used to manage the botnet. The MySQL database contained a table with information about each of the infected victim devices, as well as the C2 server communicating with each infected device. The database contained records of over 1.2 million devices worldwide that had at one time been infected with the variant, including over 385,000 unique U.S.-based victim devices. However, as of the June 5, 2024 review, the data indicated that only approximately 260,000 devices, including approximately 126,000 U.S.-based devices, were *actively* infected.

15. 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

⁴ Transmission Control Protocol (TCP) is communications standard for delivering data and messages through networks. TCP uses unique numbers, called ports, ranging from 1 to 65,535.

⁵ MySQL is an open-source database management software that allows a computer to store and organize information in a way that can be accessed for later use by computer programs and their users.

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).

16. IP addresses are geographically organized, and the general location of an IP address, and the likely location of the user, can be identified based on open-source databases. The FBI has investigated the geographic locations of the IP addresses 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)(5)(A) and 371 have been committed in the Western District of Pennsylvania and more than four other federal districts.

FLAX TYPHOON USES THE MIRAI-BASED BOTNET

17. [REDACTED]

[REDACTED] the FBI observed that the C2 servers and the upstream management servers described in paragraph 13 were accessed on multiple occasions from a certain IP address registered to China Unicom Beijing Province Network, including by using TCP port 34125, showing that the user of this Chinese IP address was interacting with and controlling this botnet.

18. In August 2023, Microsoft Threat Intelligence published a report explaining that a group of Chinese hackers, known as Flax Typhoon, “has been active since mid-2021 and has targeted government agencies and education, critical manufacturing, and information technology organizations in Taiwan,” as well as “elsewhere in Southeast Asia, as well as in North America and Africa.”⁶ The Microsoft blog post also listed some of the computer intrusion tactics and IP addresses used by Flax Typhoon.

⁶ Microsoft Threat Intelligence is a Microsoft community of security researchers, analysts, and cyber threat hunters. It has provided credible and reliable information in the past that the FBI has been able to independently verify.

19. In September 2023, a California company (California victim) reported to the FBI that it was the victim of a computer intrusion. The California victim provided the FBI with a list of several IP addresses that were assigned to servers used to commit the computer intrusion. These IP addresses, as well the computer intrusion tactics, matched some of those that Microsoft identified in the prior month's blog post describing Flax Typhoon.

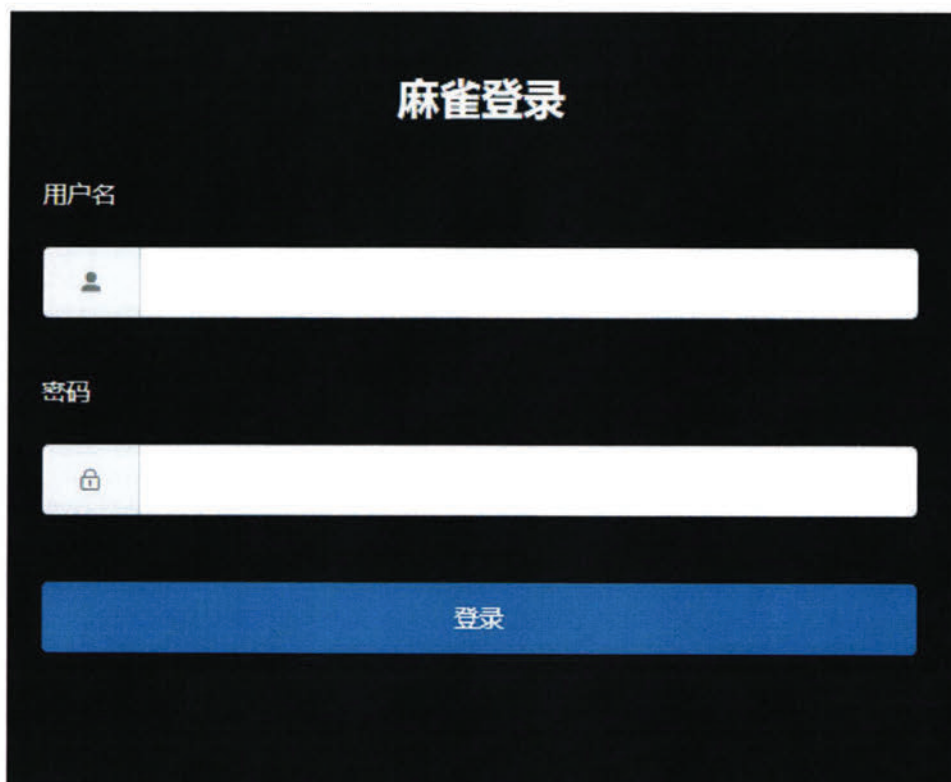
20. Upon receiving the California victim's report, the FBI began investigating servers that were the source of unauthorized connections to the California victim's network. One such server (IP Address 1) was accessed as recently as June 2024 by the same China Unicom Beijing Province Network IP address, described in paragraph 17, that also regularly accessed the upstream management and botnet C2 servers. Additional servers used to gain unauthorized access to the California victim's networks were also accessed from IP Address 1, thus associating the California victim activity with the China Unicom Beijing Province Network IP address.

21. Based on information the FBI collected from other victims of Flax Typhoon computer intrusion activity, the FBI determined that multiple IP addresses used to access the IP Address 1 server, including two additional China Unicom Beijing Province Network IP addresses that had accessed the IP Address 1 server as recently as August 2023, had also been used to access servers used in Flax Typhoon computer intrusion activities against these other hacking victims throughout 2023. These other Flax Typhoon victims include U.S. and/or foreign corporations, universities, non-governmental organizations, government agencies, telecommunications providers, and media organizations.

**FLAX TYPHOON AND THE MIRAI-BASED BOTNET
ARE ASSOCIATED WITH INTEGRITY TECHNOLOGY GROUP**

22. The FBI's investigation of the relevant variant of Mirai malware revealed that the upstream management servers hosted an application for managing the botnet's C2 servers and

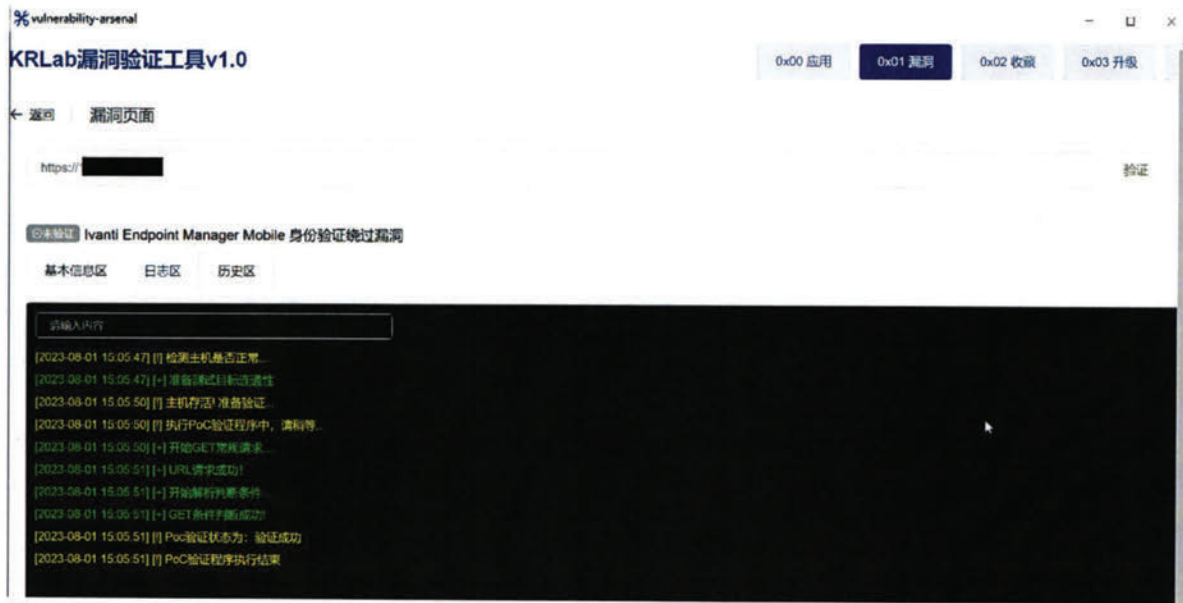
bots. The application's users could assign tasks to the bots, including uploading or downloading files, remotely executing commands, growing the botnet, or conducting cyber attacks. The application's users could also query information stored in the MySQL database hosted on the upstream management servers. The following is a screenshot of the login page for the application; the name for the application, “麻雀” (translated as “sparrow”) appears at the top of the image:



23. The MySQL database also stored logs of the users of the Sparrow application. Those records showed that specific IP addresses registered to China Unicom Beijing Province Network were repeatedly used to access the Sparrow application. These same IP addresses were also used to access servers used in multiple computer intrusions that the FBI has attributed to Flax Typhoon hackers. The FBI, therefore, assesses that the same actors are responsible for both Flax Typhoon activity and using the Sparrow application to control this botnet.

24. Based on the review of upstream management servers, the FBI determined that the source code for the Sparrow application was stored and available within an online repository hosted at https://git.li-exp.com/krlab/project_maque.git.⁷ The Chinese word for sparrow can be spelled as “maque” in Roman characters. The uniform resource locator (URL) for this repository also shows Sparrow source code was stored in a folder named KRLab. Additional information related to the Sparrow application was located at the URL [https://git.li-exp.com/\[INDIVIDUAL 1\]/sparrow/-/jobs/42911](https://git.li-exp.com/[INDIVIDUAL 1]/sparrow/-/jobs/42911). This address indicates that the Sparrow application is associated with INDIVIDUAL 1, described further below in paragraph 27.

25. The Sparrow application contains several tools, including one called “vulnerability-arsenal,” which users can use to conduct intrusions or attacks on victim computer networks, by relaying commands to the bots through the C2 servers. The following is a screenshot of the “vulnerability-arsenal” tool, which contains another reference to KRLab in the top left corner:



⁷ Git is a tool used to manage and track changes to computer files, especially source code, during software development.

26. Integrity Technology Group is a publicly-traded information security company headquartered in Beijing, China. According to its public financial statements, posted online on or around May 5, 2023, Integrity Technology Group has three main brands, one of which is named KRLab.

27. On or around February 2, 2024, the State Intellectual Property Office of the People's Republic of China published a Chinese patent application for technology to implement the installation and configuration of multiple proxy services onto an existing network of nodes. Integrity Technology Group was the applicant, and the inventors were listed as managers of the company's KRLab brand and INDIVIDUAL 1, described in paragraph 24 as an individual associated with the Sparrow application online repository. The technology discussed in this patent application is consistent with the implementation of a proxy service running on top of a botnet – i.e., the botnet functionality that allows its users to obfuscate the true location of their activities. The patent application identified that the proxy nodes would consist of devices with x86, MIPS, ARM, PPC, and SH4 processor architectures. As described in paragraph 12, the Mirai botnet malware relevant to this application is intended to run on x86, MIPS, ARM, PPC, and SH4 processor architectures.

28. Based on my training and experience, and the information described above, I assess that Integrity Technology Group is responsible for developing the Sparrow application to control this botnet and is also responsible, at least in part, for the computer intrusion activities collectively attributed to Flax Typhoon.

MANNER OF EXECUTION

29. The FBI has probable cause to believe that Flax Typhoon hackers violated 18 U.S.C. §§ 1030(a)(5)(A) and 371 by installing the variant of Mirai malware on U.S.-based devices

without authorization. The FBI seeks authorization under Federal Rule of Criminal Procedure 41(b)(6)(B) to remotely search U.S.-based C2 servers and U.S.-based infected devices and seize the unauthorized botnet, including the Flax Typhoon malware on the infected devices and other Flax Typhoon data located on U.S.-based C2 servers (the evidence and instrumentalities of the crimes).

30. As part of its native functionality, this variant of Mirai malware allows the malicious actors, who are the exclusive users of the botnet's C2 servers, to send a command to the C2 servers to provide non-content information (including IP address) about the infected devices controlled by the C2 servers. The FBI can also use this command to identify U.S.-based infected devices, as described in Attachment A.

31. As part of its native functionality, this variant of Mirai malware also allows users of the C2 servers to send one or more commands to the malware on specified infected devices, ending one or more malicious botnet-related computer processes, which will have the effect of disabling the malware. The FBI has tested these commands and confirmed that they do not affect any legitimate functionality of the infected devices or collect any content information.

32. To search and seize the botnet, the FBI seeks authorization to take one or more of the following actions on U.S.-based C2 servers and, through those and other C2 servers,⁸ on U.S.-based infected devices:

a.



prevent the Flax Typhoon actors from accessing the C2 servers and issuing commands;

⁸ These other C2 servers are located outside of the United States, and, therefore the FBI is not seeking authorization from this Court to interact with those servers.

- b. send a native malware command to the C2 servers to provide a list of infected devices controlled by the C2 servers, as well as additional non-content information about each device;
- c. send native malware commands through the C2 servers to the malware on specified infected devices identified through the method described in paragraph 32(b), or through similar actions using overseas C2 servers, which will identify and end one or more malicious botnet-related computer processes;
- d. [REDACTED] terminate the communication channel between the C2 servers and any infected devices;
- e. [REDACTED] seize any information stored on such C2 servers;
and
- f. render the C2 servers inoperable [REDACTED]
[REDACTED]

33. For the search and seizure activities described in the above paragraphs, the FBI will interact only with devices infected with this specific variant of the Mirai malware controlled by Flax Typhoon actors, as well as the C2 servers that control those infected devices. Any device or server that is not part of this specific botnet will not be affected by these commands. The FBI will not otherwise affect the C2 servers or the infected devices, except as provided in paragraph 32 of this affidavit.

TIME OF EXECUTION

34. The FBI requests that the Court authorize the government to repeat the above-described actions during a period of 14 days. The FBI requests that the Court authorize the government to execute the warrant at any time in the day or night, to reduce the chance that the

Flax Typhoon hackers will detect the FBI's actions and deploy countermeasures to frustrate the warrant.

REQUEST FOR SEALING AND DELAYED NOTICE

35. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to seal this application and warrant, as well as the return to the warrant, and to delay the service of the warrant for up to 30 days after execution of the warrant. Pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), delayed notice of the execution of a search warrant is permitted if three requirements are satisfied: (1) the Court finds reasonable cause to believe that providing immediate notification may have an adverse result, as defined in 18 U.S.C. § 2705; (2) the warrant does not allow the seizure of tangible property, wire or electronic communication, or stored wire or electronic information (unless the Court finds reasonable necessity for the seizure); and (3) the warrant provides for the giving of such notice within a reasonable period after execution, not to exceed 30 days unless the facts of the case justify a longer period. 18 U.S.C. § 3103a(b)(1)-(3). An "adverse result" includes a list of factors including "destruction of or tampering with evidence." 18 U.S.C. § 2705(a)(2).

36. Here, the facts justify a delay of up to 30 days because it may take multiple weeks to remediate the malware. Premature disclosure to the public at large or to individual subscribers could give the Flax Typhoon hackers the opportunity to make changes to the malware, enabling continued or additional damage to victims' devices.

37. When notice is no longer delayed, the United States intends to provide notice under Federal Rule of Criminal Procedure 41(f)(1)(C), explaining that:

For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be

accomplished by any means, including electronic means, reasonably calculated to reach that person.

38. The FBI will provide notice to each internet service provider (ISP) that hosts the U.S.-based IP address of the affected device or server, which will ask the ISP to provide notice those customers. For each of these notices, the FBI will attach a copy of the requested warrant and receipt. The FBI will also issue a public notice on its official website (www.fbi.gov) that the FBI conducted the operation. The Department of Justice will issue a similar notice on its official website (www.justice.gov). I believe that this combination of methods is reasonably calculated to reach those persons entitled to service of a copy of the warrant and receipt.

CONCLUSION

39. I submit that this affidavit supports probable cause for a warrant to remotely search the U.S.-based devices and U.S.-based C2 servers identified in Attachment A, and to seize the information described in Attachment B.

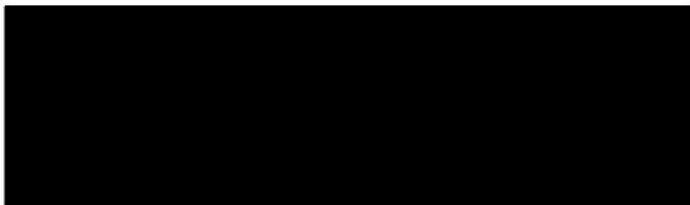
The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,



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 9th day of September, 2024.



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

This warrant applies to U.S.-based devices infected with a specific variant of Mirai botnet malware and to U.S.-based C2 servers controlling infected devices.

The U.S.-based C2 servers controlling devices infected with this specific variant of the Mirai botnet malware are identified below:

23.236.68.193
37.9.35.89
91.216.190.154
91.216.190.247
91.216.190.74
92.38.185.43
92.38.185.44
92.38.185.45
92.38.185.46
92.38.185.47

This warrant also applies to additional U.S.-based C2 servers that may be identified [REDACTED]

[REDACTED]

The FBI will identify the U.S.-based infected devices by sending a command to C2 servers controlling infected devices, including overseas C2 servers, which will provide IP addresses and other non-content information about those infected devices.

ATTACHMENT B

This warrant authorizes the remote access and search of the U.S.-based infected devices and U.S.-based C2 servers identified in Attachment A, and the seizure of data, as the evidence and instrumentalities of computer fraud and conspiracy in violation of 18 U.S.C. §§ 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy), by taking one or more of the following actions:

- a. [REDACTED] prevent the Flax Typhoon actors from accessing the C2 servers and issuing commands;
- b. send a native malware command to the C2 servers to provide a list of infected devices controlled by the C2 servers, as well as additional non-content information about each device;
- c. send native malware commands through the C2 servers to the malware on specified infected devices identified through the method described in paragraph (b), or through similar actions using overseas C2 servers, which will identify and end one or more malicious botnet-related computer processes;
- d. [REDACTED] terminate the communication channel between the C2 servers and any infected devices;
- e. [REDACTED] seize any information stored on such C2 servers; and
- f. render the C2 servers inoperable [REDACTED]
[REDACTED]

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 information.