IN THE MATTER OF THE SEARCH AND SEIZURE OF COMPUTERS IN THE UNITED STATES INFECTED WITH PLUGX MALWARE	Mag. No. 24-mj-1387 **(UNDER SEAL)**

AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A NINTH SEARCH AND SEIZURE WARRANT

I, ▮▮▮▮▮▮▮▮▮, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1.   The FBI is investigating a malicious software known as PlugX, which has been observed by the FBI since at least 2012, and which has infected thousands of Windows-based computers worldwide, including computers in the Eastern District of Pennsylvania. Hackers use PlugX malware to remotely access and execute commands on infected computers. For example, PlugX allows hackers to steal ("exfiltrate") files and other information stored on the infected computers. There is probable cause to believe that the particular variant of PlugX malware described herein is being deployed by China-based state-sponsored hackers known as Mustang Panda and/or Twill Typhoon against, among other devices, U.S.-based computers.

2.   The FBI will identify U.S.-based computers infected with the variant of PlugX malware, as described in Attachment A (the "**TARGET DEVICES**"). The FBI seeks authorization under Federal Rule of Criminal Procedure 41(b)(6)(B) to remotely search the **TARGET DEVICES** and seize the evidence and instrumentalities of the hackers' criminal offenses, as described in Attachment B. As part of this search and seizure, PlugX malware will be deleted from the **TARGET DEVICES**.

AGENT BACKGROUND

3.   I am a Special Agent with the FBI. I am currently assigned to a national security cyber squad in the FBI Philadelphia Field Office, where I investigate a wide variety of computer-related offenses, including computer intrusions. I have received specialized training in the investigation of computer-related offenses, and have substantial day-to-day experience in these investigations, both as the case agent in charge of the investigation and as a member of the investigative team.

4.   I am an "investigative or 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 of and to make arrests for offenses alleged in this affidavit.

5.   The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other FBI agents, analysts, and computer scientists. 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. Where I assert that an event took place on a particular date or at a particular time, I am asserting that it took place on or about the date or at or near the time asserted.

6.   As set forth below, there is probable cause to believe that the malware on the **TARGET DEVICES** constitutes evidence and instrumentality of violations of 18 U.S.C. § 1030(a)(5)(A) (damage to protected computers).

LEGAL AUTHORITY

7.   Title 18, United States Code, Section 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.   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."

PROBABLE CAUSE

9.   This variant of PlugX malware spreads through a computer's USB port, infecting

attached USB devices, and then potentially spreading to other Windows-based computers that the

USB device is later plugged into. Once it has infected the victim computer, the malware remains

on the machine (maintains persistence), in part by creating registry keys which automatically run

the PlugX application when the computer is started. Owners of computers infected by PlugX

malware are typically unaware of the infection.

10.   When a computer infected with this variant of PlugX malware is connected to the

internet, the PlugX malware can send a request to communicate with a command-and-control

("C2") server, whose IP address[1] is hard-coded in the malware. In reply, the C2 server can send several possible commands to the PlugX malware on the victim computer.

11.   Commands that can be remotely issued from the C2 server to the victim computer include a request for information about the victim computer (e.g., its IP address), file system exploration on the infected computer, and uploading, downloading, moving, and deleting files on the infected computer. Based on my training and experience, I know that these functionalities allow the controller of the C2 server to identify a targeted victim, and then collect and stage the victim's computer files for exfiltration.

12.   China-based state-sponsored hackers have been using PlugX malware since at least 2014. This group of computer hackers is known by cybersecurity researchers as Mustang Panda and Twill Typhoon. The FBI assesses that Mustang Panda takes payment from the Chinese government in exchange for providing malware, including PlugX, and other computer intrusion services. The FBI's multi-year investigation of Mustang Panda has confirmed that this group of computer hackers has infiltrated the computer systems of numerous government and private organizations, including in the United States. Significant foreign targets include European shipping companies in 2024, several European Governments from 2021 to 2023, ███████████████ ████████████ worldwide Chinese dissident groups, and governments throughout the Indo-Pacific (e.g., Taiwan, Hong Kong, Japan, South Korea, Mongolia, India, Myanmar, Indonesia, Philippines, Thailand, Vietnam, and Pakistan).

---

[1] Based on my training and experience, I know that an internet protocol address (IP address) is a unique numeric address used by computers on the internet. An IP address is a series of numbers separated by periods (e.g., 45.142.166.112). A computer attached to the internet is assigned an IP address so that internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address can also be used to determine, within limits, the physical location of a computer.

13.   The FBI has assessed that Mustang Panda is the user of this variant of PlugX malware, and that this variant is hard-coded to use the C2 server assigned IP address 45.142.166.112. Since September 2023, at least 45,000 IP addresses in the United States have contacted the C2 server assigned IP address 45.142.166.112. Based on my training and experience, I believe that many or all of these contacts represent an attempt to communicate with the C2 server by PlugX malware on an infected U.S.-based computer.

14.   Unauthorized infections of U.S.-based internet-connected computers are violations of 18 U.S.C. § 1030(a)(5)(A) (damage to protected computers). The FBI's investigation has confirmed that U.S.-based computers infected with this variant of PlugX malware (the "**TARGET DEVICES**") are associated with IP addresses that resolve to more than five federal districts, including the Eastern District of Pennsylvania.

15.   Based on my training and experience, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(5)(A) (damage to a protected computer) have been committed in the Eastern District of Philadelphia and more than four other federal districts.

MANNER OF EXECUTION

16.   A French law enforcement agency has gained access to the C2 server assigned IP address 45.142.166.112. This C2 server can send commands to computers infected with the variant of PlugX malware hard-coded to communicate with the C2 server's assigned IP address, 45.142.166.112.

17.   This PlugX malware variant's native functionality includes a command from a C2 server to "self-delete." This command will tell the PlugX malware on a victim computer to:

    a. delete the files created by the PlugX malware on the victim computer,

b.   delete the PlugX registry keys used to automatically run the PlugX application when the victim computer is started,

c.   create a temporary script file to delete the PlugX application after it is stopped,

d.   stop the PlugX application, and

e.   run the temporary file to delete the PlugX application, delete the directory created on the victim computer by the PlugX malware to store the PlugX files, and delete the temporary file from the victim computer.

18.   The FBI has tested this self-delete command and has confirmed that it does not affect any legitimate functions or files on the **TARGET DEVICES** nor transmit any content information from the **TARGET DEVICES**.

19.   Working with the French law enforcement agency, the FBI can send the self-delete command to the **TARGET DEVICES** infected with this variant of PlugX malware.

20.   When computers infected with PlugX malware communicate with the C2 server at the IP address 45.142.166.112, during the time period authorized by this warrant, the FBI (working with the French law enforcement agency) can identify the U.S.-based **TARGET DEVICES** by sending a command from the C2 server using the PlugX malware's native functionality, requesting each infected computer's IP address. Then, the FBI (working with the French law enforcement agency) will send a command from the C2 server through the PlugX malware to self-delete the software from each U.S.-based **TARGET DEVICE**.

21.   The self-delete command from the C2 server will only affect U.S.-based **TARGET DEVICES**, because only PlugX malware on U.S.-based **TARGET DEVICES** will receive the command from the C2 server to self-delete.

22.   Based on my training and experience, I believe there is probable cause to search the **TARGET DEVICES**, as described in Attachment A, and seize the evidence and instrumentality

of 18 U.S.C. §1030(a)(5)(A), namely the PlugX malware. The FBI seeks authorization under Federal Rule of Criminal Procedure 41(b)(6)(B) to remotely search the **TARGET DEVICES** and seize the unauthorized malware, as described in Attachment B.

23.   This application does not seek authorization to collect content information from the infected computers, nor does it seek authorization to alter the infected computers' operating systems, files, or software, except as expressly provided in Attachment B.

TIME OF EXECUTION

24.   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, so that the FBI can send commands to the **TARGET DEVICES** whenever they communicate with the C2 server at the IP address 45.142.166.112.

REQUEST FOR SEALING AND DELAYED NOTICE

25.   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 until January 11, 2025.

26.   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).

27.   Here, the facts justify a delay of up to January 11, 2025, because it may take multiple weeks to remediate the malware. Premature disclosure to the public at large or to individual owners of the **TARGET DEVICES** could result in publicity that would then give the hackers the opportunity to make changes to the malware, enabling continued or additional damage to remaining victims' devices.

28.   In addition, I request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation by, among other things, allowing the hackers the opportunity to make changes to the malware, enabling continued or additional damage to remaining victims' devices.

29.   When notice is no longer delayed, the United States intends to provide notice under Federal Rule of Criminal Procedure 41(f)(1)(C), which states 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.

30.   The FBI will provide notice to the internet service provider (ISP) that hosts the IP address for the victim, and the notice asks the ISP to provide notice to 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,

to further alert the victims. The Department of Justice will issue a similar notice on its officialwebsite (www.justice.gov). This combination of methods is reasonably calculated to reach those persons entitled to service of a copy of the warrant and receipt.

32.   The requested warrant was previously issued on August 28, 2024 and has been reissued on a rolling basis since then. The FBI has counted the daily number of TARGET DEVICES that communicated with the C2 server and were sent the command to self-delete the PlugX malware. As of December 17, 2024, the self-delete command has been sent to thousands of unique IP addresses, with a consistent rate of disinfection. The FBI has probable cause to believe that there are still numerous U.S.-based computers infected with this variant of PlugX malware. The FBI therefore requests another warrant for a period of 14 days.
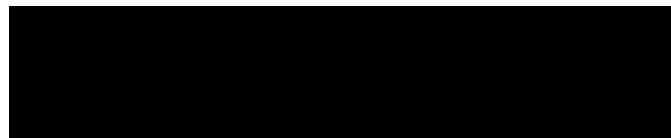
CONCLUSION

31.   I submit that this affidavit supports probable cause for a warrant to remotely search the computers identified using the method in Attachment A, and to seize the information described in Attachment B.

Respectfully submitted,

███████████

████████████████

Federal Bureau of Investigation

Subscribed and sworn to by telephone in accordance with Federal Rules of Criminal Procedure 4.1 and 41(d)(3) this day 20th of December, 2024.

████████████████████████

United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to U.S.-based computers infected with a variant of PlugX malware whose C2 server is assigned IP address 45.142.166.112 ("**TARGET DEVICES**"), and which will be identified when they request contact from the C2 server, and respond to a command sent from the C2 server for their IP addresses and other non-content information.

ATTACHMENT B

Particular Things to be Seized

This warrant authorizes the remote access and search of the **TARGET DEVICES** identified using the method in Attachment A, and the seizure of data from the **TARGET DEVICES**, as the evidence and instrumentality of unauthorized computer intrusion in violation of 18 U.S.C. § 1030(a)(5)(A) (damage to a protected computer). This warrant authorizes the government to remotely access the **TARGET DEVICES** by issuing a command through the PlugX malware to:

    a. delete the files created by the PlugX malware on the victim computer,

    b. delete the PlugX registry keys used to automatically run the PlugX application when the victim computer is started,

    c. create a temporary script file to delete the PlugX application after it is stopped,

    d. stop the PlugX application, and

    e. run the temporary file to delete the PlugX application, delete the directory created on the victim computer by the PlugX malware to store the PlugX files, and delete the temporary file from the victim computer.

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 **TARGET DEVICES** identified using the method in Attachment A.