DMP:ICR
F. #2018R01363

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH COMPUTERS CONSTITUTING THE SNAKE MALWARE NETWORK	APPLICATION FOR SEARCH WARRANT Docket No. 23-MJ-0428 (CLP)

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, TAYLOR FORRY, a Special Agent of the Federal Bureau of Investigation ("FBI"), having been duly sworn, hereby depose and state as follows:

INTRODUCTION

1. As detailed below, the FBI and the United States Attorney's Office for the Eastern District of New York have been investigating unauthorized computer intrusions perpetrated as part of a long-running cyberespionage campaign by officers assigned to a unit within Center 16 of the Federal Security Service of the Russian Federation (Федеральная Служба Безопасности) which is commonly referred to by its Russian acronym as the "FSB." Public security researchers have also tracked the cyber activities of the FSB and often attribute the cyberespionage activities discussed below to a threat actor that they have publicly identified by various names, including "Turla," "Krypton," "Boulder Bear," "Venomous Bear," "Agent.btz.," "Uroburos," "Waterbug," "Snake," "Tavdig/Wipbot," "Epic Turla," and "Carbon". In this Affidavit, I will generally refer to the FSB unit perpetrating these schemes as "Turla."

2. As early as 2004, Turla has made extensive use of numerous versions of sophisticated malicious software ("malware") that Turla has named "Uroburos" and later, "Snake" (hereinafter "Snake"). Using Snake, Turla actors have compromised computer systems throughout the United States and the world, in the process creating and controlling a covert peer-to-peer network of Snake-compromised computers, which is referred to in this Affidavit as the "Snake network." Turla uses the Snake network to identify, collect, and exfiltrate to the Russian Federation information of value to the Russian Intelligence Services. To conceal this activity, Turla actors transmit commands to, and exfiltrate data from individual Snake endpoints through the Snake network itself, thus disguising malicious activity in ostensibly innocuous network traffic between a series of Snake-compromised hop points.

3. FBI agents, analysts, and computer scientists (collectively "FBI personnel") have identified certain IP addresses of victim computers worldwide, including the U.S.-based computers identified in Attachment A ("Subject Computers"), which have been compromised by Snake and constitute a part of the global Snake network. FBI personnel have obtained physical access to some of the compromised computers through consent of their owners and have developed the capability, detailed herein, to remotely access and control the Snake malware on the Subject Computers. FBI personnel now seek authorization to electronically connect to Snake malware on the Subject Computers identified in Attachment A and issue commands to the Snake malware to permanently disable Snake on the Subject Computers. Through these actions, the FBI will neutralize Turla's ability to further access the Snake malware currently installed on the Subject Computers through technical means described in further detail below.

4. Therefore, I make this affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41(b)(6)(B) to use a remote access technique to search certain computers located in the United States, further identified in Attachment A, and to seize electronically stored information that constitutes evidence and/or instrumentalities of unauthorized access and damage, further described in Attachment B.

5. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agents. 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.

6. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy) ("Subject Offenses") have been committed in the Eastern District of New York and elsewhere. There also is probable cause to search the information described in Attachment A for evidence, contraband, fruits, and/or instrumentalities of the Subject Offenses, further described in Attachment B.

AGENT BACKGROUND

7. I have been a Special Agent of the FBI since 2012, and I am currently assigned to the Cyber Division of the New York Field Office where I am primarily responsible for the investigation of computer intrusions conducted by nation-state sponsored and directed hackers. I have extensive training and experience in the investigation of computer intrusions, and the tactics, techniques, and procedures used by nation-state hackers for cyberespionage,

including the analysis of malware used by nation-state hackers to compromise computers, exfiltrate user data, and conceal their activities from law enforcement and intelligence authorities. I have a Master's Degree in Cybersecurity. I have also received specialized training from the FBI in the investigation of computer intrusions and nation-state cyberespionage. I have also directly participated in numerous investigations of nation-state cyberespionage campaigns, including the investigation described below, in the course of which I have made extensive use of court-authorized legal process.

PREMISES TO BE SEARCHED

8. As more fully detailed below, there is probable cause to believe that the computers connected to the Internet from the following Internet Protocol ("IP") addresses located in the United States have been compromised by the FSB using Snake and thus, that evidence, fruits, and instrumentalities of the Subject Offenses will be found in the data stored on the Subject Computers identified below and in Attachment A:

Subject Computer	**IP Addresses**	**Location**	**Judicial District**
Subject Computer-1	[redacted]	Portland, Oregon	District of Oregon
Subject Computer-2		Columbia, South Carolina	District of South Carolina
Subject Computer-3		Columbia, South Carolina	District of South Carolina
Subject Computer-4		Atlanta, Georgia	Northern District of Georgia
Subject Computer-5		Windsor, Connecticut	District of Connecticut
Subject Computer-6		Rancho Cordova, California	Eastern District of California

Subject Computer	IP Addresses	Location	Judicial District
Subject Computer-7	[redacted]	Rancho Cordova, California	Eastern District of California
Subject Computer-8		Rancho Cordova, California	Eastern District of California

AUTHORITY

9. Federal Rule of Criminal Procedure 41(b)(6)(B) 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."

10. 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 as provided in subsection (c) of this section." 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[.]"

11. As detailed in this Affidavit, there is probable cause to believe that activities related to a crime may have occurred in the Eastern District of New York, this search warrant is sought in an investigation of a violation of 18 U.S.C. § 1030(a)(5), and there is probable cause to believe that the Subject Computers are "protected computers" "that have been damaged without authorization and are located in five or more districts".

PROBABLE CAUSE

I. Background on Snake and Turla's Use of the Snake Network for Espionage

12. As detailed herein, the advanced persistent threat group known by many names, including Turla, is comprised of officers of the FSB's Center 16. The FSB is the Russian Federation's principal security force, and the primary successor to the former Soviet Union's Committee for State Security (known by its Russian acronym as the "KGB"), with responsibilities for counterintelligence, internal and border security, counterterrorism, and signals intelligence, among others. Center 16 of the FSB was created in 2003 after the Russian government dissolved the former Federal Agency of Government Communication and Information, and transferred the functions of that agency's Third Chief Directorate to the FSB. FSB Center 16 is primarily responsible for the FSB's collection of signals intelligence.

13. The FSB began developing the Snake malware under the name "Uroburos" in late 2003. Development of the initial versions of the implant appeared to be

completed around early 2004, with cyber operations first conducted using the implant shortly thereafter. The name Uroburos is appropriate, as the FSB cycled it through nearly constant stages of upgrade and redevelopment, even after earlier versions of the malware were publicly disclosed, instead of abandoning it. The name appears throughout early versions of the code, in which the FSB developers also left other unique strings, including "Ur0bUr()sGoTyOu#".

14. Unique features in early versions of Uroburos included a low resolution image of a historical illustration of an uroboros by the German philosopher and theologian Jakob Böhme. For example, Turla would often place a redundant backdoor on an endpoint compromised by early versions of Uroburos that used this image as the key, and the same image has also been embedded in other Snake-related components. The image, blown up to a higher resolution, is shown below.

15. In addition, early FSB developers of the Snake malware left portions of unique code throughout the malware which reveal inside jokes, personal interests, and taunts directed at security researchers, all of which have assisted the U.S. government in attributing the

Snake malware to the FSB. For instance, the "Ur0bUr()sGoTyOu#" string referenced above was replaced with "gLASs D1cK" in 2014 following public cybersecurity reporting on Uroburos.

16. Snake malware operations are attributable to a known unit within Center 16 of the FSB, which I will refer to herein as "Turla".[1] This unit more broadly operates the numerous elements of the Turla malware toolset, and has sub-units spread throughout Russia, reflecting the Soviet Union's historical KGB signals intelligence operations to which the FSB is the KGB's modern-day successor. Snake has been a core component of this unit's operations for almost as long as Center 16 has been part of the FSB. The extensive influence of Snake across the Turla toolset demonstrates its impact on practically every aspect of the unit's modern era of cyber operations.

17. The U.S. government has monitored FSB officers assigned to Turla conducting daily operations using Snake from a known FSB facility in Ryazan, Russia, with an increase in Snake activity during FSB working hours in Ryazan, between approximately 7:00 AM to 8:00 PM, Moscow Standard Time (GMT+3). Snake's main developers were Ryazan-based FSB officers known by monikers that were included in the code of some versions of Snake. In addition to developing Snake, Ryazan-based FSB officers assigned to Turla used it to conduct worldwide operations which the FBI and the U.S. intelligence community are able to

[1] The unit identified in this Affidavit as "Turla" is distinct from a separate sister unit within FSB Center 16 to which the FBI has publicly attributed operations of the advanced persistent threat group "Dragonfly." As noted above, Turla is one of many open source terms used to describe the family of malware used by this FSB Center 16 unit. Snake and the broader Turla family have also previously been referenced in private sector reporting using the names Krypton, Venomous Bear, Penquin, Agent.BTZ, ComRAT, Waterbug, Tavdig, Wipbot, Epic Turla, Mosquito, Carbon, and others.

differentiate from other cyberespionage operations attributable to other FSB units launched from Moscow and other FSB sites based on the infrastructure and techniques employed.

18. While the development and re-tooling of Snake has historically been done by Ryazan-based FSB officers, Snake operations were also launched from an FSB Center 16-occupied building in Moscow. The U.S. government has observed some FSB operators using Snake to its full potential, as well as other FSB operators who appeared to be unfamiliar with Snake's more advanced capabilities. These observations serve to illustrate the difficulty in using such an advanced toolset across the various geographically dispersed teams comprising this unit within FSB Center 16.

19. The U.S. government has been investigating Snake and Snake-related malware tools for nearly 20 years. During that time, the FSB has used Snake in many operations, and the FSB has demonstrated the value it assigns to Snake by making numerous adjustments and revisions to keep it viable after repeated public disclosures and other mitigations. Snake's code and multiple Snake-related malware tools have been either a starting point or a key influence factor for a diverse range of other highly prolific malware implants and operational tools in the Turla malware family. Most notably, this has included "Carbon" (also known as "Cobra")—derived from Snake's code base—and the similarly Snake-adjacent malware implant "Chinch" (currently known in open sources as "ComRAT").

20. Today, Snake is the FSB's premier long-term cyberespionage malware implant. Snake provides its Turla operators numerous features, including the ability to execute arbitrary commands and to load arbitrary additional modules of executable code that allow its operators to add selected malware tools to extend its functionality to meet FSB mission

requirements. Most importantly, the worldwide collection of compromised computers acts as a covert peer-to-peer network, which utilizes customized communication protocols designed to hamper monitoring and collection efforts by adversary signals intelligence services. The majority of compromised systems serve as relay nodes (referred to as "hop points") in the Snake network, that route traffic from the FSB's ultimate target systems (referred to as "endpoints") through the network back to Turla operators in Russia.

21. Snake's Turla operators have not deployed Snake malware widely, but instead have selectively compromised specific computers, limiting the number of computers compromised by Snake to decrease the probability of detection. On those computers that Turla has compromised, the Snake implant persists on the system indefinitely, typically undetected by the machine's owner or authorized users. The FBI has monitored computers that have been compromised by Snake for years at a time, and has observed Snake persist on particular computers despite a victim's efforts to remediate the compromise.

22. Indeed, one common tool deployed with the Snake malware that contributes to its persistence on compromised systems is Snake's "keylogger," a malware tool that records every keystroke made by a computer user. Snake's keylogger enables Snake's Turla operators to steal account authentication credentials, such as usernames and passwords, from legitimate users of the computers compromised by Snake. By stealing authentication credentials for authorized users, Turla operators can use them to fraudulently re-access compromised computers and restore Snake's access to the system even after an attempt has been made to remediate the Snake malware on the compromised computer.

23. As part of the investigation, the FBI, its partners in the U.S. Intelligence Community, together with allied foreign governments, have monitored the FSB's use of the Snake network to exfiltrate data from sensitive computer systems, including those operated by North Atlantic Treaty Organization ("NATO") member governments, by routing the transmission of these data through Snake-compromised computers in the United States. The FBI assesses that Snake's Turla operators often transmit data exfiltrated from Snake endpoints outside of the United States through Snake hop points in the United States to make it more difficult for compromised victims to identify and block suspicious connections to Snake-compromised endpoints, among other reasons. Nevertheless, through existing legal authorities, the cooperation of several U.S. victims and sensitive sources, the FBI and U.S. Intelligence Community have obtained significant insight into the FSB's cyberespionage activities against the United States and its allies using Snake.

24. For example, in or about and between 2015 and 2017, the FBI monitored network communications characteristic of the Snake malware between a known Snake-compromised computer located in the United States and a computer that accesses the Internet from an IP address assigned to the Ministry of Foreign Affairs of a NATO-member state ("NATO Victim-1"). The FBI collected and decrypted communications between the U.S.-based Snake hop point and the NATO Victim-1 Snake endpoint and was able to confirm that Turla operators used Snake in an attempt to exfiltrate a large volume of what they believed to be internal United Nations and NATO documents sent from the NATO Victim-1 computer through the Snake hop point in the United States.

25. As another example, in or about and between 2017 and 2020, the FBI monitored network communications characteristic of the Snake malware between known Snake-compromised computers located in the United States and computers that accessed the Internet from IP addresses assigned to the government of a NATO-member state ("NATO Victim-2"). The payloads transmitted to the Snake hop points located in the United States by the NATO Victim-2 computers were very large and consistent with the attempted bulk theft and exfiltration of data from the NATO Victim-2 computers. The FBI collected and decrypted these communications and was able to confirm that the NATO Victim-2 computers were compromised by Snake and that Snake's Turla operators had issued commands to the Snake malware on the compromised NATO Victim-2 computers consistent with the exfiltration of data.

26. Notably, the FBI has obtained information indicating that Turla has also used Snake malware to target the personal computer of a journalist for a U.S. news media company who has reported on the government of the Russian Federation.

II. Unique Technical Features of the Snake Malware and the Snake Network

27. In the course of the investigation, the FBI has identified numerous computers that have been infected with the Snake malware and has performed technical analysis of the malware found on the Snake-compromised computers. Through this analysis, the FBI has learned that once the Snake malware is installed on a victim computer, Snake uses a sophisticated and custom method to communicate and send commands to other Snake-compromised computers. This analysis has also demonstrated that a computer infected with Snake can only complete a Snake communication session with another computer also infected by Snake.

28. To obfuscate communications between the Snake-compromised computers that comprise the Snake network, the nature of the data stolen by the FSB and the identity of the FSB as the attacker, communications between Snake implants on compromised computers are encrypted, fragmented, and sent using customized methodologies built atop common network protocols. As a result, Snake communications are difficult to distinguish from legitimate victim network traffic, and the data payloads are impossible to decrypt and interpret without software specifically designed to process the implant's custom protocols.

29. Turla developers have designed Snake implants to communicate with one another using two primary customized communications protocols that are based on and closely resemble communications protocols commonly used by legitimate network traffic. Both of these protocols are built on top of the Transmission Control Protocol ("TCP") which is built on top of the Internet Protocol ("IP").

30. TCP is one of the main protocols, or standardized languages, that computers use to communicate with one another over the Internet. TCP is used to move packets of data through networks reliably, using mechanisms such as automatic retransmission of dropped or damaged packets. TCP packets are comprised of a header section and a data section. The data contains the actual content that the sender is transmitting to the recipient. The header contains metadata information, including the source and destination port and further state-related information to the TCP session. TCP is connection-oriented, in that the two communicating computers establish a session prior to sending any data and maintain this session throughout the exchange. Sessions facilitate the reliability guarantees of TCP, ensuring that the data can be reassembled in its proper order by the receiving computer even in the presence of network

connectivity issues, including packets that are dropped and must be retransmitted, packets that arrive out of order, and other common occurrences on a busy network.

31. Major internet applications, such as the World Wide Web, email, remote administration, and file transfers rely on TCP. In order to initiate a connection, the receiving computer must be listening on the port specified by the initiating computer. A new TCP session is established through a three-step "handshake," signifying that both computers are connected and ready to share communication data. In a typical TCP session, the operating system kernel, i.e., the computer program at the core of every computer's operating system, collects the packets received from the sending computer and forwards them for processing by the application listening on the specified port.

32. In a computer that is compromised by Snake and used to facilitate the operation of the Snake network, however, the Snake malware inserts itself into the kernel's processing of every TCP packet. To allow the Snake network to function, each installation of the Snake malware on a particular computer (an "implant") comes with a file (referred to herein as the "Queue File") that includes, among other things, a list of typically four, but as many as ten, other IP addresses identifying other hop points and/or endpoints in the Snake network, i.e., other computers that have been compromised by Snake. The Queue File contains implant-specific authentication codes for the Snake implant on each compromised computer. The Snake malware is designed to send the authentication code for the Snake implant on a particular computer in the TCP packets sent to that computer. The Snake malware is designed to listen for its own authentication code in the TCP packets sent to its host computer, and to then intercept Snake-

authenticated network traffic that contains embedded communications from other Snake implants.

33. Specifically, in a computer compromised by Snake, Snake's kernel component will intercept all TCP packets sent to the host computer. Snake's kernel component examines the first packet received after the TCP handshake to determine if it contains the Snake authentication code unique to the implant receiving the communication. If Snake determines the packet to be a valid communication from another Snake implant, it will forward all subsequent traffic in the TCP session to Snake's internal processing code. When this occurs, the legitimate application listening on the port to which the Snake communication was sent will have no knowledge of the communication. On the other hand, if the initial TCP packet does not contain the appropriate authentication code, then Snake's kernel will allow the data to pass through to the application listening on the specified port. Thus, in order for the Snake implant on a particular computer to recognize a particular communication—such as a command from Snake's Turla operators, or the transfer of data exfiltrated from another victim—as originating from Snake malware on another Snake-compromised computer, the authentication code must be included in the packet sent to the host computer.

34. Snake's TCP traffic interception technique helps to conceal the existence of the Snake malware on its host computer and enables Snake implants on two computers to communicate without detection by ordinary intrusion detection and firewall security products, which typically look for network traffic directed to an unexpected port.

35. To conceal the content of authenticated communications between Snake implants, Snake encrypts communications with other Snake implants using a cryptographic key

unique to each communication's session that is derived from Turla's custom-designed session key establishment protocol. This custom protocol relies, in part, on randomization and a pre-shared key that is also contained within the Queue File. In contrast, communications between computers on the Internet are typically encrypted using one of a set of standardized protocols, such as those supported by the Secure Sockets Layer ("SSL") suite, which do not require computers to have shared a cryptographic key in advance. Thus, to read a communication between Snake implants requires knowledge of Snake's custom session key establishment protocol, the pre-shared cryptographic key from the Queue File, and the computational power to calculate an unknown random number used to create the session key.

36. To this session-encryption protocol, Turla developers have added a further level of encryption that serves to further secure Snake communications from detection and interception. Turla developers have designed Snake's command communications to be separately end-to-end encrypted, such that a command sent from one Snake implant that is transmitted through separate intermediary Snake hop points, can only be decrypted by the specific Snake hop point or endpoint that will execute the command. The Snake malware also implements this separate "command layer" encryption using a separate cryptographic key pair, one half of which is also contained within the Queue File.

37. Notably, Turla developers have designed Snake malware to execute standard commands that Turla operators can use to remotely reconfigure aspects of a particular Snake implant. These commands include but are not limited to the following: (i) reading or deleting log files; (ii) updating configuration information to, among other things, enable the Snake implant to communicate with Snake implants on newly compromised systems; (iii)

loading and unloading modules allowing the use of particular malware tools; and (iv) reading and writing data to the Queue File.

38. In transmitting the authentication code and establishing a secure session with another Snake implant, the Snake malware typically chooses to use one of two primary transportation protocols that have been further customized by Turla developers to conceal Snake-specific communications within innocuous network traffic. Snake typically uses a Turla-customized version of Hypertext Transport Protocol ("HTTP"), the protocol used by websites, which I will refer to herein as "Snake-HTTP", or a Turla-customized TCP protocol, which I will refer to herein as "Snake-TCP".[2]

39. The FBI has observed that Turla typically uses Snake-TCP to facilitate communications between multiple Snake-compromised computers on the same local network, while Turla typically uses Snake-HTTP to facilitate communications between Snake-compromised computers across the Internet. Turla's customized Snake-HTTP is designed to blend in with Internet traffic, most of which is transmitted using HTTP, and since at least 2017, Turla has primarily encoded binary information in Snake-HTTP packets using Base 62, instead of Base 64, which is used to encode most HTTP packets. Thus, Snake-HTTP packets cannot be decoded from text into the underlying binary information using conventional Base 64-

[2] As detailed above, TCP is a protocol for managing the transmission of data between computers, while HTTP is one of the protocols used to describe the data that can be contained in a TCP packet. Thus, the components of an HTTP packet, which like TCP packets include header and data components, exist within the data component of a TCP packet. In certain applications, TCP itself can also be used to describe the data contained in a TCP packet, including, as discussed herein, in the context of communications related to computer systems management.

methodologies. The FBI assesses that Turla's Snake developers designed Snake-HTTP to use Base 62 in order to further protect Snake's communications from interception and decoding by adversary signals intelligence services.

40. Critically, Turla has customized Snake-HTTP to implement session maintenance, meaning that, unlike ordinary HTTP, Snake-HTTP is designed to permit the Snake implant to treat multiple HTTP packets as part of a single session encrypted using the session key establishment protocol discussed above. To do this however, Turla's customized Snake-HTTP embeds a common 8-byte metadata structure into every Snake-HTTP packet. Turla's unique implementation of HTTP operates as a kind of signature, with the 8-byte metadata component of the Snake-HTTP packet incrementing in a predictable fashion. Accordingly, by observing as few as two or three packets of HTTP, the FBI has learned to identify computers that are communicating using Turla's Snake-HTTP and can infer from this behavior that Snake implants on the two computers have authenticated themselves as Snake malware.

III. The FBI's Use of Snake Network Traffic to Identify Snake Hop Points and Endpoints

41. Over several years, the FBI has created and refined advanced customized tools designed to distinguish, decrypt, and interpret Snake network traffic, as well as attack Snake communication protocols. As a result of this work, the FBI is able to identify network traffic that is characteristic of the Snake network, and thus to identify individual computers compromised by Snake. As a further result of this work, the FBI has developed the ability, discussed below, to issue commands to the Snake malware on Snake-compromised computers.

42. The FBI has identified numerous victims of the Snake malware both domestically and abroad. There is no legitimate purpose for the installation of the Snake

malware on victim computers, and the victim owners and authorized users of Snake-compromised computers are typically unaware that their computers have been compromised by the Snake malware until the FBI contacts them. Even on computers that are used primarily as hop points for the exfiltration of data stolen from Snake endpoints, Turla uses Snake's keylogger to steal account authentication credentials from authorized users. Thus, any computer running Snake malware is a result of Turla's unauthorized access to and intrusion on the computer, and has suffered damage as a result of or in furtherance of that unauthorized access.

43. The FBI has determined that the FSB has used the Snake malware package to compromise hundreds of computers in at least 50 countries worldwide. The FBI has been able to identify specific victims through various methods, including, as noted below, tracking connections from known compromised computers. U.S. Victims-A through -G, discussed below, offer an illustrative sample of past and present victims whose computers have been compromised by Snake.

44. In or about 2016, the FBI found an IP address in the Queue File of the Snake implant on a Snake-compromised computer that was later identified as belonging to an entity described herein as "U.S. Victim-A". Upon notification by the FBI that U.S. Victim-A was likely compromised by malware, U.S. Victim-A voluntarily permitted the FBI to use custom software to scan the identified computers for Snake. Scans of certain computers belonging to U.S. Victim-A in San Jose, California, in the Northern District of California, confirmed that they were compromised by Snake. The FBI subsequently obtained U.S. Victim-A's consent to monitor the identified Snake-compromised computers in order to identify other hop points and endpoints, and thus other victims, in the Snake network.

45. In or about 2018, the FBI observed network communications characteristic of the Snake malware between Snake-compromised computers belonging to U.S. Victim-A and computers located in Syracuse, New York, in the Northern District of New York, which belonged to an entity identified herein as "U.S. Victim-B". The FBI notified U.S. Victim-B that several of U.S. Victim-B's computers were likely infected with malware and obtained U.S. Victim-B's consent to perform customized malware scans of the identified computers. The scans confirmed the presence of Snake malware on U.S. Victim-B's computers, and the FBI subsequently obtained U.S. Victim-B's consent to monitor the identified Snake-compromised computers in order to identify other victims in the Snake network.

46. In or about January 2020, the FBI observed network communications characteristic of the Snake malware between Snake-compromised computers belonging to U.S. Victim-B and a computer connected to the Internet at an IP address hosted by a U.S. cloud service provider on a server located in Boardman, Oregon, in the District of Oregon, for a customer identified herein as "U.S. Victim-C." The FBI contacted U.S. Victim-C, was able to confirm the presence of Snake malware on the computer, and obtained U.S. Victim-C's consent to monitor the identified Snake-compromised computer in order to identify other victims in the Snake network.

47. In or about and between 2018 and 2022, the FBI observed network communications characteristic of the Snake malware between Snake-compromised computers belonging to, among others, U.S. Victim-A and U.S. Victim-B, and computers located in Columbia, South Carolina, in the District of South Carolina belonging to an entity identified herein as "U.S. Victim-D." The FBI notified U.S. Victim-D that several of U.S. Victim-D's

computers were likely infected with malware and obtained U.S. Victim-D's consent to perform customized malware scans of the identified computers. The scans confirmed the presence of Snake malware on U.S. Victim-D's computers, and the FBI subsequently obtained U.S. Victim-D's consent to monitor the identified Snake-compromised computers in order to identify other victims in the Snake network.

48. In or about and between 2021 and 2022, the FBI observed network communications characteristic of the Snake malware between Snake-compromised computers belonging to U.S. Victim-D and computers located in Van Nuys, California, in the Central District of California, and which belonged to an entity identified herein as "U.S. Victim-E." The FBI had previously provided victim notification to U.S. Victim-E after obtaining evidence in or about 2017 that one of U.S. Victim-E's computers had been compromised by Snake malware, and had been able to confirm the presence of an earlier version of Snake on U.S. Victim-E's computer after U.S. Victim-E consented to a customized malware scan. U.S. Victim-E, however, declined to permit the FBI to monitor its computers in order to identify other victims in the Snake network.

49. Notably, in or about and between 2020 and 2021, the FBI observed network communications characteristic of the Snake malware between a Snake-compromised computer belonging to U.S. Victim-A and a computer located in Hicksville, New York, in the Eastern District of New York, which belonged to an entity identified herein as "U.S. Victim-F." The FBI notified U.S. Victim-F of the likely presence of malware on its computer in or about 2022, however, U.S. Victim-F had ceased operations and had discarded the Snake-compromised computer.

50. As a final example, in or about and between February and March 2022, the FBI observed network communications characteristic of the Snake malware between Snake-compromised computers belonging to U.S. Victim-A and a computer connected to the Internet at an IP address hosted by a U.S. cloud service provider on a server located in Gaithersburg, Maryland, in the District of Maryland, for a customer identified herein as "U.S. Victim-G." The FBI notified U.S. Victim-G of the likely presence of malware on its computer, however, U.S. Victim-G ultimately refused to cooperate with the FBI's investigation.

IV. Evidence of the Snake Malware on the Subject Computers

51. Through various techniques, including those discussed above, the FBI has observed network communications characteristic of the Snake malware between identified Snake-compromised computers and the Subject Computers. While these custom Snake communications are themselves evidence that the Subject Computers have been compromised by Snake, as detailed below the FBI has developed the capability to remotely test specific computers suspected of being infected, and using that technique has already confirmed that the Subject Computers have been compromised by Snake malware.

52. Specifically, the FBI has created a technique that mimics the beginning of Snake's session authentication protocol, described above, to provoke a suspected Snake implant on another computer to provide a response that is unique to Snake network communications in a communication that is analogous to sending a "ping" to another computer, a method routinely used to test another computer's ability to communicate on an IP network. The FBI has created software named "PERSEUS" that uses this technique. Using PERSEUS, the FBI can send a series of simple TCP packets from an FBI-controlled computer to a computer that is suspected of

being compromised by Snake together with an authentication code that the Snake malware on the compromised computer will read and recognize as authenticating the sender of the TCP packet as being another Snake-compromised computer. In most instances PERSEUS attempts to contact the Snake-suspected computer using Snake-HTTP, in which case these TCP packets comprise an ordinary request to load a webpage. In the remaining instances PERSEUS attempts to contact the Snake-suspected computer using Snake-TCP, in which case these packets comprise simple TCP data transmissions.

53. If the recipient computer is compromised by Snake and the authentication value is correct, then the Snake kernel module intercepts the data packets following the initial TCP handshake, and the underlying data does not reach the legitimate listening application. Instead, Snake responds to the transmitted packets in a unique manner that clearly identifies the computer as compromised by Snake.

54. If the recipient computer is not infected with Snake or the authentication value is incorrect, the computer will pass the transmitted data to the legitimate application listening on that port, which will respond to the transmission as it would to any normal data. In the case of a Snake-HTTP transmission by PERSEUS of a GET request, i.e., a request to load a webpage, that is sent to an HTTP server, the non-compromised computer would provide the requested webpage. In the case of a Snake-TCP transmission by PERSEUS to a computer that was not compromised by Snake, the receiving application would consider the transmitted data to be invalid and thus respond with a message terminating the connection.

55. In either case, the FBI is able, based on its extensive knowledge and understanding of Snake network communications protocols, to easily distinguish the response of

a suspected computer from the narrow scope of valid responses that exist within the custom Snake-HTTP and Snake-TCP protocols. Thus, the FBI can determine that a computer that responds to PERSEUS in a manner consistent with the Snake-HTTP or Snake-TCP protocols is compromised by Snake at the time of the test.

56. The FBI has monitored network communications characteristic of the Snake malware between at least one known Snake-compromised computer and each of the Subject Computers that connect to the Internet from the IP addresses listed in the table below, and located in the judicial district identified below. Further, on the dates indicated, the Snake malware on the Subject Computers listed in the table below responded to a PERSEUS Snake-HTTP or Snake-TCP transmission in a manner confirming the presence of the Snake malware on each of the Subject Computers. Accordingly, there is probable cause to believe that each of the below-identified Subject Computers has been damaged by Turla and that Snake malware is currently present on each of the Subject Computers:

Subject Computer[3]	**IP Addresses**	**Date**	**Location**	**Judicial District**
Subject Computer-1	[redacted]	5/3/2023	Portland, Oregon	District of Oregon
Subject Computer-2		3/3/2023	Columbia, South Carolina	District of South Carolina

[3] The physical machines identified herein and in Attachment A as Subject Computer-7 and Subject Computer-8 connect to the Internet through multiple IP addresses, each of which is listed in this Affidavit and Attachment A. On the dates indicated, the FBI used PERSEUS to confirm that the Snake implants on Subject Computer-7 and Subject Computer-8 were present and have the ability to establish a Snake network connection through each of the IP addresses listed here. In this Affidavit the FBI seeks the authority to execute the remote search technique by establishing a Snake network connection to the Snake implant on Subject Computer-7 and Subject Computer-8 through any of the identified IP addresses.

Subject Computer[3]	IP Addresses	Date	Location	Judicial District
Subject Computer-3	[redacted]	3/3/2023	Columbia, South Carolina	District of South Carolina
Subject Computer-4		3/3/2023	Atlanta, Georgia	Northern District of Georgia
Subject Computer-5		4/21/2023	Windsor, Connecticut	District of Connecticut
Subject Computer-6		4/28/2023	Rancho Cordova, California	Eastern District of California
Subject Computer-7		3/3/2023	Rancho Cordova, California	Eastern District of California
		4/26/2023		
		4/26/2023		
		4/26/2023		
		4/26/2023		
		4/26/2023		
		4/26/2023		
		4/26/2023		
		4/26/2023		
Subject Computer-8		5/3/2023	Rancho Cordova, California	Eastern District of California

V. FBI's Ability to Remediate Snake Implants on the Subject Computers

57. The FBI has developed the capability, using PERSEUS, to impersonate Snake's Turla operators and issue commands to Snake malware that will effectively, and permanently, disable it. Using authentication codes that the FBI has obtained for the Snake implants on the Subject Computers, the FBI can use PERSEUS to complete the full Snake authentication and session establishment protocols, and send commands to the Subject

Computers that the Snake malware on the Subject Computers will interpret as legitimate and execute.

58. Specifically, the FBI has developed a technique that exploits some of Snake's built-in commands, discussed above, which, when transmitted by PERSEUS from an FBI-controlled computer to the Snake malware on the Subject Computers, will terminate the Snake application and, in addition, permanently disable the Snake malware by overwriting vital components of the Snake implant without affecting any legitimate applications or files on the Subject Computers..

59. The FBI has extensively tested this technique and has confirmed both that it is effective at disabling the Snake malware, and that the computer hosting the Snake malware is not adversely affected by this technique. Indeed, in testing, the FBI has confirmed that a computer infected by Snake and remediated through PERSEUS, will continue to function as normal. Notably, the commands transmitted by PERSEUS are sent using the custom communications protocols and encryption developed by Turla for the Snake malware, and thus can be interpreted and executed only by Snake implants. Thus, a computer that is not compromised by Snake could not understand PERSEUS's commands, and would disregard them. Further, and as detailed above, the applied-for warrant would authorize FBI personnel to execute the remote access technique only as to the specific Subject Computers identified in Attachment A that the FBI has already confirmed to be compromised by the Snake malware, thus limiting the scope of the remote search technique to computers currently compromised by Snake malware.

THE SUBJECT PREMISES AND THE REMOTE SEARCH TECHNIQUE

60. As described above, FBI personnel have identified the 19 IP addresses associated with the Subject Computers in the United States, and have developed the capability of impersonating Turla actors to communicate with the Snake malware on the Subject Computers and disable it. In this Affidavit, FBI personnel seek authorization to remotely search the Subject Computers and, through interactions with the Snake malware on the Subject Computers, to permanently disable the Snake malware.

61. On or about May 8, 2023, the FBI, in coordination with certain foreign governments acting outside of the United States, intends to execute a technical operation, codenamed MEDUSA, to disable Snake malware on numerous computers worldwide. Specifically, at a chosen time, FBI personnel will use PERSEUS to authenticate and establish sessions with the Snake malware on the Subject Computers, and send to the Snake implants on the Subject Computers built-in commands that will terminate the Snake application and, in addition, permanently disable the Snake malware by overwriting vital components of the Snake implant without affecting any legitimate applications or files on the Subject Computers. At the same time that the FBI executes the remote search technique described in this Affidavit to disable the Snake malware on computers located in the United States, certain foreign government authorities will take action to remediate Snake-compromised computers within their territories.

62. The FBI believes that use of the remote search technique described in this Affidavit is necessary to ensure the success of the coordinated technical operation to disrupt the Snake malware network worldwide. As detailed above, the Subject Computers are located in geographically disparate locations throughout the United States. There are not sufficient FBI

personnel available who possess the specialized training and experience with the sophisticated Snake malware to physically travel to each location to disable the Snake malware on each of the Subject Computers simultaneously. Thus, without authorization to use the remote search technique requested in this Affidavit, the FBI would not be able to timely disable the Snake malware on the Subject Computers as part of a coordinated operation against the worldwide Snake network.

63. Particularly in light of the sophistication of the Snake malware and the identity of its FSB-employed Turla operators, there is a high risk that uncoordinated action to disable individual Snake implants could provide Turla advance warning of the coordinated operation and a window of opportunity to either further damage or victimize Snake-compromised computers, or take other action to prevent or mitigate the effects of the worldwide operation to disable the Snake network. Indeed, were Turla to become aware of Operation MEDUSA before its successful execution, Turla could use the Snake malware on the Subject Computers and other Snake-compromised systems around the world to monitor the execution of the operation to learn how the FBI and other governments were able to disable the Snake malware and harden Snake's defenses. Accordingly, the FBI has assessed that the use of the remote search technique described above is necessary to ensure the success of Operation MEDUSA, and to protect the victims of Turla's Snake malware located not just in the United States, but also around the world.

64. Following the conclusion of the coordinated operation, the FBI will notify the victim owners of the Subject Computers and will provide detailed information about the

Snake implant that the FBI disabled on the Subject Computers. The FBI does not seek approval here to deliver the commands described herein to computers located outside of the United States.

65. The Subject Computers 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 Subject Computers have been "damaged" within the meaning of Rule 41(b)(6)(B) and 18 U.S.C. § 1030(e)(8) because the installation of the Snake malware has impaired the integrity and availability of data, programs, systems, and information on the servers.

66. As detailed above, the FBI's investigation has established that electronic storage media compromised by Snake malware has been located in at least five judicial districts during the course of the criminal scheme, including among others, the following: Northern District of California, Northern District of New York, District of Oregon, District of South Carolina, Central District of California, Eastern District of New York, and District of Maryland. Moreover, the FBI's investigation has established that the Subject Computers are also located in five or more judicial districts, specifically the following: District of Oregon, District of South Carolina, Northern District of Georgia, District of Connecticut, and Eastern District of California.

TIME AND MANNER OF EXECUTION

67. Because the requested warrant does not authorize the intrusion onto a physical premises, but the use of a remote search technique involving electronic storage media

located in multiple judicial districts, I submit that good cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR DELAYED NOTICE

68. The FBI intends to provide notice to the affected victims of the execution of the warrant on the Subject Computers as soon as practicable following the execution of the warrant. Nevertheless, because the execution of the warrant is just one component of a coordinated international technical operation that could be compromised by the premature disclosure of the warrant, the FBI requests that the Court authorize the FBI to delay the service of the warrant to ensure the success of the operation and to prevent Turla from defending against the technical operation to remediate the Snake malware.

69. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to delay the service of the warrant as normally required for up to thirty 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 communications, 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 endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, witness

intimidation, or "otherwise seriously jeopardizing an investigation." 18 U.S.C. § 2705(a)(2)(A)-(E).

70. I submit that the requirements of Rule 41(f)(3) and 18 U.S.C. § 3103a(b) are satisfied in this case. Specifically, until the FBI, the other U.S. government agencies, and foreign governments have completed the coordinated operation discussed above, there is a risk that premature disclosure of the requested warrant would permit Turla to make changes to the Snake malware to preserve access to compromised computers or take other steps to destroy or tamper with evidence, change patterns of behavior and otherwise seriously jeopardize the success of the operation. 18 U.S.C. § 2705(a)(2)(C), (E). Thus, reasonable cause exists to delay the service of the warrant as normally required until up to thirty days after execution of the warrant, however, as discussed above, it is the FBI's intention to provide notice of the warrant's execution to the owners of the Subject Computers as soon as practicable and likely well before the expiration of the 30-day delayed notice period requested in this Affidavit.

71. This Affidavit does not seek authorization to seize tangible property, and to the extent that the applied-for warrant authorizes the seizure of stored wire or electronic information (i.e., the transmission of commands that will disable the Snake malware), I submit that there is reasonable necessity for the seizure. See 18 U.S.C. § 3103a(b)(2).

72. Accordingly, the United States requests approval from the Court to delay notification until June 3, 2023, 30 days from the first possible date of execution on May 4, 2023, or until the FBI determines that there is no longer need for delayed notice, whichever is sooner.

See 18 U.S.C. § 3013a(b)(3) (limiting initial delayed notice to a "reasonable period not to exceed 30 days after the date of its execution," absent a later date certain).

73. The United States seeks authorization to delay notice in an abundance of caution to ensure the success of the coordinated technical operation described above. Nevertheless, during the period of delayed notice the United States may still seek to notify individual victims or to disclose information obtained as a result of the requested warrant to one or more victims or to private entities or foreign authorities for purposes of mitigating the effects of any computer intrusion or assisting in maintaining the security of computers or networks during the authorized period of delayed notice.

74. At the expiration of the period of delayed notice, or sooner when the FBI determines that there is no longer a need for delayed notice, the United States intends, pursuant to Rule 41(f)(1)(C), to provide notice both directly and through publication. Federal Rule of Criminal Procedure 41(f)(l)(C) provides the following regarding the means of providing notice of the warrant and receipt:

> 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.

75. For those victims whose publicly available Whois records contain contact information, or for whom the FBI already has obtained contact information, FBI personnel will notify such a victim of the search. For those victims who use a domain registration privacy service or whose contact information is not otherwise publicly available, the FBI will contact the privacy service or to the provider hosting the victim's domain asking them to provide notice to

the client. If none of the above options are available, the FBI will provide notice to the Internet Service Provider (ISP) that hosts the IP address for the victim asking it to provide notice to the client. For all such notifications, the FBI will provide a copy of the requested warrant and receipt. Finally, the FBI will 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 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 receipts.

CONCLUSION

76. I submit that this Affidavit supports probable cause for a warrant to use remote access to search electronic storage media described in Attachment A and to seize electronically stored information described in Attachment B.

Respectfully submitted,

[redacted]

TAYLOR FORRY
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone
or other reliable electronic means pursuant to
Fed. R. Crim. P. 4.1 and 41(d)(3) on May 4, 2023

[redacted]

THE HONORABLE CHERYL L. POLLAK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to be searched

This warrant applies to victim computers located in the United States onto which malicious cyber actors have installed, without authorization, the Snake malware, associated with the internet protocol ("IP") addresses listed below (collectively, the "Subject Computers"):

Subject Computer	**IP Addresses**
Subject Computer-1	[redacted]
Subject Computer-2	
Subject Computer-3	
Subject Computer-4	
Subject Computer-5	
Subject Computer-6	
Subject Computer-7	
Subject Computer-8	

ATTACHMENT B

Property to be seized

This warrant authorizes the use of a remote access technique to search the Subject Computers identified in Attachment A, as evidence and instrumentalities of computer fraud and conspiracy, in violation of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy).

This authorization includes the use of a remote access technique to access the Subject Computers and issue commands to: (1) overwrite vital components of the Snake malware without affecting any legitimate applications or files on the Subject Computers; and (2) terminate the Snake application running on the Subject Computers.

This warrant does not authorize the physical seizure of any tangible property, and to the extent that the applied-for warrant authorizes the seizure of stored wire or electronic information (i.e., the transmission of commands that will disable the Snake malware), the Court finds reasonable necessity for the seizure. See 18 U.S.C. § 3103a(b)(2).