NICOLA T. HANNA
United States Attorney
PATRICK R. FITZGERALD
Assistant United States Attorney
Chief, National Security Division
ANTHONY J. LEWIS (Cal. Bar No. 231825)
Assistant United States Attorney
Deputy Chief, Terrorism and Export Crimes Section
ANIL J. ANTONY (Cal. Bar No. 258839)
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-1786/6579
Facsimile: (213) 894-2927/8601
E-mail: anthony.lewis@usdoj.gov
anil.j.antony@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE: BOTNET OF COMPROMISED COMPUTERS	No. 18-MJ-02739 GOVERNMENT'S EX PARTE APPLICATION FOR A WARRANT PURSUANT TO FED. R. CRIM. P. 41(b)(6)(B) AND ORDER PURSUANT TO 18 U.S.C. § 3123 AUTHORIZING THE CONNECTION TO COMPROMISED COMPUTERS AND REQUEST TO SEAL; AFFIDAVIT OF CHADE CHOWANA-BANDHU **(UNDER SEAL)**

I. INTRODUCTION AND OVERVIEW

The United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, hereby applies for a warrant pursuant to Federal Rule of Criminal Procedure 41(b)(6)(B) and an order pursuant to Title 18, United States Code, Section 3123. The requested warrant and order and this application will allow the government to continue to search computers for an additional thirty days in accordance with the same terms as the search warrant issued by the Honorable Michael R. Wilner, United States Magistrate Judge, in Case Numbers 18-MJ-002115 (the "Second Renewal Warrant") and 18-MJ-2506 (the "Third Renewal Warrant"). The requested search warrant and order are identical to each of the last two issued by Judge Wilner. Those warrants and orders issued by Judge Wilner are a continuation, with certain revisions explained below, of search warrants and orders issued on June 11, 2018 by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01497 (the "Original Warrant"), and issued by Judge Mumm in Case No. 2:18-MJ-01904 (the "First Renewal Warrant").

An affidavit of Special Agent Chade Chowana-Bandhu is submitted herewith (the "Fourth Supplemental Affidavit" or "4th Supp. Aff."). That affidavit attaches the affidavit that was submitted in support of the Third Renewal Warrant ("Third Supplemental Affidavit" or "3d Supp. Aff."), which in turn also attaches the affidavits that were submitted in support of the Second Renewal Warrant ("Second Supplemental Affidavit" or "2d Supp. Aff."), the First Renewal

Warrant ("First Supplemental Affidavit" or "1st Supp. Aff.") and the Original Warrant (the "Original Affidavit" or "Orig. Aff.").

The requested search warrant and order will permit the Federal Bureau of Investigation (the "FBI") to cause computers compromised by a specific type of malware, Joanap, used by North Korean cyber-actors who are subjects of the government's investigation, to connect with computers within the Central District of California that are controlled by the FBI ("FBI IPs"). Computers within the network of computers infected by this North Korean malware (the "botnet"), each referred to herein as "Peers," will be prompted to communicate with FBI IPs, disclose their own lists of other known Peers, and pass addresses of the FBI IPs to other Peers in the network. This will allow the FBI to learn the Internet Protocol ("IP") addresses of the other Peers in the botnet, thus generating a map of the botnet.

In addition to identifying the IP addresses of computers infected by the Joanap malware, the requested warrant will allow the FBI to obtain other limited information regarding the connection, such as the port and the date and time of the connection. In some instances, the IP addresses of infected computers will be observed as those computers connect directly to the FBI IPs; in other instances the IP addresses of Peers will be discovered when a Peer supplies the FBI IPs with its "Peer Lists" -- the lists kept by the malware containing the IP addresses of other known Peers -- i.e., other computers infected with this North Korean malware. (See Orig. Aff. ¶¶ 39-41.) The information obtained by the FBI IPs from other Peers will be limited to information resulting from basic commands

within Joanap's ordinary vocabulary -- in other words, the FBI IPs will use commands already programmed into the malware to assist in getting those infected computers to identify themselves.

While the specific persons responsible for the compromise of the network of computers and use of that network are not yet identified, it is known that the malware was developed and used by malicious North Korean cyber-actors. (Orig. Aff. ¶¶ 10, 31, 35.) Among the offenses under investigation are violations of Title 18, United States Code, Section 1030(a)(5) (Causing Damage to Protected Computers). (Id.) There is probable cause to believe that federal crimes are being committed and that the information likely to be received -- the IP addresses of computers that have been compromised by the malware and which form a "botnet" network -- will constitute or yield evidence of that crime.

This application seeks a warrant pursuant to Rule 41(b)(6)(B) of the Federal Rules of Criminal Procedure, as well as an order pursuant to the statutory authority in Title 18, United States Code, Section 3123. The application for the warrant and order is based on the legal discussion below, the certification by an attorney for the government, and the attached affidavit of Special Agent Chowana-Bandhu.

This application also seeks authorization under Title 18, United States Code, Section 3103a(b), for reasonable cause shown, to delay notification of the requested warrant to the subscribers and users of the infected computers for a limited period of time, specifically until January 30, 2019.

This application seeks authorization to execute the requested warrant anywhere within the United States pursuant to Federal Rule of Criminal Procedure 41(b)(6)(B), and, for good cause shown, at any time of the day or night pursuant to Rule of Criminal Procedure 41(e)(2)(A)(ii).

Finally, this application requests that it, the proposed warrant that has been concurrently lodged, and the return to the warrant be sealed by the Court until such time as the Court directs otherwise. Allowing premature disclosure to the public at large would likely jeopardize the FBI's ongoing investigation and its ability to fully identify all of the compromised computers and other evidence that they may lead to, as such a disclosure would give the subjects of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, flee from prosecution, or otherwise seriously jeopardize the investigation, and would also allow them to detect the FBI IPs or modify the Joanap malware such that the requested search warrant would not be effective.

II. PEN REGISTER AND TRAP AND TRACE PROVISIONS

As noted above and in the Affidavit, in the course of executing the requested search warrant, computers infected with Joanap will connect with the FBI IPs, and the FBI IPs will then record the IP addresses of those computers along with other dialing, routing, addressing, and signaling information pursuant to a pen

register and trap and trace device.[1] (E.g., Orig. Aff. ¶ 52.b.) Based on the certification filed herewith and the facts contained in the Affidavit, and pursuant to Title 18, United States Code, Sections 3122 and 3123, the government seeks as part of the requested search warrant authorization for the following:

a. The use of a pen register anywhere in the United States to record or decode all non-content dialing, routing, addressing, or signaling information originating from or destined to the FBI IPs (as defined and described in the Affidavit), including IP addresses and IP packet header information, and to record the date and time of such transmissions, for a period of 30 days.

b. The use of a trap and trace device on each FBI IP anywhere in the United States to capture and record the incoming electronic or other impulses that identify the originating numbers or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication and to record the date, time, and duration of communications created by such incoming impulses, for a period of 30 days.

---

[1] It is not clear that the Pen Register and Trap and Trace Act's prohibition against the "installation" or "use" of a "pen register" or "trap and trace device" necessarily applies to the facts presented to the Court here. See, e.g., Capital Records Inc. v. Thomas-Rasset, 2009 WL 1664468, at *3 (D. Minn. 2009) ("[T]he Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them. If it did apply in those cases, then the Internet could not function . . . ."). Nonetheless, the United States is applying for an order authorizing the installation and use of a pen register and trap and trace device in an abundance of caution in order to be certain that its conduct does not violate the statute.

c. The IP addresses, and the dialing, routing, addressing, and signaling information called for by the requested order authorizing the use of a pen register and trap and trace device include, for any communication with an FBI IP, the IP addresses and source or destination ports for any such communication or transmission, along with the date, time, and duration.

Pursuant to Title 18, United States Code, Section 3123(d), the government requests that this application and the requested warrant be sealed until further order of the Court.

III. INFORMATION OBTAINED THROUGH ORIGINAL WARRANT AND FIRST, SECOND, AND THIRD SUPPLEMENTAL WARRANTS

As described in each of the Supplemental Affidavits, the FBI IPs have been successful in making contact with Peers and in identifying new Peers.

At the time of the First Renewal Warrant, the FBI IPs had not discovered as many Peers as has been anticipated, and because the number of new Peers being discovered had begun to plateau, the First Renewal Warrant described a new process to identify Peers using additional criteria. Specifically, the process involved identifying Joanap Peers by using historical consensually monitored computer activity of any computer infected with the Joanap malware dating back to January 1, 2018.

At the time of the Second Renewal Warrant, the IP addresses discovered through using historical consensually monitored computer activity had not significantly enhanced the FBI's ability to discover Peers. In particular, the IP addresses revealed from historical consensually monitored computer activity were either

already discovered through the execution of the search warrant by using the other criteria, or the IP addresses did not respond to the connection request from an FBI IP.

As a result, in the Second Renewal Warrant, the warrant added one additional criteria in identifying computers that will be searched. Specifically, the warrant allowed the search of computers that had certain ports (or channels) open and that met other criteria. The Joanap malware used certain ports for its communications that were traditionally used for other types of internet traffic, such as web browsing and email communications, likely as a measure to conceal the malicious traffic and make it appear like other legitimate traffic. The FBI used third-party data sets to examine which IP addresses had those specific ports open, and also which of those IP addresses did not behave the way that computers would if they were communicating on that port with whatever the "traditional" use of that port was. The Second Renewal Warrant allowed the FBI to search a computer that: (a) had at least one of three specific ports open, which ports were programmed into Joanap for its communications; (b) the use that port was not the traditional use of those ports based on how the computers behaved; (c) the computer responded to an initial cryptographic authentication step performed by the FBI to determine that the computer was infected with Joanap. This process is described in greater detail in paragraphs 9-21 of the Third Supplemental Affidavit. Multiple new IP addresses were discovered by using this technique. (4th Supp. Aff. ¶ 11.)

The principal reason that the FBI is seeking an additional period of thirty days is because the FBI and AFOSI has remedied a coding issue that was used to manage the execution of the search warrant on the FBI IPs. Specifically, as a part of the exchange between Peers, one informs the other whether it is publicly accessible or not (i.e., if it is behind a router or a firewall). The FBI IPs had inadvertently been informing Peers that they were not publicly accessible, even when they were. That in turn caused those Peers to stop using the ports they had previously used to connect with other Peers, which disrupted the connections between Peers in the botnet and the ability of the FBI IPs to fully propagate and to reach additional Peers. This process is detailed in paragraphs 12-18 of the Fourth Supplemental Affidavit.

The requested warrant and order are a continuation of the same techniques needed previously authorized, without adding any additional means of identifying Joanap peers. The requested warrant is therefore the same as the Third Supplemental Warrant (which in turn was the same as the Second Supplemental Warrant), and seeks an additional period of time in which to map the Joanap botnet.

///

IV. CONCLUSION

For the reasons set forth above and in the attached affidavit and certification, the government respectfully requests that the Court issue the accompanying warrant and order.

Dated: October 17, 2018

Respectfully submitted,

NICOLA T. HANNA
United States Attorney

PATRICK R. FITZGERALD
Assistant United States Attorney
Chief, National Security Division

ANTHONY J. LEWIS
ANIL J. ANTONY
Assistant United States Attorneys

Attorneys for Applicant
UNITED STATES OF AMERICA

CERTIFICATION

In support of this application, and pursuant to Title 18, United States Code, Section 3122, I state that I, Anthony J. Lewis, am an "attorney for the Government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure. I certify that the information likely to be obtained from the requested warrant is relevant to an ongoing criminal investigation being conducted by the Federal Bureau of Investigation of subjects who are not yet identified for violations of offenses including Title 18, United States Code, Section 1030(a)(5).

I declare under penalty of perjury under the laws of the United States of America that the foregoing paragraph is true and correct.

October 17, 2018
DATE

ANTHONY J. LEWIS
Assistant United States Attorney
Terrorism and Export Crimes Section

AFFIDAVIT

I, Chade Chowana-Bandhu, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2007. I am currently assigned to a squad that investigates computer intrusions in Los Angeles, where I specialize in the investigation of computer and high-technology crimes, including criminal and national security computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI SA, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. Prior to my work in the FBI, I received a Bachelor of Science degree in Electrical Engineering and worked as a software engineer for eight years.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant that will reveal the Internet Protocol ("IP") addresses of computers that are infected with a specific type of malware, referred to herein and in published research as "Joanap." This affidavit supplements and incorporates by reference the attached affidavit to which I swore on September 21, 2018 (the "Third Supplemental Affidavit" or "3d Supp. Aff."), which was submitted in support of a search warrant

issued that day (the "Third Renewal Warrant") by the Honorable Michael R. Wilner, United States Magistrate Judge, in Case No. 2:18-MJ-02506. That affidavit, in turn, incorporates by reference the attached affidavits to which I swore: on August 15, 2018 (the "Second Supplemental Affidavit" or "2d Supp. Aff."), which was submitted in support of a search warrant issued that day by the Honorable Michael R. Wilner, United States Magistrate Judge, in Case No. 2:18-MJ-2115; on July 24, 2018 (the "First Supplemental Affidavit" or "1st Supp. Aff."), which was submitted in support of a search warrant issued that day ("First Renewal Warrant") by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01904; and on June 11, 2018 (the "Original Affidavit" or "Orig. Aff."), which was submitted in support of the search warrant issued that day (the "Original Warrant") by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01497.

3. The requested warrant would allow the search of infected computers to continue for an additional period of thirty days according to the same terms and provisions previously authorized, for the reasons described below.

4. The facts described and nomenclature used in the Original Affidavit are assumed below. The facts in the Original Affidavit, First Supplemental Affidavit, Second Supplemental Affidavit, and Third Supplemental Affidavit remain true (except as specifically noted below) and establish probable cause for the requested renewed search warrant. Set forth below are

details regarding the execution of those search warrants and information obtained from the results of those search warrants.

A. Execution of the Original Warrant and First, Second, and Third Renewal Warrants and Information Obtained as a Result

5. This Part provides background on the execution of the search warrants and orders to date, and explains the reason why an additional period of thirty days is required due to a correction made in the FBI and AFOSI's code used to manage the execution of the search warrants and orders.

1. Background on Execution of the Warrants and Orders

6. As described in the First Supplemental Affidavit, after the warrant was issued on June 11, 2018, the FBI, working with other law enforcement counterparts at the Air Force Office of Special Investigations ("AFOSI"), first executed the search warrant on June 24, 2018. (1st Supp. Aff. ¶¶ 4-6.) Since that time, the FBI IPs have been both initiating connections with IP addresses discovered from Peers' Push Lists (and inserting themselves onto the Push Lists of those Peers), and receiving inbound connections from other IP addresses, presumably that received those Peers' Push Lists, as described in the Original Affidavit.[1] (Orig. Aff. ¶ 52-52.b.)

[1] The Original Affidavit described both Push Requests, which are requests to obtain Push Lists, and Receive Requests, which are requests to obtain Receive Lists. (Orig. Aff. ¶¶ 43.a, 43.b.) The FBI and AFOSI personnel executing the search warrant determined that additional testing would be required in order to begin implementing Receive Requests, therefore the only Request Commands that have been used are Push Requests.

7. The Original Warrant allowed the FBI to search a computer (by requesting its Peer List) if the computer was identified through consensual monitoring, through another Peer's Peer List, or if the Peer initiated a connection with an FBI IP. The number of Peers that were subsequently identified remained below the numbers predicted based on modeling performed by the FBI and AFOSI personnel. (See Orig. Aff. ¶¶ 45, 55.) As a result, two additional criteria were authorized to use by the FBI when identifying computers that could be searched.

8. The first was in the First Renewal Warrant, which authorized the FBI to continue searching computers the same way it had under the Original Warrant, and also permitted to the FBI to connect with IP addresses that were discovered through historical consensually monitored activity of computers infected with Joanap. (1st Supp. Aff. ¶¶ 10-13.) The results did not assist the FBI in identifying new Peers. Out of over 200 IP addresses identified through historical consensually monitored computer activity, approximately one quarter of them had already been discovered through the execution of the search warrant. The remaining approximately three quarters did not respond to the FBI IPs when initiating the Joanap communication sequence.

9. Then, the Second Renewal Warrant authorized the use additional criteria to identify a Peer that can be searched pursuant to the warrant. Specifically, the warrant allowed the search of computers that had certain ports (or channels) open and that met other criteria. The Joanap malware used certain ports for its communications that were traditionally used for

other types of internet traffic, such as web browsing and email communications. The selection of ports used for other ordinary purposes was likely a measure designed to conceal the malicious traffic and make it appear like other legitimate traffic. The FBI used third-party data sets to examine which IP addresses had those specific ports open, and also which of those IP addresses did not behave the way that computers would if they were communicating on that port with whatever the "traditional" use of that port was.

10. The Second Renewal Warrant thus allowed the FBI to search a computer that: (a) had at least one of three specific ports open, which ports were programmed into Joanap for its communications; (b) the use that port was not the traditional use of those ports based on how the computers behaved; (c) the computer responded to an initial cryptographic authentication step performed by the FBI to determine that the computer was infected with Joanap. This process is described in greater detail in paragraphs 9-21 of the Third Supplemental Affidavit. Multiple new IP addresses were discovered by using this technique.

11. Out of the over 750,000 IP addresses with port 110 open and abnormal termination message (according to the third-party port-scanned data sets), 3 were successfully authenticated as Joanap Peers. Approximately two million IP addresses have port 443 open and abnormal termination message, and out of those, 25 have been successfully authenticated as Joanap Peers. Approximately two million IP addresses have port 80 open and an

abnormal termination message, and since the Third Renewal Application they all have been vetted and only one IP address was successfully authenticated as a Joanap Peer.[2] (See 3d Supp. Aff. ¶¶ 20-20.b.)

2. Correction to Coding Issue Affecting FBI IPs Contact with Joanap Peers

12. On September 24, 2018, the FBI and AFOSI personnel executing the searches remedied a coding issue that was used to manage the execution of the search warrant on the FBI IPs. Although the previous application stated that it would likely be the last renewal, this coding issue has caused the FBI to seek an additional thirty days to complete the searches to map the Joanap botnet. Before explaining the coding issue that was corrected, some additional information on the operation of the Joanap malware is provided below.

13. A computer infected with Joanap is capable of operating as a "client" or a "server," but which role it plays depends in part on its environment. In a typical Joanap peer-to-peer connection, one Peer (the client) initiates the connection with another Peer (the server). In order to be able to receive inbound connections, the server must have a publicly accessible IP address; the port that the Peer is listening on cannot be behind a router or a firewall, or a "NAT Peer" as described herein. (Orig. Aff. ¶¶ 42, 53.b.) It should be noted

[2] Three of the IP addresses with each of those port numbers open that also met the other criteria did not return a Peer List when contacted by FBI IPs, though, and it is abnormal for a computer infected with Joanap to be operating on more than one port.

that a Peer that is publicly available can and does at times behave as a client and initiates connections with other Peers, for example to request new Peer Lists. Those Peer Lists (Push Lists specifically, Orig. Aff. ¶ 40.a) contain the IP address and open port for other publicly available Peers. The inverse is not true: A NAT Peer cannot receive initial inbound connections.

14. During an exchange between Peers, a client (the Peer initiating a connection) may ask the server it is contacting if it (the client) is publicly accessible on a given port. The server then attempts to connect to the port advertised by the client in that session and then informs the client whether the client is or is not publicly accessible.

15. The issue that had arisen in the way the FBI IPs were executing the searches is that when other Peers contacted the FBI IPs, the FBI IPs inadvertently always informed the clients that the clients were not publicly accessible, even when they were. Because of the way the Joanap malware operates, that caused a Peer ("Peer A" here) that in fact was publicly accessible to "believe" it was not publicly accessible, which in turn prompts Peer A to close the port it had been using to receive inbound connections from other Peers. Only when Peer A initiated a connection with another non-FBI Peer ("Peer B") would it learn that it was in fact publicly available, but at that point the Peer would use a different port to receive connections. All the other Peers that had stored Peer A's IP

address with the old port number (now closed) would not be able to connect successfully with Peer.

16. Through additional exchanges, this issue works itself out with some time. Peer A, having been informed by the FBI IPs that it was not publicly available, would inevitably contact another server Peer (Peer B), and Peer B would record the new, correct port number with Peer A's IP address, and propagate that information to other client Peers that contacted Peer B. Those clients could then successfully connect with Peer A. But the FBI IPs have been propagating through the botnet such that up to 15 IP addresses on each Peer List of 50 IP addresses are FBI IPs. (Orig. Aff. ¶ 47.) Each Peer selects an IP address randomly from its Receive List every three hours to make contact. (Id. ¶ 45.) That means that server Peers that have been in communication with the FBI IPs will periodically reconnect with FBI IPs. And each time an FBI IP contacts Peer A, the FBI IP would inform Peer A that Peer A was not publicly accessible, and the process would repeat.

17. The FBI and AFOSI personnel who are managing the executing of the search warrant identified the issue and on September 24, 2018, patched the code so that the FBI IPs would accurately inform client Peers connecting with it whether the clients were publicly accessible or not. Since that time, as of October 16, 2018, approximately 2398 client Peers and 123 server Peers (i.e., Peers that are publicly accessible) have been identified. The 2398 client Peers include some of the 123 server Peers. Of these, no new client Peers were discovered and

11 of the server Peers are newly identified since the code was patched on September 24, 2018.[3] The fact that new servers have been identified, however, means that additional time is warranted to determine whether those servers lead to additional Peers. As described in the Original Affidavit: the FBI IPs first make contact with a server Peer; as a result, the FBI IPs become entries on that server's Push List; when other Peers contact that server, they will receive the Push List containing the FBI IPs; and those Peers will then initiate contact with the FBI IPs. (Original Affidavit ¶¶ 45, 53-53.b, 67.) Because a Peer only initiates contact every three hours pursuant to the peer-to-peer functionality, that propagation process takes time. (Id.)

18. The reason that additional time is needed to continue mapping the botnet is because some time is needed to restore and stabilize the connections between Peers. For example, if a cluster of Peers had been in contact with Peer A, they may have lost contact with Peer A when Peer A jumped to a new port after

---

[3] The Third Supplemental Affidavit noted that by September 17, 2018, approximately 1,788 unique IP addresses had been identified, though only approximately 82 were publicly accessible (and not NAT Peers) and acting as "servers" that would supply Push Lists to other Peers. Due to a separate coding issue, the scripts used to operate the FBI IPs had recorded the results of the authentication step as "passed" even when the authentication step failed. This resulted in approximately 151 IP addresses being counted as Peers when in fact they do not appear to have been infected by Joanap. This did not affect the Peers that were searched pursuant to the port-scanned data described in paragraphs 9-21 of the Third Renewal Affidavit because the authentication step used to test those IP addresses were not done by FBI IPs using the scripts and code that were used to request Peer Lists from other Peers.

contact with an FBI IP. Within that cluster may be other server Peers, that in turn were in touch with other clusters of Peers. The result is that the botnet requires time to re-establish the connections that may have been interrupted by the coding issue. When that occurs, the FBI IPs will be able to propagate further and illuminate any parts of the botnet whose connection with the FBI IPs via Peer A (and other server Peers) had been severed. Because each Peer only checks its own Receive List every three hours, that process requires some time to complete, which is the reason for requesting an additional thirty days to conduct the searches authorized by the requested warrant.

B. Delayed Notice, Sealing, and Execution at Any Time of Day

19. For all of the reasons set forth in the Original Affidavit, the government seeks authority to delay notice of the warrant, that the warrant, application, and affidavit be filed under seal, and that the FBI and AFOSI be able to execute the search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In executing the search warrant, FBI and AFOSI personnel have not observed any indication that any of the subjects have been alerted to the presence of the FBI IPs in the Joanap botnet. Alerting them to the existence of the search warrant would likely cause the adverse results described in the Original Affidavit. (Id.) The Original Warrant and First Renewal Warrant sought to delay notification until August 31, 2018; those two periods of delay have been continued until November 7, 2018 by order of the Court, and the Second Renewal Warrant

authorized a delay of notification until November 7, 2018. This requested search warrant and order also seek to delay notification until January 30, 2019.

III. CONCLUSION

20. For all of the above reasons, there is probable cause to believe that the evidence to be requested through the requested search warrant executed within, and being investigated within, the Central District of California, will constitute or yield evidence of violations of the offenses listed above.

Chade Chowana-Bandhu
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me this ____ day of October, 2018.

UNITED STATES MAGISTRATE JUDGE

Exhibit

Third Supplemental Affidavit

AFFIDAVIT

I, Chade Chowana-Bandhu, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2007. I am currently assigned to a squad that investigates computer intrusions in Los Angeles, where I specialize in the investigation of computer and high-technology crimes, including criminal and national security computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI SA, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. Prior to my work in the FBI, I received a Bachelor of Science degree in Electrical Engineering and worked as a software engineer for eight years.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant that will reveal the Internet Protocol ("IP") addresses of computers that are infected with a specific type of malware, referred to herein and in published research as "Joanap." This affidavit supplements and incorporates by reference the attached affidavit to which I swore on August 15, 2018 (the "Second Supplemental Affidavit" or "2d Supp. Aff."), which was submitted in support of a search warrant issued that

day (the "Second Renewal Warrant") by the Honorable Michael R. Wilner, United States Magistrate Judge, in Case No. 2:18-MJ-02115. This affidavit, in turn, incorporates by reference the attached affidavit to which I swore on July 24, 2018 (the "First Supplemental Affidavit" or "1st Supp. Aff."), which was submitted in support of a search warrant issued that day ("First Renewal Warrant") by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01904, and the affidavit to which I swore on June 11, 2018 (the "Original Affidavit" or "Orig. Aff."), which was submitted in support of the search warrant issued that day (the "Original Warrant") by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01497.

3. The requested warrant would allow the search of infected computers to continue for an additional period of thirty days according to the same terms and provisions previously authorized.

4. The facts described and nomenclature used in the Original Affidavit are assumed below. The facts in the Original Affidavit, First Supplemental Affidavit, and Second Supplemental Affidavit remain true and establish probable cause for the requested renewed search warrant. Set forth below are details regarding the execution of those search warrants and information obtained from the results of those search warrants.

A. Execution of the Original Warrant and First and Second Renewal Warrants and Information Obtained as a Result

5. As described in the First Supplemental Affidavit, after the warrant was issued on June 11, 2018, the FBI, working with other law enforcement counterparts at the Air Force Office of Special Investigations ("AFOSI"), first executed the search warrant on June 24, 2018. (1st Supp. Aff. ¶¶ 4-6.) Since that time, the FBI IPs have been both initiating connections with IP addresses discovered from Peers' Push Lists (and inserting themselves onto the Push Lists of those Peers), and receiving inbound connections from other IP addresses, presumably that received those Peers' Push Lists, as described in the Original Affidavit.[1] (Orig. Aff. ¶ 52-52.b.)

6. In executing the search warrant, the FBI IPs have discovered new Peers. For example, by July 3, 2018, over 200 unique IP addresses had been identified, though only approximately 18 were publicly accessible (and not NAT Peers; see Orig. Aff. ¶¶ 42, 53.b) and acting as "servers" that would supply Push Lists to other Peers; one such Peer was located in the Central District of California.[2] By July 17, 2018, 628 new

---

[1] The Original Affidavit described both Push Requests, which are requests to obtain Push Lists, and Receive Requests, which are requests to obtain Receive Lists. (Orig. Aff. ¶¶ 43.a, 43.b.) The FBI and AFOSI personnel executing the search warrant determined that additional testing would be required in order to begin implementing Receive Requests, therefore the only Request Commands that have been used are Push Requests.

[2] The First Supplemental Affidavit and the Second Supplemental Affidavit made reference to the fact that "one such Peer" was located in the Central District of California, and at that time the FBI had understood that a "server" Peer was located in this District. (1st Supp. Aff. ¶ 9; 2d Supp. Aff.

unique IP addresses had been identified, with 18 that were publicly accessible and acting as servers. By August 3, 2018, over 900 unique IP addresses had been identified, though only approximately 42 were publicly accessible (and not NAT Peers) and acting as "servers" that would supply Push Lists to other Peers.[3] By September 17, 2018, approximately 1,788 unique IP addresses had been identified, though only approximately 82 were publicly accessible (and not NAT Peers) and acting as "servers" that would supply Push Lists to other Peers.

7. The First Renewal Warrant authorized the FBI to continue searching computers the same way it had under the Original Warrant, and also permitted to the FBI to connect with IP addresses that were discovered through historical consensually monitored activity of computers infected with Joanap. (1st Supp. Aff. ¶¶ 10-13.) The results did not assist the FBI in identifying new Peers. Out of over 200 IP addresses identified through historical consensually monitored computer

---

¶ 6.) On re-examination, the IP address referenced was actually one of the FBI IP addresses located in this District. As of September 17, 2018, however, three "client" IP addresses have been identified in the Central District of California.

[3] It should be noted that references to the number of unique IPs operating as servers (42 in this reference) do not appear to be 42 concurrently running machines. Because the way the search warrant is executed using specific commands in Joanap's vocabulary, the specific device identifier is not reflected in the communications identified in the exchanges between Peers, only the IP address assigned to it and the port it is using. Moreover, some of the IP addresses of the Peers acting as servers are similar, indicating they are part of the same block of IP addresses used by the same network that re-assigns IP usage to different computers. For these reasons, it is estimated that there are far fewer unique Joanap servers amongst those 42 unique addresses that are publicly facing.

activity, approximately one quarter of them had already been discovered through the execution of the search warrant. The remaining approximately three quarters did not respond to the FBI IPs when initiating the Joanap communication sequence.

8. According to the FBI and AFOSI personnel executing the search warrant, the number of new Peers being identified had been leveling off. The number of Peers that have been identified to date remain below the numbers predicted based on modeling performed by the FBI and AFOSI personnel as well. (See Orig. Aff. ¶¶ 45, 55.) As described in the First Supplemental Affidavit, one possible reason that the numbers of Peers are low is because of a possible coding issue in the way the malware maintains Peer Lists. (1st Supp. Aff. ¶ 10.) Specifically, the inactive Peers do not appear to be "pruned" from the Peer Lists effectively, and instead active Peers are pruned. (Id.) As a result, it appeared that the FBI IPs were stuck in a "pocket" of the botnet without being able to connect with or map the rest of the botnet. (Id.)

9. For this reason, the Second Renewal Warrant authorized the use additional criteria to identify a Peer that can be searched pursuant to the warrant. The Original Warrant allowed the FBI to search a computer (by requesting its Peer List) if the computer was identified through consensual monitoring, through another Peer's Peer List, or if the Peer initiated a connection with an FBI IP. The First Renewal Warrant used those same criteria and allowed the FBI to use historical consensually monitored activity going back to January 1, 2018. The Second

Renewal Warrant retained those same criteria, and to expand them to include one additional criteria, which is described in the following paragraphs.

10. There are multiple companies that make available publicly or for a fee the results of port-scanning IP addresses. In addition to the IP addresses used to route traffic on the internet, internet traffic also includes a "port." Once the right IP address is located and the traffic is routed there, the port is effectively a channel that allows the computer to separate different kinds of internet traffic based on different types of communication protocols. For example, web browsers often communicate over port 80 or 8080, secure web browsing often occurs over port 443, and certain email protocols use port 25, 110, or 143.

11. Port-scanning refers to the process of checking whether various ports on a computer are "open" and available to communicate or not. Not only will port-scanning results show whether a port is open or not, the computer conducting the scan can make an initial data request to the open port. This initial request solicits data which is routinely provided once a client connects to the server's port. That data is often referred to as a "banner," providing the client with the initial information necessary to continue engaging the application bound to that port on the server. The companies that conduct the scans of these ports also make publicly available the results of the banner produced by the server once the connection is established. Banners can include host names, server software

version numbers, and digital certificate information required to establish a secure connection. Additionally, if a port is found to be open, but abnormality occurs, the abnormality information may be logged. Abnormalities can include premature termination (no banner presented) and invalid banner information (indicating that software other than what is expected is running on the server port).

12. Joanap is configured to use 26 ports as preferred listening ports (meaning that the port is open). The list begins with ports 443, 110, 53, and 80, in that order of preference. The traditional uses of those ports are: port 443 is used for HTTPS (or secure web browsing); port 110 is used for POP3 (a protocol used for receiving email); port 53 is used for DNS or Domain Name Service (used to translate a domain into an IP address)[4]; and port 80 is used for ordinary web traffic. Using ports that are traditionally utilized for other types of traffic is a common technique used by hackers to conceal their connections as internet traffic that would otherwise appear to be legitimate.

13. The FBI and AFOSI will therefore use the publically available port-scanning data to discern which IP addresses have these ports open. That alone, however, can be filtered further.

---

[4] The Domain Name Service, or "DNS," is a naming system for computers, services, or any other resources connected to the internet. An often-used analogy to explain the DNS is that it serves as the phone book for the internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name "www.justice.gov" may translate to the IP address 149.101.146.50.

Specifically, many of the IP addresses that have those ports open will be using them in a traditional way. For example, an IP address with an open port 443 may be a legitimate web server. Where it is a legitimate web server, however, the port-scanning data will reflect a legitimate banner used by clients to communicate with encrypted HTML sockets (443) and plain text HTML sockets (80). In the case of a mail server (110), traditional mail server banner information would be provided. Thus, only those IP addresses where (a) the specified port is open, and (b) the specific abnormality of a prematurely terminated session prior to receiving a banner, will be considered viable to be searched pursuant to the requested search warrant.

14. One of these ports will not be used in the requested warrant: port 53. The reason for that is because port 53 traditionally hosts Domain Name Service or DNS, as noted above. DNS services utilize a protocol that does not provide the connection termination message required to detect an abnormal termination. Therefore the port-scanning data does not provide a means of discriminating between legitimate or traditional use of port 53 and instances in which the port is open because of an abnormality--such as infection with the Joanap malware.[5]

[5] DNS traditionally operates using User Datagram Protocol (UDP). UDP is a "connectionless" protocol, not requiring any packets to be acknowledged or verified. Transmission Control Protocol (TCP) is a "connection oriented" stateful protocol utilized for Web (443) and Mail (SMTP) and provides the connection termination message required to detect an abnormal termination. Therefore, the publically available 53 scans to

15. Even using only the IP addresses that (a) have one of the three specified ports (443, 80, 110) open, and (b) provide a premature session disconnection (indicating that the ports are not being used for their intended purpose) yielded a significant number of IP addresses. Data available in July 2018, for example, shows that those criteria are satisfied for over 2,000,000 IP addresses for port 443, over 2,000,000 IP addresses for port 80, and over 750,000 IP addresses for port 110.

16. That list, however, is further narrowed down. As described in the Original Affidavit, in the ordinary course of how Joanap's peer-to-peer functionality operates, a Peer initiating a connection (the "client") sends a pseudo-random string of text that the other Peer (acting as the "server") returns encrypted to the client. The client then sends an encrypted message with known plain text. If the server can decode the known plain text correctly, the peer has performed a cryptographic handshake and validates itself to the other Peer (thus authenticating itself as a computer infected with Joanap). (Orig. Aff. ¶ 44.) Specifically, when one Peer (a client) initiates a connection to another Peer (a server), the client will first send a very small (4-byte) value. The client will then sends a 16-byte pseudorandom value to the server. The server will then send back to the client the 16-byte value that has been encrypted. That 16-byte value is encrypted with a

---

collect DNS server information are UDP oriented, and do not provide the granularity necessary to detect an abnormal termination.

certain, standard encryption system (referred to as RC4), and using the encryption key contained in the Joanap malware. If the client is able to decrypt that value, then the client will send an encrypted message, where the known plain text that is encrypted is "https://www.google.com/index.h". If the server decodes that message to match the plain text written above, then each node is satisfied that they are both Joanap Peers.

17. In performing this additional step to further narrow down the IP addresses to discern which are infected with Joanap, the FBI and AFOSI only attempt the first half of the cryptographic handshake on the IP addresses filtered using the previous two criteria. The FBI will use computers (not necessarily the FBI IPs) to pose as clients and only execute that initial part of the authentication step--sending a 4-byte value followed by a 16-byte value--and await the response. Only if the response is encrypted using Joanap's method of encryption and its encryption key, then the IP address is one that will be included for execution of the search warrant to request a Peer List from it. If the IP address is not a Joanap Peer, then it will terminate the session or the session will time out and will not pass the initial part of the cryptographic handshake. The FBI and AFOSI have used and tested this technique on other computers and has not observed any indications that performing this initial part of the authentication step causes any impairment of a computer's ability to function. Unlike the search authorized by the warrant that allows the FBI to request a Peer List, this step does not cause the computer to divulge

any of its own information--at most it would return information sent to it by the FBI or AFOSI (after encrypting it).

18. It should also be noted that using port-scanning data is likely to allow the FBI to develop a more current and complete map of the botnet because the information is more recent than historically monitored activity. Different services make data sets available that are more or less recent; for example, one service makes data available that is one month old, and another service makes data available that is one week old. That is more likely to assist in generating a current map of the botnet, and also to reveal other "pockets" of the broader botnet that were not visible starting from the individual consensually monitored IP addresses. That will be of particular assistance given the way that Joanap "prunes" Peers on the Peer Lists it maintains: starting with an up-to-date data set regarding which IP addresses may be infected is more likely to overcome the FBI IPs inability to "see" through fragmentation in the botnet that may have occurred as a result of Peer Lists losing contact with neighbors because of stale or outdated Peers.

19. Even after an IP address has satisfied each of those three criteria, as with every other connection made by the FBI IPs, each connection to Peers identified by any means pursuant to the search warrant will be initiated with an authentication step to determine if the computer is a Peer in fact infected with Joanap. (Orig. Aff. ¶ 44.) Only if the computer passes the authentication step will the FBI IP continue with a Request

Command. (See Orig. Aff. ¶ 43.) Thus only computers that are in fact infected with Joanap will be searched by the FBI IPs.

20. As noted above in paragraph 15, data available in July 2018 shows that open port and the abnormal termination message are satisfied for over 2,000,000 IP addresses for port 443, over 2,000,000 IP addresses for port 80, and over 750,000 IP addresses for port 110. The following details were compiled as of September 17, 2018:

a. Out of the over 750,000 IP addresses with port 110 open and abnormal termination message (according to the third-party port-scanned data sets), 3 were successfully authenticated as Joanap peers. Approximately two million IP addresses have port 443 open and abnormal termination message, and out of those, 25 have been successfully authenticated as Joanap peers. Approximately two million IP addresses have port 80 open and abnormal termination message, and out of nearly 500,000 that have been tested with just the first authentication step, 3 have been successfully authenticated as Joanap peers.

b. As noted above, three IP addresses were successfully authenticated as Peers that had port 80 and port 110 open; not only are those 3 IP addresses the same, but they are among the twenty-five authenticated peers that had port 443 open. Those three IP addresses moreover behaved abnormally: none of those 3 IP addresses returned a Peer List when it was requested, and it is abnormal for an infected Peer to be operating on more than one port, as Joanap typically only operates using a single port. Aside from these 3 IP addresses,

out of the remaining 22 that were authenticated using port 443, 7 failed when a Peer List was requested (meaning no Peer List was provided), 2 had not yet had their Peer Lists requested, and 13 successfully returned a Peer List. At least some of IP addresses contained in the Peer Lists received from the authenticated Peers had not previously been discovered through the execution of the search warrant.

21. Thus, while the authentication of port-scanned IP addresses with ports 110, 443, and 80 open is nearly complete, some additional time is requested in order to determine whether the results of this process lead to other "pockets" of the botnet or if the map is as complete as possible. Furthermore, as the FBI IPs have been executing the search warrant and communicating with Peers, and both requesting Peer Lists and including themselves onto other Peers' Peer Lists, the number of unique IP addresses has continued to grow, now nearly double what it was in the beginning of last month (over 900 unique IP addresses by August 3, 2018, and approximately 1,788 unique IP addresses by September 17, 2018).

22. Thus, with this next (and anticipated to be the last) renewal of the search warrant, the FBI and AFOSI will be able to determine with more confidence if there are any other "pockets" of Peers that were not in communication with the groups of Peers in the botnet that the FBI had observed. By the end of the period in the requested search warrant, the Joanap botnet will be mapped by the FBI and AFOSI as completely as possible using the means authorized by the search warrants.

B. Delayed Notice, Sealing, and Execution at Any Time of Day

23. For all of the reasons set forth in the Original Affidavit, the government seeks authority to delay notice of the warrant, that the warrant, application, and affidavit be filed under seal, and that the FBI and AFOSI be able to execute the search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In executing the search warrant, FBI and AFOSI personnel have not observed any indication that any of the subjects have been alerted to the presence of the FBI IPs in the Joanap botnet. Alerting them to the existence of the search warrant would likely cause the adverse results described in the Original Affidavit. (Id.) The Original Warrant and First Renewal Warrant sought to delay notification until August 31, 2018; those two periods of delay have been continued until November 7, 2018 by order of the Court, and the Second Renewal Warrant authorized a delay of notification until November 7, 2018. This requested search warrant and order also seek to delay notification until November 8, 2018.

III. CONCLUSION

24. For all of the above reasons, there is probable cause to believe that the evidence to be requested through the requested search warrant executed within, and being investigated

///

within, the Central District of California, will constitute or yield evidence of violations of the offenses listed above.

/s/
Chade Chowana-Bandhu
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me
this 21 day of September, 2018.

UNITED STATES MAGISTRATE JUDGE
MICHAEL R. WILNER

Exhibit

Second Supplemental Affidavit

AFFIDAVIT

I, Chade Chowana-Bandhu, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2007. I am currently assigned to a squad that investigates computer intrusions in Los Angeles, where I specialize in the investigation of computer and high-technology crimes, including criminal and national security computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI SA, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. Prior to my work in the FBI, I received a Bachelor of Science degree in Electrical Engineering and worked as a software engineer for eight years.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant that will reveal the Internet Protocol ("IP") addresses of computers that are infected with a specific type of malware, referred to herein and in published research as "Joanap." This affidavit supplements and incorporates by reference the attached affidavit to which I swore on July 24, 2018 (the "First Supplemental Affidavit" or "1st Supp. Aff."), which was submitted in support of a search warrant issued that

day ("First Renewal Warrant") by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01904. That affidavit, in turn, attaches the affidavit to which I swore on June 11, 2018 (the "Original Affidavit" or "Orig. Aff."), which was submitted in support of the search warrant issued that day (the "Original Warrant") by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01497.

3. The requested warrant would allow the search of infected computers to continue for an additional period of thirty days. It would also allow the FBI to search computers identified as infected by Joanap using one additional criteria, described in greater detail below.

4. The facts described and nomenclature used in the Original Affidavit are assumed below. The facts in the Original Affidavit and First Supplemental Affidavit remain true and establish probable cause for the requested renewed search warrant. Set forth below are details regarding the execution of those search warrants, information obtained from the results of those search warrants, and how the provisions that were in those search warrants are modified in the provisions of the requested warrant.

A. Execution of the Original Warrant and First Supplemental Warrant and Information Obtained as a Result

5. As described in the First Supplemental Affidavit, after the warrant was issued on June 11, 2018, the FBI, working with other law enforcement counterparts at the Air Force Office of Special Investigations ("AFOSI"), first executed the search

warrant on June 24, 2018. (1st Supp. Aff. ¶¶ 4-6.) Since that time, the FBI IPs have been both initiating connections with IP addresses discovered from Peers' Push Lists (and inserting themselves onto the Push Lists of those Peers), and receiving inbound connections from other IP addresses, presumably that received those Peers' Push Lists, as described in the Original Affidavit.[1] (Orig. Aff. ¶ 52-52.b.)

6. In executing the search warrant, the FBI IPs have discovered new Peers. For example, by August 3, 2018, over 900 unique IP addresses had been identified, though only approximately 42 were publicly accessible (and not NAT Peers; see Orig. Aff. ¶¶ 42, 53.b) and acting as "servers" that would supply Push Lists to other Peers; one such Peer was located in the Central District of California. It should be noted that the 42 unique IPs operating as servers do not appear to be 42 concurrently running machines. Because the way the search warrant is executed using specific commands in Joanap's vocabulary, the specific device identifier is not reflected in the communications identified in the exchanges between Peers, only the IP address assigned to it and the port it is using. Moreover, some of the IP addresses of the Peers acting as servers are similar, indicating they are part of the same block

---

[1] The Original Affidavit described both Push Requests, which are requests to obtain Push Lists, and Receive Requests, which are requests to obtain Receive Lists. (Orig. Aff. ¶¶ 43.a, 43.b.) The FBI and AFOSI personnel executing the search warrant determined that additional testing would be required in order to begin implementing Receive Requests, therefore the only Request Commands that have been used are Push Requests.

of IP addresses used by the same network that re-assigns IP usage to different computers. For these reasons, it is estimated that there are far fewer unique Joanap servers amongst those 42 unique addresses that are publicly facing.

7. The First Renewal Warrant authorized the FBI to continue searching computers the same way it had under the Original Warrant, and also permitted to the FBI to connect with IP addresses that were discovered through historical consensually monitored activity of computers infected with Joanap. (1st Supp. Aff. ¶¶ 10-13.)

8. That process has now occurred, and the results have not assisted the FBI in identifying new Peers. Out of over 200 IP addresses identified through historical consensually monitored computer activity, approximately one quarter of them had already been discovered through the execution of the search warrant. The remaining approximately three quarters did not respond to the FBI IPs when initiating the Joanap communication sequence.

B. New Provisions in the Requested Warrant

9. According to the FBI and AFOSI personnel executing the search warrant, the number of new Peers being identified continues to be leveling off. The number of Peers that have been identified to date remain below the numbers predicted based on modeling performed by the FBI and AFOSI personnel as well. (See Orig. Aff. ¶¶ 45, 55.) As described in the First Supplemental Affidavit, one possible reason that the numbers of Peers are low is because of a possible coding issue in the way

the malware maintains Peer Lists. (1st Supp. Aff. ¶ 10.) Specifically, the inactive Peers do not appear to be "pruned" from the Peer Lists effectively, and instead active Peers are pruned. (Id.) As a result, it appears likely that the FBI IPs are stuck in a "pocket" of the botnet without being able to connect with or map the rest of the botnet. (Id.)

10. For this reason, the requested warrant seeks to use one additional criteria to identify a Peer that can be searched pursuant to the warrant. The First Renewal Warrant provided the following with respect to how the FBI can identify a computer as a member of the Joanap botnet that could be searched:

> The FBI will determine whether a computer is a Peer in the Joanap botnet by virtue of one or more of the following conditions (1) consensually monitored computer activity reflecting the presence of the Joanap malware, including both computer activity occurring after the issuance of this search warrant during the period authorized by the warrant as well as such activity dating back to January 1, 2018; (2) the computer initiates a connection with an FBI IP, or (3) the IP address of the computer is received by the FBI IPs on a Peer List from another computer infected with Joanap.

11. The requested warrant seeks to retain those criteria, and to expand them to include one additional criteria.

12. There are multiple companies that make available publicly or for a fee the results of port-scanning IP addresses. In addition to the IP addresses used to route traffic on the internet, internet traffic also includes a "port." Once the right IP address is located and the traffic is routed there, the port is effectively a channel that allows the computer to

separate different kinds of internet traffic based on different types of communication protocols. For example, web browsers often communicate over port 80 or 8080, secure web browsing often occurs over port 443, and certain email protocols use port 25, 110, or 143.

13. Port-scanning refers to the process of checking whether various ports on a computer are "open" and available to communicate or not. Not only will port-scanning results show whether a port is open or not, the computer conducting the scan can make an initial data request to the open port. This initial request solicits data which is routinely provided once a client connects to the server's port. That data is often referred to as a "banner," providing the client with the initial information necessary to continue engaging the application bound to that port on the server. The companies that conduct the scans of these ports also make publicly available the results of the banner produced by the server once the connection is established. Banners can include host names, server software version numbers, and digital certificate information required to establish a secure connection. Additionally, if a port is found to be open, but abnormality occurs, the abnormality information may be logged. Abnormalities can include premature termination (no banner presented) and invalid banner information (indicating that software other than what is expected is running on the server port).

14. Joanap is configured to use 26 ports as preferred listening ports (meaning that the port is open). The list

begins with ports 443, 110, 53, and 80, in that order of preference. The traditional uses of those ports are: port 443 is used for HTTPS (or secure web browsing); port 110 is used for POP3 (a protocol used for receiving email); port 53 is used for DNS or Domain Name Service (used to translate a domain into an IP address)[2]; and port 80 is used for ordinary web traffic. Using ports that are traditionally utilized for other types of traffic is a common technique used by hackers to conceal their connections as internet traffic that would otherwise appear to be legitimate.

15. The FBI and AFOSI will therefore use the publically available port-scanning data to discern which IP addresses have these ports open. That alone, however, can be filtered further. Specifically, many of the IP addresses that have those ports open will be using them in a traditional way. For example, an IP address with an open port 443 may be a legitimate web server. Where it is a legitimate web server, however, the port-scanning data will reflect a legitimate banner used by clients to communicate with encrypted HTML sockets (443) and plain text HTML sockets (80). In the case of a mail server (110), traditional mail server banner information would be provided. Thus, only those IP addresses where (a) the specified port is

---

[2] The Domain Name Service, or "DNS," is a naming system for computers, services, or any other resources connected to the internet. An often-used analogy to explain the DNS is that it serves as the phone book for the internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name "www.justice.gov" may translate to the IP address 149.101.146.50.

open, and (b) the specific abnormality of a prematurely terminated session prior to receiving a banner, will be considered viable to be searched pursuant to the requested search warrant.

16. One of these ports will not be used in the requested warrant: port 53. The reason for that is because port 53 traditionally hosts Domain Name Service or DNS, as noted above. DNS services utilize a protocol that does not provide the connection termination message required to detect an abnormal termination. Therefore the port-scanning data does not provide a means of discriminating between legitimate or traditional use of port 53 and instances in which the port is open because of an abnormality--such as infection with the Joanap malware.[3]

17. Even using only the IP addresses that (a) have one of the three specified ports (443, 80, 110) open, and (b) provide a premature session disconnection (indicating that the ports are not being used for their intended purpose) yields a significant number of IP addresses. Data available in July 2018, for example, shows that those criteria are satisfied for over 2,000,000 IP addresses for port 443, over 2,000,000 IP addresses for port 80, and over 750,000 IP addresses for port 110.

---

[3] DNS traditionally operates using User Datagram Protocol (UDP). UDP is a "connectionless" protocol, not requiring any packets to be acknowledged or verified. Transmission Control Protocol (TCP) is a "connection oriented" stateful protocol utilized for Web (443) and Mail (SMTP) and provides the connection termination message required to detect an abnormal termination. Therefore, the publically available 53 scans to collect DNS server information are UDP oriented, and do not provide the granularity necessary to detect an abnormal termination.

18. That list, however, will be further narrowed down. As described in the Original Affidavit, in the ordinary course of how Joanap's peer-to-peer functionality operates, a Peer initiating a connection (the "client") sends a pseudo-random string of text that the other Peer (acting as the "server") returns encrypted to the client. The client then sends an encrypted message with known plain text. If the server can decode the known plain text correctly, the peer has performed a cryptographic handshake and validates itself to the other Peer (thus authenticating itself as a computer infected with Joanap). (Orig. Aff. ¶ 44.) Specifically, when one Peer (a client) initiates a connection to another Peer (a server), the client will first send a very small (4-byte) value. The client will then sends a 16-byte pseudorandom value to the server. The server will then send back to the client the 16-byte value that has been encrypted. That 16-byte value is encrypted with a certain, standard encryption system (referred to as RC4), and using the encryption key contained in the Joanap malware. If the client is able to decrypt that value, then the client will send an encrypted message, where the known plain text that is encrypted is "https://www.google.com/index.h". If the server decodes that message to match the plain text written above, then each node is satisfied that they are both Joanap Peers.

19. In performing this additional step to further narrow down the IP addresses to discern which are infected with Joanap, the FBI and AFOSI will only attempt the first half of the cryptographic handshake on the IP addresses filtered using the

previous two criteria. The FBI will use computers (not necessarily the FBI IPs) to pose as clients and only execute that initial part of the authentication step--sending a 4-byte value followed by a 16-byte value--and await the response. Only if the response is encrypted using Joanap's method of encryption and its encryption key, then the IP address is one that will be included for execution of the search warrant to request a Peer List from it. If the IP address is not a Joanap Peer, then it will terminate the session or the session will time out and will not pass the initial part of the cryptographic handshake. The FBI and AFOSI have used and tested this technique on other computers and has not observed any indications that performing this initial part of the authentication step causes any impairment of a computer's ability to function. Unlike the search authorized by the warrant that allows the FBI to request a Peer List, this step does not cause the computer to divulge any of its own information--at most it would return information sent to it by the FBI or AFOSI (after encrypting it).

20. It should also be noted that using port-scanning data is likely to allow the FBI to develop a more current and complete map of the botnet because the information is more recent than historically monitored activity. Different services make data sets available that are more or less recent; for example, one service makes data available that is one month old, and another service makes data available that is one week old. That is more likely to assist in generating a current map of the botnet, and also to reveal other "pockets" of the broader botnet

that were not visible starting from the individual consensually monitored IP addresses. That will be of particular assistance given the way that Joanap "prunes" Peers on the Peer Lists it maintains: starting with an up-to-date data set regarding which IP addresses may be infected is more likely to overcome the FBI IPs inability to "see" through fragmentation in the botnet that may have occurred as a result of Peer Lists losing contact with neighbors because of stale or outdated Peers.

21. Even after an IP address has satisfied each of those three criteria, as with every other connection made by the FBI IPs, each connection to Peers identified by any means pursuant to the search warrant will be initiated with an authentication step to determine if the computer is a Peer in fact infected with Joanap. (Orig. Aff. ¶ 44.) Only if the computer passes the authentication step will the FBI IP continue with a Request Command. (See Orig. Aff. ¶ 43.) Thus only computers that are in fact infected with Joanap will be searched by the FBI IPs.

C. Delayed Notice, Sealing, and Execution at Any Time of Day

22. For all of the reasons set forth in the Original Affidavit, the government seeks authority to delay notice of the warrant, that the warrant, application, and affidavit be filed under seal, and that the FBI and AFOSI be able to execute the search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In executing the search warrant, FBI and AFOSI personnel have not observed any indication that any of the subjects have been alerted to the presence of the FBI IPs in the Joanap botnet.

Alerting them to the existence of the search warrant would likely cause the adverse results described in the Original Affidavit. (Id.) While the Original Warrant and First Renewal Warrant sought to delay notification until August 31, 2018, the requested warrant seeks to delay notification until November 7, 2018.

III. CONCLUSION

23. For all of the above reasons, there is probable cause to believe that the evidence to be requested through the requested search warrant executed within, and being investigated within, the Central District of California, will constitute or yield evidence of violations of the offenses listed above.

_____
Chade Chowana-Bandhu
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me
this ____ day of August, 2018.

_____
UNITED STATES MAGISTRATE JUDGE

Exhibit

First Supplemental Affidavit

AFFIDAVIT

I, Chade Chowana-Bandhu, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2007. I am currently assigned to a squad that investigates computer intrusions in Los Angeles, where I specialize in the investigation of computer and high-technology crimes, including criminal and national security computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI SA, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. Prior to my work in the FBI, I received a Bachelor of Science degree in Electrical Engineering and worked as a software engineer for eight years.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant that will reveal the Internet Protocol ("IP") addresses of computers that are infected with a specific type of malware, referred to herein and in published research as "Joanap." This affidavit supplements and incorporates by reference the attached affidavit to which I swore on June 11, 2018 (the "Original Affidavit" or "Orig. Aff."), which was submitted in support of a search warrant issued that day (the

"Original Warrant") by the Honorable Frederick F. Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01497. The requested warrant would allow the search of infected computers to continue for an additional period of thirty days.

3. The facts described and nomenclature used in the Original Affidavit are assumed below. The facts in the Original Affidavit remain true and establish probable cause for the requested renewed search warrant. Set forth below are details regarding the execution of the Original Warrant, information obtained from the results of the Original Warrant, and how the provisions that were in the Original Warrant are modified in the provisions of the requested warrant.

A. Execution of the Original Warrant and Information Obtained as a Result

4. After the warrant was issued on June 11, 2018, the FBI, working with other law enforcement counterparts at the Air Force Office of Special Investigations ("AFOSI"), completed the final preparations in order to execute the warrant. After leasing the use of certain IP addresses to operate as the FBI IPs described in the Original Affidavit; technical issues arose with the service provider that had leased the servers to the FBI, and the FBI was required to lease the use of additional servers.

5. Once the use of new servers was secured, the FBI and AFOSI prepared to execute the warrant by connecting with two Joanap Peers that were being monitored by law enforcement pursuant to consent. One of those monitored Peers had become

disconnected June 15 in connection with the owner relocating its office and associated computer equipment.

6. The second of those monitored Peers was still being monitored pursuant to consent, but the area where it was located suffered a loss of internet connection beginning on June 8, 2018 that lasted until June 22, 2018. The FBI and AFOSI had tried to connect to that monitored Peer between June 11, 2018 and June 22, 2018 but no connection could be made. On Sunday, June 24, 2018, the FBI and AFOSI successfully made contact with that Peer. It provided a file that was one of its Peer Lists (the Push List; see Orig. Aff. ¶ 40.a), but the file was empty of the entries it would ordinarily contain (the IP address, port number, and date and time stamp; see Orig. Aff. ¶ 40.a).[1]

7. At that point, the FBI and AFOSI used the traffic that had been monitored pursuant to consent from Saturday, June 23, 2018 that reflected the presence of Joanap on another Peer, and the FBI and AFOSI made a connection with that Peer and requested its Push List. The IP addresses in that Push List either did not respond or failed the authentication step that initiates communication using Joanap's protocols. (See Orig. Aff. ¶ 44.) The FBI and AFOSI then identified another Peer from the consensually monitored traffic on June 28, 2018 and obtained a new Push List that identified new Peers.

---

[1] Although the reason it supplied an empty Push List is not yet known, it is most likely that the Push List was purged as a result of system (and malware) being active but disconnected from the internet for a sustained period of time. This state typically causes the malware to change from server to client mode, therefore dumping the peer list.

8. Since that time, the FBI IPs have been both initiating connections with IP addresses discovered from Peers' Push Lists (and inserting themselves onto the Push Lists of those Peers), and receiving inbound connections from other IP addresses, presumably that received those Peers' Push Lists, as described in the Original Affidavit.[2] (Orig. Aff. ¶ 52-52.b.)

9. In executing the search warrant, the FBI IPs have discovered new Peers. For example, by July 3, 2018, over 200 unique IP addresses had been identified, though only approximately 18 were publicly accessible (and not NAT Peers; see Orig. Aff. ¶¶ 42, 53.b) and acting as "servers" that would supply Push Lists to other Peers; one such Peer was located in the Central District of California. By July 17, 2018, 628 new unique IP addresses had been identified, with 18 that were publicly accessible and acting as servers. It should be noted that the 18 unique IPs operating as servers do not appear to be 18 concurrently running machines. Because the way the search warrant is executed using specific commands in Joanap's vocabulary, the specific device identifier is not reflected in the communications identified in the exchanges between Peers, only the IP address assigned to it and the port it is using. Moreover, some of the IP addresses of the Peers acting as

---

[2] The Original Affidavit described both Push Requests, which are requests to obtain Push Lists, and Receive Requests, which are requests to obtain Receive Lists. (Orig. Aff. ¶¶ 43.a, 43.b.) The FBI and AFOSI personnel executing the search warrant determined that additional testing would be required in order to begin implementing Receive Requests, therefore the only Request Commands that have been used are Push Requests.

servers are similar, indicating they are part of the same block of IP addresses used by the same network that re-assigns IP usage to different computers. For these reasons, it is estimated that there are 8 or fewer unique servers amongst those 18 unique addresses.

B. New Provisions in the Requested Warrant

10. According to the FBI and AFOSI personnel executing the search warrant, the number of new Peers being identified appears to be leveling off. The number of Peers that have been identified to date are below the numbers predicted based on modeling performed by the FBI and AFOSI personnel as well. (See Orig. Aff. ¶¶ 45, 55.) One possible reason that the numbers of Peers are low is because of a possible coding issue in the way the malware maintains Peer Lists. Specifically, the inactive Peers do not appear to be "pruned" from the Peer Lists effectively, and instead active Peers are pruned. As a result, it appears likely that the FBI IPs are stuck in a "pocket" of the botnet without being able to connect with or map the rest of the botnet. One of the ways the FBI IPs may be able to connect with and map the rest of the broader Joanap botnet is to identify other Peers through historical connections.

11. For this reason, the requested warrant seeks to use additional criteria to identify a Peer that can be searched pursuant to the warrant. The Original Warrant provided the following with respect to how the FBI can identify a computer as a member of the Joanap botnet that could be searched:

The FBI will determine whether a computer is a Peer in the Joanap botnet by virtue of one or more of the following conditions (1) consensually monitored computer activity reflecting the presence of the Joanap malware; (2) the computer initiates a connection with an FBI IP, or (3) the IP address of the computer is received by the FBI IPs on a Peer List from another computer infected with Joanap

12. The requested warrant seeks to retain those criteria, and to expand them. Specifically, with respect to "consensually monitored computer activity reflecting the presence of the Joanap malware," the requested warrant seeks authority to use consensually monitored computer activity that is not only monitored during the period authorized by the search warrant, but that is historical dating back to January 1, 2018.

13. As with every other connection made by the FBI IPs, each connection to Peers identified through historical computer activity beginning in January 1, 2018 will be initiated with an authentication step to determine if the computer is a Peer in fact infected with Joanap. (Orig. Aff. ¶ 44.) Only if the computer passes the authentication step will the FBI IP continue with a Request Command. (See Orig. Aff. ¶ 43.) Thus only computers that are in fact infected with Joanap will be searched by the FBI IPs.

C. Delayed Notice, Sealing, and Execution at Any Time of Day

14. For all of the reasons set forth in the Original Affidavit, the government seeks authority to delay notice of the warrant, that the warrant, application, and affidavit be filed under seal, and that the FBI and AFOSI be able to execute the

search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In executing the search warrant, FBI and AFOSI personnel have not observed any indication that any of the subjects have been alerted to the presence of the FBI IPs in the Joanap botnet. Alerting them to the existence of the search warrant would likely cause the adverse results described in the Original Affidavit. (Id.)

III. CONCLUSION

15. For all of the above reasons, there is probable cause to believe that the evidence to be requested through the requested search warrant executed within, and being investigated within, the Central District of California, will constitute or yield evidence of violations of the offenses listed above.

/s/
Chade Chowana-Bandhu
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me this 24th day of July, 2018.

Frederick F. Mumm
UNITED STATES MAGISTRATE JUDGE

Exhibit

Original Affidavit

AFFIDAVIT

I, Chade Chowana-Bandhu, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2007. I am currently assigned to a squad that investigates computer intrusions in Los Angeles, where I specialize in the investigation of computer and high-technology crimes, including criminal and national security computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI SA, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. Prior to my work in the FBI, I received a Bachelor of Science degree in Electrical Engineering and worked as a software engineer for eight years.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant that will reveal the Internet Protocol ("IP") addresses of computers that are infected with a specific type of malware, referred to herein and in published research as "Joanap."

3. As described in more detail below, Joanap is a type of malware that allows the subjects of the investigation controlling it to perform various types of functions on the

computers compromised by Joanap. Joanap also contains a peer-to-peer function that causes each infected computer to share information with its "neighbor" peers so that each infected computer contains a current (but not exhaustive) list of fifty other computers that are compromised.

4. The requested warrant and order seeks authority to use one or more computers that in turn will utilize up to fifteen IP addresses that are under the control of the FBI (the "FBI IPs") in order to pose as Joanap-infected computers so that other Joanap-infected computers ("Peers") can be identified. Infected Peers will be identified through two methods. First, Peers that have learned of the FBI IPs (through Joanap's automatic routine that causes Peers to request and share lists of Peers or "Peer Lists" with each other) will initiate communication with the FBI IPs, revealing their own IP addresses as ones where computers are located that are infected by Joanap. Second, the FBI IPs will initiate contact with individual Peers and request that those Peers share their lists of Peers ("Peer Lists," described more below in ¶¶ 39-41), which lists are maintained by the Peer's local instance of Joanap running on that Peer.

5. Because of the way that the Joanap peer connectivity works, Joanap has certain commands ("Push Requests," see ¶ 43.a) that each Peer automatically executes to update its own list of Peers; it does so by asking other Peers for their Peer Lists. Other commands ("Receive Requests," see ¶ 43.b) can be manually sent that cause another Peer to share a different list of Peers. Both the "automatic" and the "manual" commands are referred to

collectively as "Request Commands." Those Request Commands will be sent by the FBI IPs. Each of these (and most other) Joanap commands, in addition to requesting a Peer List, include at least two other parts: first, an initial cryptographic handshake is used to verify that the Peer is a Joanap-infected computer, and thus that the two computers can communicate with each other using Joanap's built-in set of commands; and second, a "validation" is performed to determine whether the requesting Peer is publically accessible on the Internet. During the validation step, if a Peer is publically accessible, the requesting Peer's IP address will be added to one of the receiving Peer's Peer Lists. The FBI IPs initiating contact with other Peers will have public Internet access, and will cause their IP addresses to be incorporated into other Peer's peer lists.

6. Thus, the FBI IPs are designed to serve as a listening post for Joanap-infected Peers, recording the IP addresses of the Peers that contact the FBI IPs and receiving Peer Lists from other Peers. Each of the Request Commands are within the ordinary vocabulary of Joanap, and one of the two commands (the Push Request) is routinely exchanged automatically between Peers in the Joanap botnet. With respect to those "Push Requests," the FBI IPs thus will be participating in exchanges that already routinely and automatically occur between infected Peers; the FBI IPs in effect will be displacing other infected Peers that would be populating the stored list of Peers and communicating with other Peers in order to map the Joanap botnet.

7. In order to effectively identify as much of the Joanap botnet as possible, (a) the FBI IPs must communicate -- using Request Commands -- with other Peers they have discovered, in order for those Peers to incorporate the FBI IPs onto one of their Peer Lists and spread the FBI IPs to other "neighbor" Peers; (b) the FBI IPs will each record the IP addresses, their respective port numbers, and date and times, of compromised computers trying to connect with them; and (c) the FBI IPs will request Peer Lists through their connections with other Peers in order to identify additional Peers that the FBI IPs will contact. The requested warrant is therefore sought pursuant to Federal Rule of Criminal Procedure 41(b)(6)(B) and Title 18, United States Code, Section 3123.

8. The requested warrant will authorize the FBI IPs to continue this process for a period of 30 days.

9. The requested warrant also seeks (a) authorization under Title 18, United States Code, Section 3103a(b), for reasonable cause shown below, to delay notification of the proposed warrant until August 31, 2018 for the reasons described below, and to permit the acquisition of electronic information or electronic communications (specifically, the Peer Lists, discussed below); (b) authorization under Federal Rule of Criminal Procedure 41(b)(6)(B) to execute the warrant anywhere within the United States; (c) authorization under Federal Rule of Criminal Procedure 41(e)(2)(A)(ii) to execute the warrant at any time of day or night.

10. As described in greater detail below, I respectfully submit that there is probable cause to believe that IP addresses and other information likely to be obtained during the period of the requested warrant will constitute or yield evidence of federal offenses, including specifically violations of Title 18, United States Code, Section 1030(a)(5) (Causing Damage to Protected Computers), being committed by subjects of the investigation who are not yet identified.

11. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from various law enforcement personnel and witnesses, my review of reports regarding Joanap and other malware, and my written and oral communications with FBI and other computer scientists and technical personnel. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of, or the government's investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates are on or about the dates listed.

III. LEGAL BACKGROUND

A. Jurisdiction to Issue Requested Search Warrant

12. Federal Rule of Criminal Procedure 41(b)(6)(B) permits magistrate judges in one district to issue search warrants that may be executed in multiple judicial districts to address this scenario. Rule 41(b)(6)(B) provides in relevant part:

> 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.

13. Title 18, United States Code, Section 1030(a)(5), is one of the offenses under investigation, and it provides in relevant part:

> (a) Whoever--
>
> (5) (A) 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;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

14. Joanap has infected computers in the Central District of California and in at least five other districts. (Aff. ¶ 36.) Moreover, as noted above and elsewhere in the Affidavit, the FBI IPs will be located in the Central District of California. (Aff. ¶ 30.)

15. The authority in the requested warrant will apply only to Peer computers located in the United States. While the Joanap botnet operates in multiple countries, and computers under the control of the FBI may be in contact with Peers in the

Joanap network that are both inside the United States and outside the United States, the requested search warrant only authorizes activities within the territory of the United States.

B. Delayed Notice

16. Title 18, United States Code, Section 3103a(b) provides in relevant part:

> (b) Delay.--With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if--
>
> (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);
>
> (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and
>
> (3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.

17. Title 18, United States Code, Section 2705(a)(2), provides in relevant part the definition of an adverse result:

> An adverse result . . . is--
>
> (A) endangering the life or physical safety of an individual;
>
> (B) flight from prosecution;
>
> (C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying trial.

18. Here, the requested warrant provides for giving notice on August 31, 2018, and prohibits, as part of the receipt of the requested information, the seizure of any tangible property and wire information or wire communications. 18 U.S.C. § 3103a(b)(2). The requested warrant permits the seizure of electronic information or electronic communications, specifically the Peer Lists stored on Joanap-infected computers and certain other information incidental to the exchange between the FBI IPs and Peers, because the Affidavit sets forth reasonable necessity to seize them. Id. (Aff. ¶¶ 64-65.) As discussed later in the Affidavit, immediate notification of this order to the user(s) of the compromised computers in the botnet may have an adverse result. (Aff. ¶¶ 60-63.)

C. Execution and Means of Notice

19. Federal Rule of Criminal Procedure 41(e)(2)(A)(ii) provides in relevant part that a search warrant "must command the officer to . . . execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." As discussed below, the FBI cannot control when Peers will contact the FBI IPs, and the execution of the warrant should occur without users being aware that it is occurring. (Aff. ¶ 66.)

20. Although the requested warrant, once issued, must commence within fourteen days of being issued (see Federal Rule of Criminal Procedure 41(e)(2)(A)(i)), the requested warrant

provides that the period during which the FBI can complete its execution of the search warrant will be a period of up to 30 days.

21. Finally, Federal Rule of Criminal Procedure 41(f)(1)(C) provides the following regarding 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.

22. The requested warrant specifically provides for notice by electronic means or publication and other means reasonably calculated to reach each such person.

IV. TERMINOLOGY

23. Botnet: A "botnet" is a network of computers that cyber criminals have infected with malware that gives a cyber-criminal access to each computer and allows a cyber-criminal to control each computer remotely.

24. Compile date: A "compile date" is the date and time on which source code was compiled into an executable file, also called machine code or object code, which is time-stamped in the file.

25. Dropper: A "dropper" file often behaves as an "installer" of other pieces of malware. Droppers can install other malware by downloading them from pre-configured locations, for example by causing a victim computer to connect to a

specific IP address or domain, or by storing compressed files within the dropper itself that the dropper then unpacks on the victim's computer. (Oftentimes, malware that is being loaded onto a computer surreptitiously is encrypted or otherwise compressed, and must be "unpacked" or decompressed before it can be executed on a victim computer.)

26. Hashes: A "hash" value can be calculated for any computer file by applying a one-way algorithm to the data contained in the file. An MD5 hash is the name of one such hash value generated by a particular algorithm. If any of the content of the file is changed, even a change as minor as adding an extra "space" character, the algorithm will produce a different hash when it is applied to the file. Although there is an extremely small possibility of two separate files calculating the same hash (it has been proven by researchers to be possible), when two files have the same hash value they are assumed to be identical files, thus providing verification to a very high degree of confidence that the two files are identical.

27. IP address: An Internet Protocol is a unique address of a computer or other device connected to a network, and is used to route Internet communications to and from the computer or other device. An IP version 4 address, or "IPv4 address," is a set of four numbers, each ranging from 0 to 255 and separated by a period (".") that is used to route traffic on the Internet. A single IP address can manage Internet traffic for more than one computer or device, such as when a router in one's home routes traffic to one's desktop computer, as well as one's

tablet or smartphone, while all using the same IP address to access the Internet. A newer system used by some computers or networks, referred to as IP version 6, serves the same function and uses a longer value that is a combination of numbers and letters (allowing for more addresses).

28. Malware: "Malware" is malicious computer software intended to cause a victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, usually unbeknownst to the owner or user of the victim computer.

29. Peer-to-peer: "Peer-to-peer" refers to a means of networking computers such that they communicate directly with each other, rather than through a centralized management point.

V. FACTS

30. As described below, there is probable cause to believe that the IP addresses to be discovered through the execution of the search warrant are the IP addresses of computers infected with the Joanap malware, and therefore are fruits, evidence, and instrumentalities of Title 18, United States Code, Section 1030(a)(5) (Causing Damage to Protected Computers).

A. JOANAP

1. Background on Joanap

31. The FBI is investigating multiple computer intrusions carried out by North Korean cyber actors. Among their intrusion campaigns is the creation of a botnet using malware referred to as Joanap. On May 29, 2018, the National Cybersecurity and Communications Integration Center published "Technical Alert

TA18-149A" that indicated that Joanap has been attributed to North Korean cyber actors and is one of their many malware tools.[1] Joanap has been used in connection with targeting and successful intrusions of victims in multiple sectors and countries.

32. Joanap is a peer-to-peer malware family that enables North Korean cyber actors to rapidly establish a set of infrastructure across the Joanap botnet, as well as to provide remote administration functionality on each infected computer.[2] Joanap was developed to run discreetly on Microsoft Windows operating systems. At least one iteration of it has an MD5 hash value 4613f51087f01715bf9132c704aea2c2. This particular hash value, which serves as the unique identifier for the copy of Joanap used in the development of software for this investigation and search warrant, matches a "VirusTotal.com"[3]

---

[1] The National Cybersecurity and Communications Integration Center, or "NCCIC," serves as a central location where multiple partners, including U.S. government agencies, the private sector companies, and international entities involved in cybersecurity coordinate and synchronize their efforts.

[2] These characteristics describe the Joanap malware generally. The execution of the warrant will begin when the FBI IPs initiate connection with two computers that are in fact members of the Joanap botnet, and will proceed to contact and identify other members of that botnet through connections that are cryptographically verified. Thus the way in which the warrant will be executed will involve only members of the Joanap botnet, which Peers use its communication protocols and commands and that are able to cryptographically authenticate themselves.

[3] VirusTotal, which is owned by Google, is an online service that analyzes files and URLs enabling the identification of viruses, worms, Trojans, and other kinds of malicious content detected by antivirus engines and website scanners. VirusTotal does not distribute or advertise any products belonging to third-parties. VirusTotal aggregates dozens of antivirus

malware entry with a compile date of 2011-09-14 05:38:38. Technical Alert TA18-149A referred to the same hash value, and also referenced a series of supplemental reports published by Novetta. One of the Novetta reports was title "Operation Blockbuster: Remote Administration Tools and Content Staging Malware Report." That Novetta report identified an installer package for a version of Joanap, titled SierraJuliett-MikeOne (Joanap v1), which was compiled 16 minutes later than the version on VirusTotal. Novetta also identifies a second version of Joanap, titled SierraJuliett-MikeTwo (Joanap v2), which was compiled at a later date and thus does not match the test sample with the MD5 hash described above. Novetta's report indicated that the "communication protocol of (Joanap v2) is incompatible with the protocol of (Joanap v1)," meaning that the two versions of Joanap are distinguishable. The version of Joanap, and the botnet created using it, that is the subject of this search warrant is thus Joanap v1.

33. Based on my review of publicly available materials and internal government reports, my discussions with other cyber security professionals and with FBI experts, I have learned that Joanap is a strain of malware that has been observed for many years. It is referred to as a "second stage" malware, meaning it is "dropped" by another malware. In the case of Joanap, it has often been observed being dropped by an automated worm

---

engines and scanners to scan each file submitted and provides the detection results of these engines, free of charge.

referred to in published reporting as "Brambul."[4] Brambul, which has been in existence since 2009, crawls from computer to computer, trying to infect computers using exploits against a particular set of vulnerabilities and then, if successful in compromising the computer, relays the credentials and victim host information (that are necessary to gain access to the compromised computers) to certain email accounts hard-coded into the malware.[5]

34. Joanap grants malicious actors significant control over victim computers within the botnet, including "root" level access, which means access to all commands and files on a computer. Some of the capabilities of the Joanap malware include: registering itself as a service to operate discretely;

---

[4] Other public cyber security experts have previously reported on this malware. The IT security firm Trend Micro has written analytical reports on Brambul and Joanap, and identified first receiving samples of Brambul on December 14, 2012 and first receiving samples of Joanap on May 10, 2013. McAfee Labs was able to identify certain email accounts as being recipients of the credentials of infected computers sent by different strains of the malware, although McAfee did not use the same naming convention of "Brambul." See http://home.mcafee.com/virusinfo/virusprofile.aspx?key=570006#none; http://home.mcafee.com/virusinfo/virusprofile.aspx?key=257183#none.

[5] The Brambul worm spreads through self-replication by infecting new victim systems via brute force attacks of the victim's Server Message Block ("SMB") protocol. SMB is a method that Microsoft systems use to share files on a network. When Brambul is successful in gaining access to a victim computer, the Brambul malware conducts a survey of the victim machine and collects certain information, including the victim's IP address, system name, operating system, username last logged in, and last password used. That information is then sent via Simple Mail Transfer Protocol ("SMTP") from a spoofed email address to one or more of the email accounts hard-coded (or pre-programmed) into the Brambul malware.

starting and terminating processes on the victim computer (the computer it has infected); downloading and running executables (oftentimes malicious tools and additional malware); saving, moving, and deleting files; writing data to the victim computer's memory; and creating directories and downloading and writing files to the victim's file system. Joanap also contains a peer-to-peer functionality discussed below. These and other capabilities give Joanap persistence, meaning that the malicious actors have significant control over the victim computer and that the malware is difficult to remove or exclude, and it also allows those actors to install other malware onto computers infected with Joanap.

35. The Joanap botnet has historically provided North Korean cyber actors with an extensive global infrastructure from which they can facilitate computer network operations. The Joanap botnet -- the network of infected computers -- provides a global operational platform that North Korean cyber actors can then put to use to further their hacking operations. Technical Alert TA18-149A indicated that, since at least 2009, North Korean cyber actors have likely been using both Joanap and Brambul malware to target multiple victims globally and in the United States -- including the media, aerospace, financial, and critical infrastructure sectors. Evidence has also shown that computers infected with Joanap were also infected with other North Korean malware, showing that Joanap has been used by North Korean cyber actors to stage other hacking operations.

36. Based on my review of internal government reports and discussions with cyber security professionals and FBI experts, I have determined that computers infected with the Joanap malware remain prevalent within the United States and around the world. I have read reporting of analysis performed on a Joanap-infected computer and its Peer List and learned that, between February and March of 2018, 86 Peers operating within the United States have communicated with just this one infected computer. I know that the Peer computers were within the United States based on their IP addresses. Specifically, using geo-location tools that query online databases containing location data of IP addresses, I identified the locations of some of the Joanap-infected computers within the United States, and they included IP addresses in (1) the Central District of California, (2) the Southern District of Texas, (3) the Southern District of Indiana, (4) the Southern District of Ohio, (5) the District of Utah, and (6) the Middle District of Florida, among other districts.

37. Based on my training and experience, I know that when malware like Joanap is detected, it requires costs to remediate the computers and networks on which it is found. That is particularly true where the Jonap malware itself as well as other malware that the subjects of the investigation use Joanap to install are capable of escalating privileges, copying information, and executing commands on infected computers. Therefore remediating the computers infected with the Joanap

malware and addressing the compromise that has resulted from it are not as simple as deleting the file.

2. Joanap's Peer-to-Peer Functionality

38. I have learned the following from my review of publicly available materials and technical documentation prepared by the FBI. Joanap-infected Peers operate as a peer-to-peer botnet. The Joanap botnet requires that each Peer be able to communicate solely with other Peers in the network when using commands within the Joanap vocabulary. Peers do this by periodically querying neighboring, previously validated Peers for their up-to-date Peer Lists -- the lists of IP addresses of other Peers stored on a given Peer. Unlike many other botnets, there is not a centralized command-and-control device, domain, IP address, or other infrastructure that can globally control the entire botnet. While the malicious actors maintain access to the infected Peers, in order to make use of the botnet they have to "crawl" the botnet by querying individual Peers, or "nodes," and having queries propagate through Peers. Once a target Peer is identified, malicious actors may then communicate directly with that Peer.

39. Each Peer has been configured to maintain two sets of Peer Lists, consisting of IP addresses and operating ports of other Joanap-infected Peers, along with a corresponding time-

stamp.[6] That time-stamp denotes the last time that communication successfully occurred with a Peer.

40. There are two types of Peer Lists maintained by Joanap on an infected Peer. Each of the two lists serve different purposes, and each is populated using different information:

a. Push List: A "Push List" is the list of IP addresses, ports, and time stamps that a Peer will "push" or supply to another Peer upon a request. The Push List has a maximum limit of 50 IP addresses and a new IP address is only added to the Push List after a Request Command is issued to it from a publically accessible Peer with that IP address.

i. Specifically, Peer B will only update its own Push List with Peer A's IP address after (a) Peer A initiates contact with Peer B, and (b) Peer B then reaches back to Peer A and successfully connects with it, before actually adding Peer A's IP address to Peer B's Push List.

ii. Thus, the Push List only contains "vetted" IP addresses of Peers that are (a) publically accessible on the Internet and (b) have affirmatively reached out to a Peer and completed a successful exchange. This is one of the features

---

[6] In addition to IP addresses used to route traffic on the internet, internet traffic will also include a "port." Once the right IP address is located and the traffic is routed there, the port is effectively a channel that allows the computer to separate different kinds of internet traffic often based on different types of communication protocols. For example, web browsers often communicate over port 80 or 8080, secure web browsers often occurs over port 443, and certain email protocols use port 25, 110, or 143.

that requires the FBI IPs to make connections directly with each Peer it identifies, as discussed below.

iii. The Push List is kept in "volatile" or "random access memory" ("RAM"), and is not stored in that form on the infected Peer's hard drive. It is created through the automatic operation of Joanap's peer-to-peer functionality, and is not the result of action taken by the user of the computer, nor would the user even know of its presence (unless for some reason the user was aware of the infection, for example in the case of a security researcher who was examining how Joanap operated).

b. Receive List: A "Receive List" is the list of IP addresses, ports, and time stamps that is kept on a given Peer that is populated using the Push Lists that a Peer has requested and received from other Peers. It is used to periodically initiate contact with other Peers by the Peer keeping it. Like the Push List, the Receive List is kept in volatile memory.

i. Thus, once Peer B supplies its Push List to Peer A, Peer A will then incorporate the entries, through a process of sorting and merging, into Peer A's Receive List. The Receive List is then used by Peer A as a directory to periodically initiate contact and issue a Request Command (the "Push Request," see ¶ 43.a) for the Push List from those Peers. Over time, each Peer on the Receive List is merged with Peers from the Push List and, through Joanap's automatic operation, the Receive List will retain the fifty most recent Peers by chronological order and discard the remaining Peers.

ii. While the Push List is requested and then supplied in response to the periodic Push Requests that occur automatically, the Receive Lists can be requested by another command (a "Receive Request," described below). A Receive Request in the ordinary course of the Joanap botnet is not automatic and is generally performed by someone who would manually send the command. It is, however, a command programmed into and recognized by Joanap.

41. Each Peer List is ordered chronologically, keeping the most recent entries and overwriting more stale entries with newer ones.

42. As noted above, a Push List is the list that is supplied by a Peer when it is requested by another Peer. It is possible that a significant portion of all Peers are behind a firewall or another Network Address Translation ("NAT") device, like a router, that routes Internet traffic between computers on a private network through a single IP address (collectively "NAT Peers").

a. Because they are "behind" NAT devices or firewalls, NAT Peers are not seen by Joanap as publicly accessible on the Internet, and they therefore will not receive contact initiated by another Peer. That is because Joanap has a built-in feature of its communications between Peers that distinguishes whether a Peer is publicly accessible or not. When they are not (i.e., when they are NAT Peers), Joanap is configured to cause other Peers not to ingest NAT Peers into their Push Lists. As a result, a NAT Peer will neither maintain

its own Push List, nor will it appear on other Peers' Push Lists (or Receive Lists).

b. NAT Peers do, however, initiate contact with other public Peers and issue commands (Push Requests) for those Peers' Push Lists. This is because Joanap permits NAT Peers to request and receive Push Lists from public Peers. Therefore, a NAT Peer will maintain its own Receive List, consisting of Peers from Push Lists supplied by other Peers.

43. As noted above, Joanap can execute a number of commands, including several root level commands. (See ¶ 34.) The commands at issue here relate to its peer-to-peer functionality, and specifically just those Request Commands that prompt a Peer to supply its own Peer Lists.[7] As noted above in paragraphs 40.b.i and 40.b.ii, Push Requests occur automatically when Joanap peers periodically connect with other Peers on their Receive Lists, and Receive Requests do not occur automatically but are generally sent manually. Both, however, are commands that are programmed into the malware and that are recognized by the Joanap malware. Each Request Command is described in further detail in the following paragraphs.

a. Push Request: A "Push Request" is a Request Command that is automatically and routinely issued from a Peer

[7] The commands are denoted as 0x2000 and 0x8000 series and 0x4002 commands. Each series command contains a "validating" feature to determine public accessibility and a "request" feature to request another Peer's Push List. The commands typically occur after the cryptographic handshake, or a 0x1000 series command, that establishes that each Peer is in fact a Joanap Peer and can send and accept commands in Joanap's vocabulary.

to a distant Peer, causing the Push List to be supplied to the Peer issuing the command. When a Peer (Peer A) initiates contact with a distant Peer (Peer B), Peer A issues a Push Request that (a) validates that Peer A is publically accessible on the Internet (if true, Peer A will appear on Peer B's Push List) and (b) performs a query for Peer B's Peer List. Peer B will respond to the request by supplying Peer A with its Push List.

i. On certain occasions dictated by Joanap's protocol, a Peer may issue a specific type of Push Request that prompts a distant Peer to also supply certain system information in addition to supplying its Push List. In this case, Peer B will respond to Peer A's request by supplying Peer A with its Push List, and immediately afterwards supply its system information, which may include its IP address, port number, MAC address (Media Access Control, which is a device identifier), operating system information, and CPU (central processing unit) information. Although Joanap processes these commands in this manner, FBI IPs will not issue this type of command to prompt other Peers to reveal their system information. Conversely, FBI IPs will disregard prompts to supply their system information, and will respond to these commands by only supplying their Push Lists.

b. Receive Request: A "Receive Request" is a Request Command that functions similar to a Push Request with the exception that this command is manually issued to a distant Peer for the Peer's Receive List, causing the Receive List to be

supplied to the Peer issuing the command. FBI IPs will issue Receive Requests to other Peers at various intervals to more efficiently identify Peers and propagate themselves through the botnet. In the event that any computers issue Receive Requests to FBI IPs, those commands will be disregarded by the FBI IPs.

44. During these (and many other) commands between Joanap Peers, when a Peer (Peer A) sends a command to another Peer (Peer B), the Peers also exchange the port numbers to use for their communications. Peer B uses a pseudo-random string of text that is encrypted to perform a cryptographic handshake and validate itself to Peer A (thus authenticating itself as a computer infected with Joanap), and only after that -- in the case of a Push Request -- Peer B will provide Peer A with its Push List. In addition to these exchanges, the Peers exchange certain ancillary information while performing the commands.[8]

45. In connection with the automatic connections that Joanap causes a Peer to periodically initiate, each Peer selects a Peer on its Receive List every three hours in order to initiate contact and exchange the commands discussed above. This means that the time it takes the new Peers' IP addresses to propagate through the Joanap network can be time consuming. In order for the activity described below to identify as many Peers that are reasonably likely to be identified through this process

---

[9] This ancillary information includes the status of the exchange, the time of the system that received the initial connection, and certain numerical values generated in the course of the exchange (e.g., when generating and completing the cryptographic handshake).

based on the FBI's current understanding of the botnet, I am informed the process is likely to take a minimum of 20 days to map 80 percent of the botnet, although that is based on certain assumptions, such as the percentage of Peers that have publicly available IP addresses assigned versus the percentage that do not (i.e., the portion of the botnet that is made up of NAT Peers). Therefore the requested period of 30 days will allow the FBI to collect a significant amount of information about the identities of the Peers in the botnet, which may allow the FBI to map all or nearly all of it. Depending on the rate of new Peers being identified, the FBI may apply for a new warrant to extend that period if it appears that mapping the botnet is not yet complete or close to complete.

B. OPERATION OF THE REQUESTED SEARCH WARRANT

1. Infrastructure

46. The FBI IPs will be a maximum of 15 public facing IP addresses located in the United States, and specifically in the Central District of California, that will be used to connect with other Joanap Peers. Each of the FBI IPs will be configured, through custom scripts written by the FBI, to communicate with other Joanap Peers, and will be the outward-facing, Internet-accessible IP addresses used in the execution of the warrant, although they will be controlled by those scripts and by other computers under the control of the FBI. The FBI IPs will only emulate Joanap-infected computers and will not actually be running Joanap malware. For example, one practical difference is that while ordinarily a Receive List is

maintained up to a maximum of 50 Peers, here the purpose of the search warrant is to collect and record a complete map of all of the Joanap Peers, and therefore that list will not be limited to 50 Peers.

47. Although Push Lists may contain up to 50 Peers, only 15 FBI maintained IP addresses will be used. Only 15 FBI IPs will be used in order to increase the chances that an FBI IP will be contacted by a Peer when it initiates a connection every three hours while at the same time not fully populating the entire Peer List. Populating the entire Peer Lists with FBI IPs would cause the Peers to only connect with the FBI IPs and therefore could "sink-hole" the Joanap botnet, meaning that Peers would not be reaching out to other non-FBI IP Peers.

48. It is important to sufficiently saturate the botnet with FBI IPs, but not sink-hole it, in order to fully map as many Peers on the botnet as possible. First, populating the entire Receive Lists of multiple Peers with FBI IPs would effectively remove those Peers from the "wild" and they would no longer be in contact with other Peers. That would reduce the FBI's ability to identify additional Peers, and would more likely result in sink-holing only part of the botnet before fully identifying all of the infected Peers. Second, if the FBI IPs consume the entire Peer Lists, it could alert the North Korean cyber actors who operate the botnet about the FBI's actions. That could cause them to employ counter-measures, including excluding the FBI IPs from the botnet, which would

also likely halt the FBI's ability to map the botnet before it is complete.

49. Each FBI IP will maintain a Push List, which may hold up to 50 entries and may contain the 15 FBI IPs as well as 35 other publicly available Joanap Peer IP addresses (the latter are the same type of IP addresses each Peer would ordinarily include). Each entry will include a port number as well as a timestamp that reflects the last contact with that Peer. Providing the FBI IPs via their own Push Lists will cause Peers to continue to contact FBI IPs through the duration of the search warrant and thus generate a current map at the end of the authorized period. It will also more accurately emulate the behavior of a true Joanap-infected Peer so that their behavior does not appear aberrant to the subjects controlling the botnet.

2. Execution of the Search Warrant

50. Execution of the search warrant will commence when the FBI IPs initiate connections with Peers in the Joanap botnet and issue commands to them. Specifically, each FBI IP will first initiate contact with two particular Peers, located in the United States, which are infected with the Joanap malware. The owners of each of those computers have consented to the FBI or another law enforcement agency monitoring communications on those computers (although not specifically to these connections for which the search warrant is sought).

51. As a result of those initial connections, the FBI IPs will be supplied with Push Lists from those two infected Peers. The FBI IPs will then use the results of those Push Lists to

initiate contact with and issue commands to other Peers for their Peer Lists. That in turn will cause the FBI IPs to be supplied with the Push Lists held by those Peers, and the process will continue to proceed in that manner.

52. As this cycle continues, the FBI IPs will learn the identities (i.e., the IP addresses) of new Peers in two ways: First, each FBI IP will receive the contents of other Peers' Push Lists and Receive Lists; and second, each FBI IP will begin to receive inbound commands from other Peers.

a. First, each time the FBI IP contacts a Peer and issues a Push Request or a Receive Request command, the FBI IP will receive that Peer's Push List or Receive List and thus a list of up to 50 other Peers.

b. Second, each time an FBI IP contacts a Peer (Peer A) and issues Request Commands, the FBI IP will also become an entry on that Peer's (Peer A's) Push List. When another Peer (Peer B) then contacts Peer A in the ordinary course of the botnet's communication, and sends a Push Request (or certain other commands), Peer B will be supplied with Peer A's Push List. Peer B will then sort and merge Peer A's Push List (with an FBI IP on it) into Peer B's Receive List. Peer B will then select one of the Peers from its own Receive List, which includes an FBI IP, to initiate another contact. Although the entry selected for connection from its Receive List by Peer B is random in any given instance, this protocol makes it likely that the FBI IP will eventually receive a contact initiated from Peer B.

53. The FBI IPs will use each of these sources of Peer IP addresses to initiate connections with Peers and issue Push Requests or Receive Requests to them. It is essential for the FBI IPs to widely populate or saturate Push Lists:

a. First, given that the update process occurs every three hours, having a significant presence (i.e., multiple FBI IPs on a given Push List) on numerous Push Lists allows the search warrant to take less time to fully map the botnet. (The FBI IPs will contact the list of IPs that they have collected from the sources discussed above -- shared Push Lists and Receive Lists, and inbound Peer connections -- more frequently than every three hours, but the FBI IPs cannot cause other infected Peers to contact another Peer more frequently than the periodic three-hour programmed schedule.)

b. Second, the FBI IPs must rely at least in part on receiving inbound connections from Peers in order to fully map the botnet. Because some Peers (NAT Peers) are behind a NAT or a firewall and are not publically accessible, they do not appear on other Peers' Peer Lists or Receive Lists. Therefore, the only way the FBI IPs will learn of NAT Peers' existence is when a NAT Peer attempts to contact an FBI IP, and the communication attempt is recorded. That, in turn, will occur only after the NAT Peer receives a Push List from another Peer that includes an FBI IP, and the NAT Peer incorporates the FBI IP into its Receive List.

54. This procedure will not take control of the Joanap botnet or disrupt its operation. As time progresses, however,

more and more Peers will incorporate the FBI IPs into their Receive Lists and Push Lists so that, according to current estimates, it is possible that most if not all of the Joanap botnet will connect with the FBI IPs during the 30-day period in the requested warrant. (As noted below, however, those estimates are based on assumptions and parameters that may vary from the actual characteristics of the Joanap botnet.)

55. Testing of the connections and commands between FBI IPs and Joanap-infected computers was performed in a security "sandbox," or a security mechanism for separating running programs, in an effort to mitigate system failures or vulnerabilities from spreading. FBI IPs and infected Joanap computers were also simulated in a "virtualized" environment and monitored. (A virtualized environment is one that emulates a computer system without containing all of the various hardware components that ordinarily make one up.) In this virtualized environment, FBI IPs were observed initiating contact and issuing commands, and supplying, receiving, and processing Peer Lists with infected Joanap virtual machines. Additionally, testing confirmed that FBI IPs were not able to initiate contact with NAT Peers and thus were not able to send Request Commands to them. Upon the conclusion of testing, the FBI estimated that it will take a minimum of 20 days for FBI IPs to identify 80 percent of the Joanap botnet on the Internet. That estimate is based upon assumptions and parameters that may not be accurate regarding the characteristics of the Joanap botnet, for example the percentage of Peers that are NAT Peers.

56. The FBI did not observe evidence indicating that use of the FBI IPs in the limited manner provided in the requested search warrant would interrupt or interfere with other processes of a computer infected by Joanap. I have learned from computer scientists and technical experts at the FBI that by executing the requested warrant and sending and receiving the limited types of communications permitted by the search warrant, the legitimate function of infected computers will not be compromised, interrupted, or degraded.

3. Evidence to be Collected

57. For each inbound connection to the FBI IPs, each FBI IP will record all of the inbound connections, including the IP address and port number, as well as the date and time of each such connection and other ancillary information exchanged through the Request Commands, as described in the requested warrant.

58. Each FBI IP will also record information, including the IP addresses and port number, from each of the Peer Lists it receives from other Peers, along with the date and time the Peer List was received and the IP address of the Peer from which it was received.

59. The FBI IPs will also record all commands sent to it, along with the IP address sending them, regardless of whether those commands are Push Requests (to which it will respond) or other commands (to which it will not).

VI. DELAYED NOTICE, SEALING, AND EXECUTION AT ANY TIME OF DAY

60. Pursuant to Section 3103a(b), and 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 as normally required until August 31, 2018.

61. Based upon the information provided in this Affidavit, my training and experience, and discussions with other Special Agents of the FBI, allowing premature disclosure to the public at large or to individual users of Joanap-infected computers would likely jeopardize the ongoing investigation. Such a disclosure would reveal that the government was mapping the Joanap botnet network, and the means by which it was doing so. This could prompt the subjects to make changes to the Joanap malware, which could then propagate across the botnet and prevent the FBI IPs from inserting themselves into the botnet. That would therefore prevent the FBI from mapping the botnet and determining the identity of all of the infected computers.

62. Premature disclosure, to the public or to individual victims, could also truncate the FBI's ability to map the entire network because in order for the FBI's execution of the requested warrant to be effective, the botnet needs to be sufficiently saturated with FBI IPs so that the update process will allow all Peers, including those behind NAT devices or firewalls, to connect with FBI IPs. Moreover, inasmuch as the Joanap-infected computers in the botnet serve as staging

infrastructure for other attacks, limiting the FBI's ability to fully map the botnet would interfere with the FBI's ability to identify other intrusions and related activities that may be discovered after each of the Joanap-infected peers is identified and the activity related to those IP addresses is assessed.

63. The investigation is ongoing, and immediate disclosure of the warrant will compromise that investigation. There is therefore reasonable cause to believe that notice or disclosure will result in flight from prosecution, destruction of or tampering with evidence, and will otherwise seriously jeopardize the investigation. 18 U.S.C. § 2705(a)(2)(B), (C), (E).

64. As this warrant seeks delayed notice pursuant to Title 18, Untied States Code, Section 3103a, it does not seek authorization to seize any tangible property. In addition to delaying notice, pursuant to Title 18, United States Code, Section 3103a(b)(2), reasonable necessity exists to seize stored electronic information and electronic communications found on Peers that connect with the FBI IPs, i.e., the Push Lists and Receive Lists that the FBI IPs receive from other Peers.

65. Specifically, as noted above, there are only two ways that the FBI IPs will identify Peers in the Joanap botnet, and one of them is through acquisition of the Push Lists and Receive Lists stored on infected Peers. It is essential to acquire the IP addresses of Peers through both means -- observing inbound connections and receiving Push Lists and Receive Lists -- because illuminating the Joanap botnet would take significantly longer if FBI IPs could only initiate connections to known Peers

without learning about new Peers through Push Lists and Receive Lists. Each Push List and each Receive List contains up to 50 new Peers, whereas an FBI IP initiating a single outbound connection to another Peer places that FBI IP on just one other Peer's Push List, which will then need to be propagated further before any new Peer will connect with the FBI IP. Proceeding by initiating connections alone and not receiving Push Lists and Receive Lists would therefore limit the FBI's ability to fully map the Joanap network, given how infrequently (every three hours) Peers initiate connections using their Receive lists. Moreover, the FBI's current estimate that 80 percent of the botnet may be mapped in 20 days is based upon both obtaining Peer Lists through commands, and propagating the FBI IPs through the exchange of commands. Both methods must be used in order to map the botnet as quickly as possible.

66. Furthermore, there is good cause for the order to be issued such that the warrant may be executed at any time of the day or night. As noted above, Peers will initiate contact once every three hours, irrespective of the time of day. Moreover, it is essential for the FBI IPs to saturate the botnet quickly in order to maximize the probability that the FBI will be able to complete the search by mapping the botnet within the 30-day period. Finally, inasmuch as the Peers are computers that are infected unbeknownst to the users of those computers (except in rare instances, such as security researchers), and the activity of the Joanap malware occurs without the user being aware of it,

executing the search warrant during the night time versus the day time will make little difference to the user of any Peer.

67. While the FBI seeks authorization to delay notice, during the period of delayed notice the FBI 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.

VII. CONCLUSION

68. For all of the above reasons, there is probable cause to believe that the evidence to be requested through the requested search warrant executed within, and being investigated within, the Central District of California, will constitute or yield evidence of violations of the offenses listed above.

/s/
Chade Chowana-Bandhu
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me this 11th day of June, 2018.

/s/
UNITED STATES MAGISTRATE JUDGE
FREDERICK F. MUMM