

1 NICOLA T. HANNA
United States Attorney
2 PATRICK R. FITZGERALD
Assistant United States Attorney
3 Chief, National Security Division
ANTHONY J. LEWIS (Cal. Bar No. 231825)
4 Assistant United States Attorney
Deputy Chief, Terrorism and Export Crimes Section
5 ANIL J. ANTONY (Cal. Bar No. 258839)
Assistant United States Attorney
6 Cyber & Intellectual Property Crimes Section
1500 United States Courthouse
7 312 North Spring Street
Los Angeles, California 90012
8 Telephone: (213) 894-1786/6579
Facsimile: (213) 894-2927/8601
9 E-mail: anthony.lewis@usdoj.gov
anil.j.antony@usdoj.gov

10 Attorneys for Applicant
11 UNITED STATES OF AMERICA

12 UNITED STATES DISTRICT COURT
13
14 FOR THE CENTRAL DISTRICT OF CALIFORNIA

15 IN RE: BOTNET OF COMPROMISED
16 COMPUTERS

No. 18-MJ-02739

17 GOVERNMENT'S EX PARTE APPLICATION
18 FOR A WARRANT PURSUANT TO FED. R.
19 CRIM. P. 41(b)(6)(B) AND ORDER
20 PURSUANT TO 18 U.S.C. § 3123
21 AUTHORIZING THE CONNECTION TO
22 COMPROMISED COMPUTERS AND REQUEST
23 TO SEAL; AFFIDAVIT OF CHADE
24 CHOWANA-BANDHU

25
26
27
28
(UNDER SEAL)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

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

16 In addition to identifying the IP addresses of computers
17 infected by the Joanap malware, the requested warrant will allow the
18 FBI to obtain other limited information regarding the connection,
19 such as the port and the date and time of the connection. In some
20 instances, the IP addresses of infected computers will be observed
21 as those computers connect directly to the FBI IPs; in other
22 instances the IP addresses of Peers will be discovered when a Peer
23 supplies the FBI IPs with its "Peer Lists" -- the lists kept by the
24 malware containing the IP addresses of other known Peers -- i.e.,
25 other computers infected with this North Korean malware. (See Orig.
26 Aff. ¶¶ 39-41.) The information obtained by the FBI IPs from other
27 Peers will be limited to information resulting from basic commands
28

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

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

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

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

1 This application seeks authorization to execute the requested
2 warrant anywhere within the United States pursuant to Federal Rule
3 of Criminal Procedure 41(b)(6)(B), and, for good cause shown, at any
4 time of the day or night pursuant to Rule of Criminal Procedure
5 41(e)(2)(A)(ii).

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

19 **II. PEN REGISTER AND TRAP AND TRACE PROVISIONS**

20 As noted above and in the Affidavit, in the course of
21 executing the requested search warrant, computers infected with
22 Joanap will connect with the FBI IPs, and the FBI IPs will then
23 record the IP addresses of those computers along with other dialing,
24 routing, addressing, and signaling information pursuant to a pen
25
26
27
28

1 register and trap and trace device.¹ (E.g., Orig. Aff. ¶ 52.b.)

2 Based on the certification filed herewith and the facts contained in
3 the Affidavit, and pursuant to Title 18, United States Code,
4 Sections 3122 and 3123, the government seeks as part of the
5 requested search warrant authorization for the following:

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

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

22 ¹ It is not clear that the Pen Register and Trap and Trace Act's
23 prohibition against the "installation" or "use" of a "pen register"
24 or "trap and trace device" necessarily applies to the facts
25 presented to the Court here. See, e.g., Capital Records Inc. v.
26 Thomas-Rasset, 2009 WL 1664468, at *3 (D. Minn. 2009) ("[T]he Pen
27 Register Act cannot be intended to prevent individuals who receive
28 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.

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

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

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

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

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

23 At the time of the Second Renewal Warrant, the IP addresses
24 discovered through using historical consensually monitored computer
25 activity had not significantly enhanced the FBI's ability to
26 discover Peers. In particular, the IP addresses revealed from
27 historical consensually monitored computer activity were either
28

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

4 As a result, in the Second Renewal Warrant, the warrant added
5 one additional criteria in identifying computers that will be
6 searched. Specifically, the warrant allowed the search of computers
7 that had certain ports (or channels) open and that met other
8 criteria. The Joanap malware used certain ports for its
9 communications that were traditionally used for other types of
10 internet traffic, such as web browsing and email communications,
11 likely as a measure to conceal the malicious traffic and make it
12 appear like other legitimate traffic. The FBI used third-party data
13 sets to examine which IP addresses had those specific ports open,
14 and also which of those IP addresses did not behave the way that
15 computers would if they were communicating on that port with
16 whatever the "traditional" use of that port was. The Second Renewal
17 Warrant allowed the FBI to search a computer that: (a) had at least
18 one of three specific ports open, which ports were programmed into
19 Joanap for its communications; (b) the use that port was not the
20 traditional use of those ports based on how the computers behaved;
21 (c) the computer responded to an initial cryptographic
22 authentication step performed by the FBI to determine that the
23 computer was infected with Joanap. This process is described in
24 greater detail in paragraphs 9-21 of the Third Supplemental
25 Affidavit. Multiple new IP addresses were discovered by using this
26 technique. (4th Supp. Aff. ¶ 11.)
27
28

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

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

20
21 ///
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

1
2 **AFFIDAVIT**

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

5 **I. INTRODUCTION**

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

20 **II. PURPOSE OF AFFIDAVIT**

21 2. This affidavit is made in support of an application
22 for a warrant that will reveal the Internet Protocol ("IP")
23 addresses of computers that are infected with a specific type of
24 malware, referred to herein and in published research as
25 "Joanap." This affidavit supplements and incorporates by
26 reference the attached affidavit to which I swore on September
27 21, 2018 (the "Third Supplemental Affidavit" or "3d Supp.
28 Aff."), which was submitted in support of a search warrant

1 issued that day (the "Third Renewal Warrant") by the Honorable
2 Michael R. Wilner, United States Magistrate Judge, in Case No.
3 2:18-MJ-02506. That affidavit, in turn, incorporates by
4 reference the attached affidavits to which I swore: on August
5 15, 2018 (the "Second Supplemental Affidavit" or "2d Supp.
6 Aff."), which was submitted in support of a search warrant
7 issued that day by the Honorable Michael R. Wilner, United
8 States Magistrate Judge, in Case No. 2:18-MJ-2115; on July 24,
9 2018 (the "First Supplemental Affidavit" or "1st Supp. Aff."),
10 which was submitted in support of a search warrant issued that
11 day ("First Renewal Warrant") by the Honorable Frederick F.
12 Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01904;
13 and on June 11, 2018 (the "Original Affidavit" or "Orig. Aff."),
14 which was submitted in support of the search warrant issued that
15 day (the "Original Warrant") by the Honorable Frederick F. Mumm,
16 United States Magistrate Judge, in Case No. 2:18-MJ-01497.

17
18 3. The requested warrant would allow the search of
19 infected computers to continue for an additional period of
20 thirty days according to the same terms and provisions
21 previously authorized, for the reasons described below.

22 4. The facts described and nomenclature used in the
23 Original Affidavit are assumed below. The facts in the Original
24 Affidavit, First Supplemental Affidavit, Second Supplemental
25 Affidavit, and Third Supplemental Affidavit remain true (except
26 as specifically noted below) and establish probable cause for
27 the requested renewed search warrant. Set forth below are
28

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

3
4 **A. Execution of the Original Warrant and First, Second,**
5 **and Third Renewal Warrants and Information Obtained as**
6 **a Result**

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

12 1. Background on Execution of the Warrants and
13 Orders

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

25 _____
26 ¹ The Original Affidavit described both Push Requests, which
27 are requests to obtain Push Lists, and Receive Requests, which
28 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.

1
2 7. The Original Warrant allowed the FBI to search a
3 computer (by requesting its Peer List) if the computer was
4 identified through consensual monitoring, through another Peer's
5 Peer List, or if the Peer initiated a connection with an FBI IP.
6 The number of Peers that were subsequently identified remained
7 below the numbers predicted based on modeling performed by the
8 FBI and AFOSI personnel. (See Orig. Aff. ¶¶ 45, 55.) As a
9 result, two additional criteria were authorized to use by the
10 FBI when identifying computers that could be searched.

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

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

1 other types of internet traffic, such as web browsing and email
2 communications. The selection of ports used for other ordinary
3 purposes was likely a measure designed to conceal the malicious
4 traffic and make it appear like other legitimate traffic. The
5 FBI used third-party data sets to examine which IP addresses had
6 those specific ports open, and also which of those IP addresses
7 did not behave the way that computers would if they were
8 communicating on that port with whatever the "traditional" use
9 of that port was.
10

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

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

1 abnormal termination message, and since the Third Renewal
2 Application they all have been vetted and only one IP address
3 was successfully authenticated as a Joanap Peer.² (See 3d Supp.
4 Aff. ¶¶ 20-20.b.)
5

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

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

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

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

1 that a Peer that is publicly available can and does at times
2 behave as a client and initiates connections with other Peers,
3 for example to request new Peer Lists. Those Peer Lists (Push
4 Lists specifically, Orig. Aff. ¶ 40.a) contain the IP address
5 and open port for other publicly available Peers. The inverse
6 is not true: A NAT Peer cannot receive initial inbound
7 connections.
8

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

15 15. The issue that had arisen in the way the FBI IPs were
16 executing the searches is that when other Peers contacted the
17 FBI IPs, the FBI IPs inadvertently always informed the clients
18 that the clients were not publicly accessible, even when they
19 were. Because of the way the Joanap malware operates, that
20 caused a Peer ("Peer A" here) that in fact was publicly
21 accessible to "believe" it was not publicly accessible, which in
22 turn prompts Peer A to close the port it had been using to
23 receive inbound connections from other Peers. Only when Peer A
24 initiated a connection with another non-FBI Peer ("Peer B")
25 would it learn that it was in fact publicly available, but at
26 that point the Peer would use a different port to receive
27 connections. All the other Peers that had stored Peer A's IP
28

1 address with the old port number (now closed) would not be able
2 to connect successfully with Peer.
3

4 16. Through additional exchanges, this issue works itself
5 out with some time. Peer A, having been informed by the FBI IPs
6 that it was not publicly available, would inevitably contact
7 another server Peer (Peer B), and Peer B would record the new,
8 correct port number with Peer A's IP address, and propagate that
9 information to other client Peers that contacted Peer B. Those
10 clients could then successfully connect with Peer A. But the
11 FBI IPs have been propagating through the botnet such that up to
12 15 IP addresses on each Peer List of 50 IP addresses are FBI
13 IPs. (Orig. Aff. ¶ 47.) Each Peer selects an IP address
14 randomly from its Receive List every three hours to make
15 contact. (Id. ¶ 45.) That means that server Peers that have
16 been in communication with the FBI IPs will periodically
17 reconnect with FBI IPs. And each time an FBI IP contacts Peer
18 A, the FBI IP would inform Peer A that Peer A was not publicly
19 accessible, and the process would repeat.

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

1 11 of the server Peers are newly identified since the code was
2 patched on September 24, 2018.³ The fact that new servers have
3 been identified, however, means that additional time is
4 warranted to determine whether those servers lead to additional
5 Peers. As described in the Original Affidavit: the FBI IPs
6 first make contact with a server Peer; as a result, the FBI IPs
7 become entries on that server's Push List; when other Peers
8 contact that server, they will receive the Push List containing
9 the FBI IPs; and those Peers will then initiate contact with the
10 FBI IPs. (Original Affidavit ¶¶ 45, 53-53.b, 67.) Because a
11 Peer only initiates contact every three hours pursuant to the
12 peer-to-peer functionality, that propagation process takes time.
13 (Id.)

14
15 18. The reason that additional time is needed to continue
16 mapping the botnet is because some time is needed to restore and
17 stabilize the connections between Peers. For example, if a
18 cluster of Peers had been in contact with Peer A, they may have
19 lost contact with Peer A when Peer A jumped to a new port after
20

21 ³ The Third Supplemental Affidavit noted that by September
22 17, 2018, approximately 1,788 unique IP addresses had been
23 identified, though only approximately 82 were publicly
24 accessible (and not NAT Peers) and acting as "servers" that
25 would supply Push Lists to other Peers. Due to a separate
26 coding issue, the scripts used to operate the FBI IPs had
27 recorded the results of the authentication step as "passed" even
28 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.

1 contact with an FBI IP. Within that cluster may be other server
2 Peers, that in turn were in touch with other clusters of Peers.
3 The result is that the botnet requires time to re-establish the
4 connections that may have been interrupted by the coding issue.
5 When that occurs, the FBI IPs will be able to propagate further
6 and illuminate any parts of the botnet whose connection with the
7 FBI IPs via Peer A (and other server Peers) had been severed.
8 Because each Peer only checks its own Receive List every three
9 hours, that process requires some time to complete, which is the
10 reason for requesting an additional thirty days to conduct the
11 searches authorized by the requested warrant.
12

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

15 19. For all of the reasons set forth in the Original
16 Affidavit, the government seeks authority to delay notice of the
17 warrant, that the warrant, application, and affidavit be filed
18 under seal, and that the FBI and AFOSI be able to execute the
19 search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In
20 executing the search warrant, FBI and AFOSI personnel have not
21 observed any indication that any of the subjects have been
22 alerted to the presence of the FBI IPs in the Joanap botnet.
23 Alerting them to the existence of the search warrant would
24 likely cause the adverse results described in the Original
25 Affidavit. (Id.) The Original Warrant and First Renewal
26 Warrant sought to delay notification until August 31, 2018;
27 those two periods of delay have been continued until November 7,
28 2018 by order of the Court, and the Second Renewal Warrant

1 authorized a delay of notification until November 7, 2018. This
2 requested search warrant and order also seek to delay
3 notification until January 30, 2019.
4

5 **III. CONCLUSION**

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

11 _____
12 Chade Chowana-Bandhu
13 Special Agent
Federal Bureau of Investigation

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

16 _____
UNITED STATES MAGISTRATE JUDGE
17
18
19
20
21
22
23
24
25
26
27
28

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

1 day (the "Second Renewal Warrant") by the Honorable Michael R.
2 Wilner, United States Magistrate Judge, in Case No. 2:18-MJ-
3 02115. This affidavit, in turn, incorporates by reference the
4 attached affidavit to which I swore on July 24, 2018 (the "First
5 Supplemental Affidavit" or "1st Supp. Aff."), which was
6 submitted in support of a search warrant issued that day ("First
7 Renewal Warrant") by the Honorable Frederick F. Mumm, United
8 States Magistrate Judge, in Case No. 2:18-MJ-01904, and the
9 affidavit to which I swore on June 11, 2018 (the "Original
10 Affidavit" or "Orig. Aff."), which was submitted in support of
11 the search warrant issued that day (the "Original Warrant") by
12 the Honorable Frederick F. Mumm, United States Magistrate Judge,
13 in Case No. 2:18-MJ-01497.

14
15 3. The requested warrant would allow the search of
16 infected computers to continue for an additional period of
17 thirty days according to the same terms and provisions
18 previously authorized.

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

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

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

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

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

28 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.

1 unique IP addresses had been identified, with 18 that were
2 publicly accessible and acting as servers. By August 3, 2018,
3 over 900 unique IP addresses had been identified, though only
4 approximately 42 were publicly accessible (and not NAT Peers)
5 and acting as "servers" that would supply Push Lists to other
6 Peers.³ By September 17, 2018, approximately 1,788 unique IP
7 addresses had been identified, though only approximately 82 were
8 publicly accessible (and not NAT Peers) and acting as "servers"
9 that would supply Push Lists to other Peers.
10

11 7. The First Renewal Warrant authorized the FBI to
12 continue searching computers the same way it had under the
13 Original Warrant, and also permitted to the FBI to connect with
14 IP addresses that were discovered through historical
15 consensually monitored activity of computers infected with
16 Joanap. (1st Supp. Aff. ¶¶ 10-13.) The results did not assist
17 the FBI in identifying new Peers. Out of over 200 IP addresses
18 identified through historical consensually monitored computer
19

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

24 ³ It should be noted that references to the number of unique
25 IPs operating as servers (42 in this reference) do not appear to
26 be 42 concurrently running machines. Because the way the search
27 warrant is executed using specific commands in Joanap's
28 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.

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

5
6 8. According to the FBI and AFOSI personnel executing the
7 search warrant, the number of new Peers being identified had
8 been leveling off. The number of Peers that have been
9 identified to date remain below the numbers predicted based on
10 modeling performed by the FBI and AFOSI personnel as well. (See
11 Orig. Aff. ¶¶ 45, 55.) As described in the First Supplemental
12 Affidavit, one possible reason that the numbers of Peers are low
13 is because of a possible coding issue in the way the malware
14 maintains Peer Lists. (1st Supp. Aff. ¶ 10.) Specifically, the
15 inactive Peers do not appear to be “pruned” from the Peer Lists
16 effectively, and instead active Peers are pruned. (Id.) As a
17 result, it appeared that the FBI IPs were stuck in a “pocket” of
18 the botnet without being able to connect with or map the rest of
19 the botnet. (Id.)

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

1 Renewal Warrant retained those same criteria, and to expand them
2 to include one additional criteria, which is described in the
3 following paragraphs.
4

5 10. There are multiple companies that make available
6 publicly or for a fee the results of port-scanning IP addresses.
7 In addition to the IP addresses used to route traffic on the
8 internet, internet traffic also includes a "port." Once the
9 right IP address is located and the traffic is routed there, the
10 port is effectively a channel that allows the computer to
11 separate different kinds of internet traffic based on different
12 types of communication protocols. For example, web browsers
13 often communicate over port 80 or 8080, secure web browsing
14 often occurs over port 443, and certain email protocols use port
15 25, 110, or 143.

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

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

8
9 12. Joanap is configured to use 26 ports as preferred
10 listening ports (meaning that the port is open). The list
11 begins with ports 443, 110, 53, and 80, in that order of
12 preference. The traditional uses of those ports are: port 443
13 is used for HTTPS (or secure web browsing); port 110 is used for
14 POP3 (a protocol used for receiving email); port 53 is used for
15 DNS or Domain Name Service (used to translate a domain into an
16 IP address)⁴; and port 80 is used for ordinary web traffic.
17 Using ports that are traditionally utilized for other types of
18 traffic is a common technique used by hackers to conceal their
19 connections as internet traffic that would otherwise appear to
20 be legitimate.

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

24
25 ⁴ The Domain Name Service, or "DNS," is a naming system for
26 computers, services, or any other resources connected to the
27 internet. An often-used analogy to explain the DNS is that it
28 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.

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

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

24 ⁵ DNS traditionally operates using User Datagram Protocol
25 (UDP). UDP is a "connectionless" protocol, not requiring any
26 packets to be acknowledged or verified. Transmission Control
27 Protocol (TCP) is a "connection oriented" stateful protocol
28 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

1
2 15. Even using only the IP addresses that (a) have one of
3 the three specified ports (443, 80, 110) open, and (b) provide a
4 premature session disconnection (indicating that the ports are
5 not being used for their intended purpose) yielded a significant
6 number of IP addresses. Data available in July 2018, for
7 example, shows that those criteria are satisfied for over
8 2,000,000 IP addresses for port 443, over 2,000,000 IP addresses
9 for port 80, and over 750,000 IP addresses for port 110.

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

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

1 certain, standard encryption system (referred to as RC4), and
2 using the encryption key contained in the Joanap malware. If
3 the client is able to decrypt that value, then the client will
4 send an encrypted message, where the known plain text that is
5 encrypted is "https://www.google.com/index.h". If the server
6 decodes that message to match the plain text written above, then
7 each node is satisfied that they are both Joanap Peers.
8

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

1 any of its own information--at most it would return information
2 sent to it by the FBI or AFOSI (after encrypting it).
3

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

21 19. Even after an IP address has satisfied each of those
22 three criteria, as with every other connection made by the FBI
23 IPs, each connection to Peers identified by any means pursuant
24 to the search warrant will be initiated with an authentication
25 step to determine if the computer is a Peer in fact infected
26 with Joanap. (Orig. Aff. ¶ 44.) Only if the computer passes
27 the authentication step will the FBI IP continue with a Request
28

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

3
4 20. As noted above in paragraph 15, data available in July
5 2018 shows that open port and the abnormal termination message
6 are satisfied for over 2,000,000 IP addresses for port 443, over
7 2,000,000 IP addresses for port 80, and over 750,000 IP
8 addresses for port 110. The following details were compiled as
9 of September 17, 2018:

10 a. Out of the over 750,000 IP addresses with port
11 110 open and abnormal termination message (according to the
12 third-party port-scanned data sets), 3 were successfully
13 authenticated as Joanap peers. Approximately two million IP
14 addresses have port 443 open and abnormal termination message,
15 and out of those, 25 have been successfully authenticated as
16 Joanap peers. Approximately two million IP addresses have port
17 80 open and abnormal termination message, and out of nearly
18 500,000 that have been tested with just the first authentication
19 step, 3 have been successfully authenticated as Joanap peers.

20 b. As noted above, three IP addresses were
21 successfully authenticated as Peers that had port 80 and port
22 110 open; not only are those 3 IP addresses the same, but they
23 are among the twenty-five authenticated peers that had port 443
24 open. Those three IP addresses moreover behaved abnormally:
25 none of those 3 IP addresses returned a Peer List when it was
26 requested, and it is abnormal for an infected Peer to be
27 operating on more than one port, as Joanap typically only
28 operates using a single port. Aside from these 3 IP addresses,

1 out of the remaining 22 that were authenticated using port 443,
2 7 failed when a Peer List was requested (meaning no Peer List
3 was provided), 2 had not yet had their Peer Lists requested, and
4 13 successfully returned a Peer List. At least some of IP
5 addresses contained in the Peer Lists received from the
6 authenticated Peers had not previously been discovered through
7 the execution of the search warrant.
8

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

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

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

3 23. For all of the reasons set forth in the Original
4 Affidavit, the government seeks authority to delay notice of the
5 warrant, that the warrant, application, and affidavit be filed
6 under seal, and that the FBI and AFOSI be able to execute the
7 search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In
8 executing the search warrant, FBI and AFOSI personnel have not
9 observed any indication that any of the subjects have been
10 alerted to the presence of the FBI IPs in the Joanap botnet.
11 Alerting them to the existence of the search warrant would
12 likely cause the adverse results described in the Original
13 Affidavit. (Id.) The Original Warrant and First Renewal
14 Warrant sought to delay notification until August 31, 2018;
15 those two periods of delay have been continued until November 7,
16 2018 by order of the Court, and the Second Renewal Warrant
17 authorized a delay of notification until November 7, 2018. This
18 requested search warrant and order also seek to delay
19 notification until November 8, 2018.

20 **III. CONCLUSION**

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

24 ///
25
26
27
28

1 within, the Central District of California, will constitute or
2 yield evidence of violations of the offenses listed above.
3

4 /s/
5 Chade Chowana-Bandhu
6 Special Agent
7 Federal Bureau of Investigation

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

10 
11 UNITED STATES MAGISTRATE JUDGE
12 MICHAEL R. WILNER
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit

Second Supplemental Affidavit

1
2 AFFIDAVIT

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

5 I. INTRODUCTION

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

20 II. PURPOSE OF AFFIDAVIT

21 2. This affidavit is made in support of an application
22 for a warrant that will reveal the Internet Protocol ("IP")
23 addresses of computers that are infected with a specific type of
24 malware, referred to herein and in published research as
25 "Joanap." This affidavit supplements and incorporates by
26 reference the attached affidavit to which I swore on July 24,
27 2018 (the "First Supplemental Affidavit" or "1st Supp. Aff."),
28 which was submitted in support of a search warrant issued that

1 day ("First Renewal Warrant") by the Honorable Frederick F.
2 Mumm, United States Magistrate Judge, in Case No. 2:18-MJ-01904.
3 That affidavit, in turn, attaches the affidavit to which I swore
4 on June 11, 2018 (the "Original Affidavit" or "Orig. Aff."),
5 which was submitted in support of the search warrant issued that
6 day (the "Original Warrant") by the Honorable Frederick F. Mumm,
7 United States Magistrate Judge, in Case No. 2:18-MJ-01497.
8

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

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

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

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

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

9 6. In executing the search warrant, the FBI IPs have
10 discovered new Peers. For example, by August 3, 2018, over 900
11 unique IP addresses had been identified, though only
12 approximately 42 were publicly accessible (and not NAT Peers;
13 see Orig. Aff. ¶¶ 42, 53.b) and acting as "servers" that would
14 supply Push Lists to other Peers; one such Peer was located in
15 the Central District of California. It should be noted that the
16 42 unique IPs operating as servers do not appear to be 42
17 concurrently running machines. Because the way the search
18 warrant is executed using specific commands in Joanap's
19 vocabulary, the specific device identifier is not reflected in
20 the communications identified in the exchanges between Peers,
21 only the IP address assigned to it and the port it is using.
22 Moreover, some of the IP addresses of the Peers acting as
23 servers are similar, indicating they are part of the same block

24
25 ¹ The Original Affidavit described both Push Requests, which
26 are requests to obtain Push Lists, and Receive Requests, which
27 are requests to obtain Receive Lists. (Orig. Aff. ¶¶ 43.a,
28 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.

1 of IP addresses used by the same network that re-assigns IP
2 usage to different computers. For these reasons, it is
3 estimated that there are far fewer unique Joanap servers amongst
4 those 42 unique addresses that are publicly facing.
5

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

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

20 **B. New Provisions in the Requested Warrant**

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

1 the malware maintains Peer Lists. (1st Supp. Aff. ¶ 10.)
2 Specifically, the inactive Peers do not appear to be "pruned"
3 from the Peer Lists effectively, and instead active Peers are
4 pruned. (Id.) As a result, it appears likely that the FBI IPs
5 are stuck in a "pocket" of the botnet without being able to
6 connect with or map the rest of the botnet. (Id.)
7

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

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

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

27 12. There are multiple companies that make available
28 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

1 separate different kinds of internet traffic based on different
2 types of communication protocols. For example, web browsers
3 often communicate over port 80 or 8080, secure web browsing
4 often occurs over port 443, and certain email protocols use port
5 25, 110, or 143.

6
7 13. Port-scanning refers to the process of checking
8 whether various ports on a computer are "open" and available to
9 communicate or not. Not only will port-scanning results show
10 whether a port is open or not, the computer conducting the scan
11 can make an initial data request to the open port. This initial
12 request solicits data which is routinely provided once a client
13 connects to the server's port. That data is often referred to
14 as a "banner," providing the client with the initial information
15 necessary to continue engaging the application bound to that
16 port on the server. The companies that conduct the scans of
17 these ports also make publicly available the results of the
18 banner produced by the server once the connection is
19 established. Banners can include host names, server software
20 version numbers, and digital certificate information required to
21 establish a secure connection. Additionally, if a port is found
22 to be open, but abnormality occurs, the abnormality information
23 may be logged. Abnormalities can include premature termination
24 (no banner presented) and invalid banner information (indicating
25 that software other than what is expected is running on the
26 server port).

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

1 begins with ports 443, 110, 53, and 80, in that order of
2 preference. The traditional uses of those ports are: port 443
3 is used for HTTPS (or secure web browsing); port 110 is used for
4 POP3 (a protocol used for receiving email); port 53 is used for
5 DNS or Domain Name Service (used to translate a domain into an
6 IP address)²; and port 80 is used for ordinary web traffic.
7 Using ports that are traditionally utilized for other types of
8 traffic is a common technique used by hackers to conceal their
9 connections as internet traffic that would otherwise appear to
10 be legitimate.
11

12 15. The FBI and AFOSI will therefore use the publically
13 available port-scanning data to discern which IP addresses have
14 these ports open. That alone, however, can be filtered further.
15 Specifically, many of the IP addresses that have those ports
16 open will be using them in a traditional way. For example, an
17 IP address with an open port 443 may be a legitimate web server.
18 Where it is a legitimate web server, however, the port-scanning
19 data will reflect a legitimate banner used by clients to
20 communicate with encrypted HTML sockets (443) and plain text
21 HTML sockets (80). In the case of a mail server (110),
22 traditional mail server banner information would be provided.
23 Thus, only those IP addresses where (a) the specified port is
24

25 ² The Domain Name Service, or "DNS," is a naming system for
26 computers, services, or any other resources connected to the
27 internet. An often-used analogy to explain the DNS is that it
28 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.

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

5
6 16. One of these ports will not be used in the requested
7 warrant: port 53. The reason for that is because port 53
8 traditionally hosts Domain Name Service or DNS, as noted above.
9 DNS services utilize a protocol that does not provide the
10 connection termination message required to detect an abnormal
11 termination. Therefore the port-scanning data does not provide
12 a means of discriminating between legitimate or traditional use
13 of port 53 and instances in which the port is open because of an
14 abnormality--such as infection with the Joanap malware.³

15 17. Even using only the IP addresses that (a) have one of
16 the three specified ports (443, 80, 110) open, and (b) provide a
17 premature session disconnection (indicating that the ports are
18 not being used for their intended purpose) yields a significant
19 number of IP addresses. Data available in July 2018, for
20 example, shows that those criteria are satisfied for over
21 2,000,000 IP addresses for port 443, over 2,000,000 IP addresses
22 for port 80, and over 750,000 IP addresses for port 110.

23 ³ DNS traditionally operates using User Datagram Protocol
24 (UDP). UDP is a "connectionless" protocol, not requiring any
25 packets to be acknowledged or verified. Transmission Control
26 Protocol (TCP) is a "connection oriented" stateful protocol
27 utilized for Web (443) and Mail (SMTP) and provides the
28 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.

1
2 18. That list, however, will be further narrowed down. As
3 described in the Original Affidavit, in the ordinary course of
4 how Joanap's peer-to-peer functionality operates, a Peer
5 initiating a connection (the "client") sends a pseudo-random
6 string of text that the other Peer (acting as the "server")
7 returns encrypted to the client. The client then sends an
8 encrypted message with known plain text. If the server can
9 decode the known plain text correctly, the peer has performed a
10 cryptographic handshake and validates itself to the other Peer
11 (thus authenticating itself as a computer infected with Joanap).
12 (Orig. Aff. ¶ 44.) Specifically, when one Peer (a client)
13 initiates a connection to another Peer (a server), the client
14 will first send a very small (4-byte) value. The client will
15 then send a 16-byte pseudorandom value to the server. The
16 server will then send back to the client the 16-byte value that
17 has been encrypted. That 16-byte value is encrypted with a
18 certain, standard encryption system (referred to as RC4), and
19 using the encryption key contained in the Joanap malware. If
20 the client is able to decrypt that value, then the client will
21 send an encrypted message, where the known plain text that is
22 encrypted is "https://www.google.com/index.h". If the server
23 decodes that message to match the plain text written above, then
24 each node is satisfied that they are both Joanap Peers.

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

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

19
20 20. It should also be noted that using port-scanning data
21 is likely to allow the FBI to develop a more current and
22 complete map of the botnet because the information is more
23 recent than historically monitored activity. Different services
24 make data sets available that are more or less recent; for
25 example, one service makes data available that is one month old,
26 and another service makes data available that is one week old.
27 That is more likely to assist in generating a current map of the
28 botnet, and also to reveal other "pockets" of the broader botnet

1 that were not visible starting from the individual consensually
2 monitored IP addresses. That will be of particular assistance
3 given the way that Joanap "prunes" Peers on the Peer Lists it
4 maintains: starting with an up-to-date data set regarding which
5 IP addresses may be infected is more likely to overcome the FBI
6 IPs inability to "see" through fragmentation in the botnet that
7 may have occurred as a result of Peer Lists losing contact with
8 neighbors because of stale or outdated Peers.
9

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

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

21 22. For all of the reasons set forth in the Original
22 Affidavit, the government seeks authority to delay notice of the
23 warrant, that the warrant, application, and affidavit be filed
24 under seal, and that the FBI and AFOSI be able to execute the
25 search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In
26 executing the search warrant, FBI and AFOSI personnel have not
27 observed any indication that any of the subjects have been
28 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

Case 2:18-mj-01904-DUTY *SEALED* Document 12 *SEALED* Filed 07/24/18 Page 9 of 50
Page ID #:9

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

Case 2:18-mj-01904-DUTY *SEALED* Document 12 *SEALED* Filed 07/24/18 Page 10 of 50
Page ID #:10

1
2 "Original Warrant") by the Honorable Frederick F. Mumm, United
3 States Magistrate Judge, in Case No. 2:18-MJ-01497. The
4 requested warrant would allow the search of infected computers
5 to continue for an additional period of thirty days.

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

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

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

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

Case 2:18-mj-01904-DUTY-SEALED* Document 12-SEALED* Filed 07/24/18 Page 11 of 50
Page ID #:11

1
2 disconnected June 15 in connection with the owner relocating its
3 office and associated computer equipment.

4 6. The second of those monitored Peers was still being
5 monitored pursuant to consent, but the area where it was located
6 suffered a loss of internet connection beginning on June 8, 2018
7 that lasted until June 22, 2018. The FBI and AFOSI had tried to
8 connect to that monitored Peer between June 11, 2018 and June
9 22, 2018 but no connection could be made. On Sunday, June 24,
10 2018, the FBI and AFOSI successfully made contact with that
11 Peer. It provided a file that was one of its Peer Lists (the
12 Push List; see Orig. Aff. ¶ 40.a), but the file was empty of the
13 entries it would ordinarily contain (the IP address, port
14 number, and date and time stamp; see Orig. Aff. ¶ 40.a).¹

15 7. At that point, the FBI and AFOSI used the traffic that
16 had been monitored pursuant to consent from Saturday, June 23,
17 2018 that reflected the presence of Joanap on another Peer, and
18 the FBI and AFOSI made a connection with that Peer and requested
19 its Push List. The IP addresses in that Push List either did
20 not respond or failed the authentication step that initiates
21 communication using Joanap's protocols. (See Orig. Aff. ¶ 44.)
22 The FBI and AFOSI then identified another Peer from the
23 consensually monitored traffic on June 28, 2018 and obtained a
24 new Push List that identified new Peers.

25 ¹ Although the reason it supplied an empty Push List is not
26 yet known, it is most likely that the Push List was purged as a
27 result of system (and malware) being active but disconnected
28 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.

Case 2:18-mj-01904-DUTY *SEALED* Document 1 *SEALED* Filed 07/24/18 Page 12 of 50
Page ID #:12

1
2 8. Since that time, the FBI IPs have been both initiating
3 connections with IP addresses discovered from Peers' Push Lists
4 (and inserting themselves onto the Push Lists of those Peers),
5 and receiving inbound connections from other IP addresses,
6 presumably that received those Peers' Push Lists, as described
7 in the Original Affidavit.² (Orig. Aff. ¶ 52-52.b.)

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

24
25 ² The Original Affidavit described both Push Requests, which
26 are requests to obtain Push Lists, and Receive Requests, which
27 are requests to obtain Receive Lists. (Orig. Aff. ¶¶ 43.a,
28 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.

Case 2:18-mj-01904-DUTY *SEALED* Document 1 *SEALED* Filed 07/24/18 Page 13 of 50
Page ID #:13

1
2 servers are similar, indicating they are part of the same block
3 of IP addresses used by the same network that re-assigns IP
4 usage to different computers. For these reasons, it is
5 estimated that there are 8 or fewer unique servers amongst those
6 18 unique addresses.

7 **B. New Provisions in the Requested Warrant**

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

23 11. For this reason, the requested warrant seeks to use
24 additional criteria to identify a Peer that can be searched
25 pursuant to the warrant. The Original Warrant provided the
26 following with respect to how the FBI can identify a computer as
27 a member of the Joanap botnet that could be searched:
28

Case 2:18-mj-01904-DUTY *SEALED* Document 12 *SEALED* Filed 07/24/18 Page 14 of 50
Page ID #:14

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

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

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

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

27 14. For all of the reasons set forth in the Original
28 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

Case 2:18-mj-01904-DUTY *SEALED* Document 1 *SEALED* Filed 07/24/18 Page 15 of 50
Page ID #:15

1 search warrant at any time of day. (Orig. Aff. ¶¶ 60-67.) In
2 executing the search warrant, FBI and AFOSI personnel have not
3 observed any indication that any of the subjects have been
4 alerted to the presence of the FBI IPs in the Joanap botnet.
5 Alerting them to the existence of the search warrant would
6 likely cause the adverse results described in the Original
7 Affidavit. (Id.)
8

9 **III. CONCLUSION**

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

16 15/
17 Chade Chowana-Bandhu
18 Special Agent
19 Federal Bureau of Investigation

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

22 **Frederick F. Mumm**

23 UNITED STATES MAGISTRATE JUDGE
24
25
26
27
28

Exhibit

Original Affidavit

1
2 AFFIDAVIT

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

5 I. INTRODUCTION

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

20 II. PURPOSE OF AFFIDAVIT

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

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

1 computers compromised by Joanap. Joanap also contains a peer-
2 to-peer function that causes each infected computer to share
3 information with its "neighbor" peers so that each infected
4 computer contains a current (but not exhaustive) list of fifty
5 other computers that are compromised.
6

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

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

1 collectively as "Request Commands." Those Request Commands will
2 be sent by the FBI IPs. Each of these (and most other) Joanap
3 commands, in addition to requesting a Peer List, include at
4 least two other parts: first, an initial cryptographic
5 handshake is used to verify that the Peer is a Joanap-infected
6 computer, and thus that the two computers can communicate with
7 each other using Joanap's built-in set of commands; and second,
8 a "validation" is performed to determine whether the requesting
9 Peer is publically accessible on the Internet. During the
10 validation step, if a Peer is publically accessible, the
11 requesting Peer's IP address will be added to one of the
12 receiving Peer's Peer Lists. The FBI IPs initiating contact
13 with other Peers will have public Internet access, and will
14 cause their IP addresses to be incorporated into other Peer's
15 peer lists.
16

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

1
2 7. In order to effectively identify as much of the Joanap
3 botnet as possible, (a) the FBI IPs must communicate -- using
4 Request Commands -- with other Peers they have discovered, in
5 order for those Peers to incorporate the FBI IPs onto one of
6 their Peer Lists and spread the FBI IPs to other "neighbor"
7 Peers; (b) the FBI IPs will each record the IP addresses, their
8 respective port numbers, and date and times, of compromised
9 computers trying to connect with them; and (c) the FBI IPs will
10 request Peer Lists through their connections with other Peers in
11 order to identify additional Peers that the FBI IPs will
12 contact. The requested warrant is therefore sought pursuant to
13 Federal Rule of Criminal Procedure 41(b)(6)(B) and Title 18,
14 United States Code, Section 3123.

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

17 9. The requested warrant also seeks (a) authorization
18 under Title 18, United States Code, Section 3103a(b), for
19 reasonable cause shown below, to delay notification of the
20 proposed warrant until August 31, 2018 for the reasons described
21 below, and to permit the acquisition of electronic information
22 or electronic communications (specifically, the Peer Lists,
23 discussed below); (b) authorization under Federal Rule of
24 Criminal Procedure 41(b)(6)(B) to execute the warrant anywhere
25 within the United States; (c) authorization under Federal Rule
26 of Criminal Procedure 41(e)(2)(A)(ii) to execute the warrant at
27 any time of day or night.
28

1
2 10. As described in greater detail below, I respectfully
3 submit that there is probable cause to believe that IP addresses
4 and other information likely to be obtained during the period of
5 the requested warrant will constitute or yield evidence of
6 federal offenses, including specifically violations of Title 18,
7 United States Code, Section 1030(a)(5) (Causing Damage to
8 Protected Computers), being committed by subjects of the
9 investigation who are not yet identified.

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

23 III. LEGAL BACKGROUND

24 A. Jurisdiction to Issue Requested Search Warrant

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

1
2 a magistrate judge with authority in any district
3 where activities related to a crime may have occurred
4 has authority to issue a warrant to use remote access
5 to search electronic storage media and to seize or
6 copy electronically stored information located within
7 or outside that district if:

8

9 (B) in an investigation of a violation of 18 U.S.C.
10 § 1030(a)(5), the media are protected computers that
11 have been damaged without authorization and are
12 located in five or more districts.

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

16 (a) Whoever--

17 (5) (A) knowingly causes the transmission of a
18 program, information, code, or command, and as
19 a result of such conduct, intentionally causes
20 damage without authorization, to a protected
21 computer;

22 (B) intentionally accesses a protected computer
23 without authorization, and as a result of such
24 conduct, recklessly causes damage; or

25 (C) intentionally accesses a protected computer
26 without authorization, and as a result of such
27 conduct, causes damage and loss.

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

1 Joanap network that are both inside the United States and
2 outside the United States, the requested search warrant only
3 authorizes activities within the territory of the United States.
4

5 B. Delayed Notice

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

8 (b) Delay.--With respect to the issuance of any
9 warrant or court order under this section, or any
10 other rule of law, to search for and seize any
11 property or material that constitutes evidence of a
12 criminal offense in violation of the laws of the
13 United States, any notice required, or that may be
14 required, to be given may be delayed if--

12 (1) the court finds reasonable cause to believe that
13 providing immediate notification of the execution of
14 the warrant may have an adverse result (as defined
15 in section 2705, except if the adverse results
16 consist only of unduly delaying a trial);

15 (2) the warrant prohibits the seizure of any
16 tangible property, any wire or electronic
17 communication (as defined in section 2510), or,
18 except as expressly provided in chapter 121, any
19 stored wire or electronic information, except where
20 the court finds reasonable necessity for the
21 seizure; and

19 (3) the warrant provides for the giving of such
20 notice within a reasonable period not to exceed 30
21 days after the date of its execution, or on a later
22 date certain if the facts of the case justify a
23 longer period of delay.

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

24 An adverse result . . . is--

25 (A) endangering the life or physical safety of an
26 individual;

26 (B) flight from prosecution;

27 (C) destruction of or tampering with evidence;
28

1 (D) intimidation of potential witnesses; or

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

4 18. Here, the requested warrant provides for giving
5 notice on August 31, 2018, and prohibits, as part of the receipt
6 of the requested information, the seizure of any tangible
7 property and wire information or wire communications. 18 U.S.C.
8 § 3103a(b)(2). The requested warrant permits the seizure of
9 electronic information or electronic communications,
10 specifically the Peer Lists stored on Joanap-infected computers
11 and certain other information incidental to the exchange between
12 the FBI IPs and Peers, because the Affidavit sets forth
13 reasonable necessity to seize them. Id. (Aff. ¶¶ 64-65.) As
14 discussed later in the Affidavit, immediate notification of this
15 order to the user(s) of the compromised computers in the botnet
16 may have an adverse result. (Aff. ¶¶ 60-63.)

17 C. Execution and Means of Notice

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

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

1 provides that the period during which the FBI can complete its
2 execution of the search warrant will be a period of up to 30
3 days.
4

5 21. Finally, Federal Rule of Criminal Procedure
6 41(f)(1)(C) provides the following regarding notice of the
7 warrant and receipt:

8 For a warrant to use remote access to search
9 electronic storage media and seize or copy
10 electronically stored information, the officer must
11 make reasonable efforts to serve a copy of the warrant
12 and receipt on the person whose property was searched
13 or who possessed the information that was seized or
14 copied. Service may be accomplished by any means,
15 including electronic means, reasonably calculated to
16 reach that person.

17 22. The requested warrant specifically provides for notice
18 by electronic means or publication and other means reasonably
19 calculated to reach each such person.
20

21 IV. TERMINOLOGY

22 23. Botnet: A "botnet" is a network of computers that ,
23 cyber criminals have infected with malware that gives a cyber-
24 criminal access to each computer and allows a cyber-criminal to
25 control each computer remotely.
26

27 24. Compile date: A "compile date" is the date and time
28 on which source code was compiled into an executable file, also
called machine code or object code, which is time-stamped in the
file.
29

30 25. Dropper: A "dropper" file often behaves as an
31 "installer" of other pieces of malware. Droppers can install
32 other malware by downloading them from pre-configured locations,
33 for example by causing a victim computer to connect to a
34

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

7
8 26. Hashes: A "hash" value can be calculated for any
9 computer file by applying a one-way algorithm to the data
10 contained in the file. An MD5 hash is the name of one such hash
11 value generated by a particular algorithm. If any of the
12 content of the file is changed, even a change as minor as adding
13 an extra "space" character, the algorithm will produce a
14 different hash when it is applied to the file. Although there
15 is an extremely small possibility of two separate files
16 calculating the same hash (it has been proven by researchers to
17 be possible), when two files have the same hash value they are
18 assumed to be identical files, thus providing verification to a
19 very high degree of confidence that the two files are identical.

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

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

6
7 28. Malware: "Malware" is malicious computer software
8 intended to cause a victim computer to behave in a manner
9 inconsistent with the intention of the owner or user of the
10 victim computer, usually unbeknownst to the owner or user of the
11 victim computer.

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

15 V. FACTS

16 30. As described below, there is probable cause to believe
17 that the IP addresses to be discovered through the execution of
18 the search warrant are the IP addresses of computers infected
19 with the Joanap malware, and therefore are fruits, evidence, and
20 instrumentalities of Title 18, United States Code, Section
21 1030(a)(5) (Causing Damage to Protected Computers).

22 A. JOANAP

23 1. Background on Joanap

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

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

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

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

20 ² These characteristics describe the Joanap malware
21 generally. The execution of the warrant will begin when the FBI
22 IPs initiate connection with two computers that are in fact
23 members of the Joanap botnet, and will proceed to contact and
24 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.

25 ³ VirusTotal, which is owned by Google, is an online service
26 that analyzes files and URLs enabling the identification of
27 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

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

18
19 33. Based on my review of publicly available materials and
20 internal government reports, my discussions with other cyber
21 security professionals and with FBI experts, I have learned that
22 Joanap is a strain of malware that has been observed for many
23 years. It is referred to as a "second stage" malware, meaning
24 it is "dropped" by another malware. In the case of Joanap, it
25 has often been observed being dropped by an automated worm

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

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

9
10 34. Joanap grants malicious actors significant control
11 over victim computers within the botnet, including "root" level
12 access, which means access to all commands and files on a
13 computer. Some of the capabilities of the Joanap malware
14 include: registering itself as a service to operate discretely;

15
16 ⁴ Other public cyber security experts have previously
17 reported on this malware. The IT security firm Trend Micro has
18 written analytical reports on Brambul and Joanap, and identified
19 first receiving samples of Brambul on December 14, 2012 and
20 first receiving samples of Joanap on May 10, 2013. McAfee Labs
21 was able to identify certain email accounts as being recipients
22 of the credentials of infected computers sent by different
23 strains of the malware, although McAfee did not use the same
24 naming convention of "Brambul." See
25 [http://home.mcafee.com/virusinfo/virusprofile.aspx?key=570006#none](http://home.mcafee.com/virusinfo/virusprofile.aspx?key=570006#none;);
26 <http://home.mcafee.com/virusinfo/virusprofile.aspx?key=257183#none>.

27
28 ⁵ The Brambul worm spreads through self-replication by
infesting 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.

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

13
14 35. The Joanap botnet has historically provided North
15 Korean cyber actors with an extensive global infrastructure from
16 which they can facilitate computer network operations. The
17 Joanap botnet -- the network of infected computers -- provides a
18 global operational platform that North Korean cyber actors can
19 then put to use to further their hacking operations. Technical
20 Alert TA18-149A indicated that, since at least 2009, North
21 Korean cyber actors have likely been using both Joanap and
22 Brambul malware to target multiple victims globally and in the
23 United States -- including the media, aerospace, financial, and
24 critical infrastructure sectors. Evidence has also shown that
25 computers infected with Joanap were also infected with other
26 North Korean malware, showing that Joanap has been used by North
27 Korean cyber actors to stage other hacking operations.
28

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

20 37. Based on my training and experience, I know that when
21 malware like Joanap is detected, it requires costs to remediate
22 the computers and networks on which it is found. That is
23 particularly true where the Joanap malware itself as well as
24 other malware that the subjects of the investigation use Joanap
25 to install are capable of escalating privileges, copying
26 information, and executing commands on infected computers.
27 Therefore remediating the computers infected with the Joanap
28

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

3
4 2. Joanap's Peer-to-Peer Functionality

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

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

25
26
27
28

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

3
4 40. There are two types of Peer Lists maintained by Joanap
5 on an infected Peer. Each of the two lists serve different
6 purposes, and each is populated using different information:

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

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

18 ii. Thus, the Push List only contains "vetted"
19 IP addresses of Peers that are (a) publically accessible on the
20 Internet and (b) have affirmatively reached out to a Peer and
21 completed a successful exchange. This is one of the features
22
23

24 ⁶ In addition to IP addresses used to route traffic on the
25 internet, internet traffic will also include a "port." Once the
26 right IP address is located and the traffic is routed there, the
27 port is effectively a channel that allows the computer to
28 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.

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

3
4 iii. The Push List is kept in "volatile" or
5 "random access memory" ("RAM"), and is not stored in that form
6 on the infected Peer's hard drive. It is created through the
7 automatic operation of Joanap's peer-to-peer functionality, and
8 is not the result of action taken by the user of the computer,
9 nor would the user even know of its presence (unless for some
10 reason the user was aware of the infection, for example in the
11 case of a security researcher who was examining how Joanap
12 operated).

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

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

1
2 ii. While the Push List is requested and then
3 supplied in response to the periodic Push Requests that occur
4 automatically, the Receive Lists can be requested by another
5 command (a "Receive Request," described below). A Receive
6 Request in the ordinary course of the Joanap botnet is not
7 automatic and is generally performed by someone who would
8 manually send the command. It is, however, a command programmed
9 into and recognized by Joanap.

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

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

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

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

3
4 b. NAT Peers do, however, initiate contact with
5 other public Peers and issue commands (Push Requests) for those
6 Peers' Push Lists. This is because Joanap permits NAT Peers to
7 request and receive Push Lists from public Peers. Therefore, a
8 NAT Peer will maintain its own Receive List, consisting of Peers
9 from Push Lists supplied by other Peers.

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

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

24
25 ⁷ The commands are denoted as 0x2000 and 0x8000 series and
26 0x4002 commands. Each series command contains a "validating"
27 feature to determine public accessibility and a "request"
28 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.

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

9
10 i. On certain occasions dictated by Joanap's
11 protocol, a Peer may issue a specific type of Push Request that
12 prompts a distant Peer to also supply certain system information
13 in addition to supplying its Push List. In this case, Peer B
14 will respond to Peer A's request by supplying Peer A with its
15 Push List, and immediately afterwards supply its system
16 information, which may include its IP address, port number, MAC
17 address (Media Access Control, which is a device identifier),
18 operating system information, and CPU (central processing unit)
19 information. Although Joanap processes these commands in this
20 manner, FBI IPs will not issue this type of command to prompt
21 other Peers to reveal their system information. Conversely, FBI
22 IPs will disregard prompts to supply their system information,
23 and will respond to these commands by only supplying their Push
24 Lists.

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

1 supplied to the Peer issuing the command. FBI IPs will issue
2 Receive Requests to other Peers at various intervals to more
3 efficiently identify Peers and propagate themselves through the
4 botnet. In the event that any computers issue Receive Requests
5 to FBI IPs, those commands will be disregarded by the FBI IPs.
6

7 44. During these (and many other) commands between Joanap
8 Peers, when a Peer (Peer A) sends a command to another Peer
9 (Peer B), the Peers also exchange the port numbers to use for
10 their communications. Peer B uses a pseudo-random string of
11 text that is encrypted to perform a cryptographic handshake and
12 validate itself to Peer A (thus authenticating itself as a
13 computer infected with Joanap), and only after that -- in the
14 case of a Push Request -- Peer B will provide Peer A with its
15 Push List. In addition to these exchanges, the Peers exchange
16 certain ancillary information while performing the commands.⁹

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

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

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

14 B. OPERATION OF THE REQUESTED SEARCH WARRANT

15 1. Infrastructure

16 46. The FBI IPs will be a maximum of 15 public facing IP
17 addresses located in the United States, and specifically in the
18 Central District of California, that will be used to connect
19 with other Joanap Peers. Each of the FBI IPs will be
20 configured, through custom scripts written by the FBI, to
21 communicate with other Joanap Peers, and will be the outward-
22 facing, Internet-accessible IP addresses used in the execution
23 of the warrant, although they will be controlled by those
24 scripts and by other computers under the control of the FBI.
25 The FBI IPs will only emulate Joanap-infected computers and will
26 not actually be running Joanap malware. For example, one
27 practical difference is that while ordinarily a Receive List is
28

1 maintained up to a maximum of 50 Peers, here the purpose of the
2 search warrant is to collect and record a complete map of all of
3 the Joanap Peers, and therefore that list will not be limited to
4 50 Peers.

5
6 47. Although Push Lists may contain up to 50 Peers, only
7 15 FBI maintained IP addresses will be used. Only 15 FBI IPs
8 will be used in order to increase the chances that an FBI IP
9 will be contacted by a Peer when it initiates a connection every
10 three hours while at the same time not fully populating the
11 entire Peer List. Populating the entire Peer Lists with FBI IPs
12 would cause the Peers to only connect with the FBI IPs and
13 therefore could "sink-hole" the Joanap botnet, meaning that
14 Peers would not be reaching out to other non-FBI IP Peers.

15 48. It is important to sufficiently saturate the botnet
16 with FBI IPs, but not sink-hole it, in order to fully map as
17 many Peers on the botnet as possible. First, populating the
18 entire Receive Lists of multiple Peers with FBI IPs would
19 effectively remove those Peers from the "wild" and they would no
20 longer be in contact with other Peers. That would reduce the
21 FBI's ability to identify additional Peers, and would more
22 likely result in sink-holing only part of the botnet before
23 fully identifying all of the infected Peers. Second, if the FBI
24 IPs consume the entire Peer Lists, it could alert the North
25 Korean cyber actors who operate the botnet about the FBI's
26 actions. That could cause them to employ counter-measures,
27 including excluding the FBI IPs from the botnet, which would
28

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

3
4 49. Each FBI IP will maintain a Push List, which may hold
5 up to 50 entries and may contain the 15 FBI IPs as well as 35
6 other publicly available Joanap Peer IP addresses (the latter
7 are the same type of IP addresses each Peer would ordinarily
8 include). Each entry will include a port number as well as a
9 timestamp that reflects the last contact with that Peer.

10 Providing the FBI IPs via their own Push Lists will cause Peers
11 to continue to contact FBI IPs through the duration of the
12 search warrant and thus generate a current map at the end of the
13 authorized period. It will also more accurately emulate the
14 behavior of a true Joanap-infected Peer so that their behavior
15 does not appear aberrant to the subjects controlling the botnet.

16 2. Execution of the Search Warrant

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

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

1 initiate contact with and issue commands to other Peers for
2 their Peer Lists. That in turn will cause the FBI IPs to be
3 supplied with the Push Lists held by those Peers, and the
4 process will continue to proceed in that manner.
5

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

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

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

1
2 53. The FBI IPs will use each of these sources of Peer IP
3 addresses to initiate connections with Peers and issue Push
4 Requests or Receive Requests to them. It is essential for the
5 FBI IPs to widely populate or saturate Push Lists:

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

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

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

1 more and more Peers will incorporate the FBI IPs into their
2 Receive Lists and Push Lists so that, according to current
3 estimates, it is possible that most if not all of the Joanap
4 botnet will connect with the FBI IPs during the 30-day period in
5 the requested warrant. (As noted below, however, those
6 estimates are based on assumptions and parameters that may vary
7 from the actual characteristics of the Joanap botnet.)
8

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

1
2 56. The FBI did not observe evidence indicating that use
3 of the FBI IPs in the limited manner provided in the requested
4 search warrant would interrupt or interfere with other processes
5 of a computer infected by Joanap. I have learned from computer
6 scientists and technical experts at the FBI that by executing
7 the requested warrant and sending and receiving the limited
8 types of communications permitted by the search warrant, the
9 legitimate function of infected computers will not be
10 compromised, interrupted, or degraded.

11 3. Evidence to be Collected

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

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

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

1
2 VI. DELAYED NOTICE, SEALING, AND EXECUTION AT ANY TIME OF DAY

3 60. Pursuant to Section 3103a(b), and based on my training
4 and experience and my investigation of this matter, I believe
5 that reasonable cause exists to seal this application and
6 warrant, as well as the return to the warrant, and to delay the
7 service of the warrant as normally required until August 31,
8 2018.

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

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

1 infrastructure for other attacks, limiting the FBI's ability to
2 fully map the botnet would interfere with the FBI's ability to
3 identify other intrusions and related activities that may be
4 discovered after each of the Joanap-infected peers is identified
5 and the activity related to those IP addresses is assessed.
6

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

13 64. As this warrant seeks delayed notice pursuant to Title
14 18, United States Code, Section 3103a, it does not seek
15 authorization to seize any tangible property. In addition to
16 delaying notice, pursuant to Title 18, United States Code,
17 Section 3103a(b)(2), reasonable necessity exists to seize stored
18 electronic information and electronic communications found on
19 Peers that connect with the FBI IPs, i.e., the Push Lists and
20 Receive Lists that the FBI IPs receive from other Peers.

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

1 without learning about new Peers through Push Lists and Receive
2 Lists. Each Push List and each Receive List contains up to 50
3 new Peers, whereas an FBI IP initiating a single outbound
4 connection to another Peer places that FBI IP on just one other
5 Peer's Push List, which will then need to be propagated further
6 before any new Peer will connect with the FBI IP. Proceeding by
7 initiating connections alone and not receiving Push Lists and
8 Receive Lists would therefore limit the FBI's ability to fully
9 map the Joanap network, given how infrequently (every three
10 hours) Peers initiate connections using their Receive lists.
11 Moreover, the FBI's current estimate that 80 percent of the
12 botnet may be mapped in 20 days is based upon both obtaining
13 Peer Lists through commands, and propagating the FBI IPs through
14 the exchange of commands. Both methods must be used in order to
15 map the botnet as quickly as possible.
16

17 66. Furthermore, there is good cause for the order to be
18 issued such that the warrant may be executed at any time of the
19 day or night. As noted above, Peers will initiate contact once
20 every three hours, irrespective of the time of day. Moreover,
21 it is essential for the FBI IPs to saturate the botnet quickly
22 in order to maximize the probability that the FBI will be able
23 to complete the search by mapping the botnet within the 30-day
24 period. Finally, inasmuch as the Peers are computers that are
25 infected unbeknownst to the users of those computers (except in
26 rare instances, such as security researchers), and the activity
27 of the Joanap malware occurs without the user being aware of it,
28

1
2 executing the search warrant during the night time versus the
3 day time will make little difference to the user of any Peer.

4 67. While the FBI seeks authorization to delay notice,
5 during the period of delayed notice the FBI may still seek to
6 notify individual victims or to disclose information obtained as
7 a result of the requested warrant to one or more victims or to
8 private entities or foreign authorities for purposes of
9 mitigating the effects of any computer intrusion or assisting in
10 maintaining the security of computers or networks during the
11 authorized period of delayed notice.

12 VII. CONCLUSION

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

18 /s/

19 Chade Chowana-Bandhu
20 Special Agent
Federal Bureau of Investigation

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

23 /s/

24 UNITED STATES MAGISTRATE JUDGE
25 FREDERICK F. MUMM
26
27
28