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

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE: BOTNET OF COMPROMISED COMPUTERS	No. 18-MJ-02739 ~~[PROPOSED]~~ WARRANT AND ORDER **(UNDER SEAL)**

Upon application by the United States of America, supported by the law enforcement agent's affidavit, for a search warrant.

THIS COURT FINDS THAT there is probable cause to believe that the IP addresses and other related information to be obtained from the computers infected with the Joanap malware ("Peers"), will constitute or yield evidence of violations of federal offenses, including Title 18, United States Code, Section 1030(a)(5) (Causing Damage to Protected Computers), being committed by North Korean subjects of the government's investigation who are not yet identified, which investigation is ongoing in the Central District of California. The Joanap malware has been identified through hash

values and published analysis performed by multiple sources such as National Cybersecurity and Communications Integration Center, Novetta, and VirusTotal as Joanap (version 1, or herein "Joanap"). The Court finds the use of computers ("FBI IPs") under the control of the Federal Bureau of Investigation ("FBI") to connect with Peers infected with Joanap will identify computers compromised by Joanap. Specifically, the use of the FBI IPs will cause Peers to initiate contact with the FBI IPs and reveal their own IP addresses, and the exchange of commands by FBI IPs and Peers will cause those Peers to disclose the lists of Peers ("Peer Lists") that they keep; namely, one list that is used to initiate contact with other Peers and another list that is automatically shared with other Peers upon request.

THIS COURT FURTHER FINDS THAT, pursuant to Federal Rule of Criminal Procedure 41(b)(6)(B), the media infected by Joanap are protected computers that have been damaged without authorization and are located in five or more judicial districts, including specifically the Central District of California, the Southern District of Texas, the Southern District of Indiana, the Southern District of Ohio, the District of Utah, and the Middle District of Florida.

THIS COURT FURTHER FINDS THAT, pursuant to Title 18, United States Code, Section 3123, the attorney for the government has certified that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the FBI for violations of the offense listed above.

THIS COURT FURTHER FINDS reasonable cause exists to believe that providing immediate notification of this warrant to the user or subscribers of any of the Internet Protocol ("IP") addresses that connect with the FBI IPs will result in an adverse result, specifically flight from prosecution, destruction of or tampering with evidence, and will otherwise seriously jeopardize the investigation. 18 U.S.C. § 2705(a)(2)(B), (C), (E).

THIS COURT FURTHER FINDS that reasonable necessity exists for the seizure of electronic information and electronic communications.

GOOD CAUSE HAVING BEEN SHOWN, THIS COURT HEREBY ISSUES THIS WARRANT AND FURTHER ORDERS THAT:

A. **PROPERTY TO BE SEARCHED**

1. This warrant authorizes any law enforcement officer or individual acting under the direction and control of law enforcement to communicate in the manner described below with any computer infected with the Joanap malware. Execution of this search warrant will only occur on a computer if the computer is identified during the 30 day execution of this warrant as a Peer in the Joanap botnet.

2. The FBI will determine whether a computer is a Peer in the Joanap botnet by virtue of one or more of the following conditions (1) consensually monitored computer activity reflecting the presence of the Joanap malware, including both computer activity occurring after the issuance of this search warrant during the period authorized by the warrant as well as such activity dating back to January 1, 2018; (2) the computer initiates a connection with an FBI IP, (3) the IP address of the computer is received by the FBI IPs on a Peer List from another computer infected with Joanap, or (4) the IP

address within the last sixty days (a) has had port 80, 110, or 443 open, (b) has executed a premature termination of the connection when receiving a banner request by software expected to legitimately run on that respective port and (c) passes Joanap's initial authentication step by returning a piece of data encrypted using Joanap's encryption system and encryption key.

3. The FBI, using FBI IPs, may initiate contact with and issue and receive commands used by the Joanap malware to any such computer. The commands that may be sent by or received or responded to by the FBI IPs are only those commands that identify Peers to each other and exchange Peer Lists. The FBI will not receive or record, or supply, any system information in response to such commands.

B. **PROPERTY TO BE SEIZED**

4. In each communication between an FBI IP and a Peer during those commands, whether initiated by an FBI IP or a Peer, the FBI IP may record:

a. The IP address of the connecting Peer;

b. The source port and destination port;

c. The commands used;

d. A pseudo-random string of text that is used for an encrypted handshake to authenticate the two communicating computers as Peers of the Joanap botnet;

e. The list of peers exchanged; and

f. Other ancillary information exchanged in order to complete the commands, which information may include system times, numerical values generated in the course of the exchange, whether the

Peer identifies itself as publicly accessible, and the status of the exchange, but will not include system information.

C. **PEN REGISTER AND TRAP AND TRACE DEVICE**

5. Pursuant to Title 18, United States Code, Section 3123, Special Agents of the FBI may use a pen register anywhere in the United States to record or decode all non-content dialing, routing, addressing, or signaling information originating from or destined to the FBI IPs defined and described in the Affidavit, including IP addresses and IP packet header information, and to record the date and time of such transmissions, for a period of 30 days.

6. Pursuant to Title 18, United States Code, Section 3123, Special Agents of the FBI may use a trap and trace device on each FBI IP anywhere in the United States to capture and record the incoming electronic or other impulses that identify the originating numbers or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication and to record the date, time, and duration of communications created by such incoming impulses, for a period of 30 days.

7. It is further ordered that the IP addresses, and the dialing, routing, addressing, and signaling information called for the requested pen register and trap and trace device include, for any communication with an FBI IP, the IP addresses and source or destination ports for any such communication or transmission, along with the date, time, and duration.

D. **EXECUTION, DELAYED NOTICE, AND SEALING**

8. Once commenced within fourteen days of being issued, the FBI may continue to execute the warrant for a period of 30 days.

9. This warrant's authorization applies only to the FBI's activities in executing it to the extent that those activities occur within any district or territory of the United States.

10. The FBI is prohibited from seizing any tangible property or wire communications or wire information pursuant to this warrant. 18 U.S.C. § 3103a(b)(2). The Court finds that reasonable necessity exists for the seizure of electronic information and electronic communications, specifically the lists of other Peers that are sent from Peers to FBI IPs and the information exchanged through the commands with Joanap-infected Peers.

11. The Court finds there is reasonable cause to believe that notice or disclosure will result in flight from prosecution, destruction of or tampering with evidence, and will otherwise seriously jeopardize the investigation. 18 U.S.C. § 3103a(b)(1), § 2705(a)(2)(B), (C), (E). The FBI is therefore permitted to delay service of this warrant until January 30, 2019. Any requests for a continuance of this delay should be filed with this Court, unless directed to the duty United States Magistrate Judge by this Court. This provision does not prohibit the government from providing any information received through this warrant to one or more victims or to private entities or foreign authorities for purposes of mitigating the effects of any computer intrusion or assisting in maintaining the security of computers or networks during the authorized period of delayed notice.

12. The FBI shall make a return of this warrant and order to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office within ten calendar days after the disclosure of information ceases. The return shall state the date and time the FBI began communicating with Peers, and the period during which information was provided, including pursuant to any orders permitting continued disclosure.

13. When notice is no longer delayed, a copy of this search warrant and order and the receipt may be provided to any person entitled to it by any means reasonably calculated to reach that person, including by electronic means or publication.

14. Good cause having been shown, and pursuant to Title 18, United States Code, Section 3123(d), the application, the

///

affidavit, this warrant and order, and the return to the warrant shall remain under seal until otherwise ordered by the Court.

UNITED STATES MAGISTRATE JUDGE
MICHAEL R. WILNER

DATE/TIME OF ISSUE: 10/18/2018 15:30 p.m.