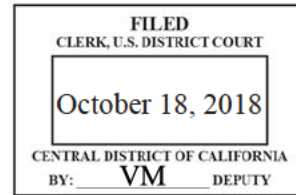


1 NICOLA T. HANNA
United States Attorney
2 PATRICK R. FITZGERALD
Assistant United States Attorney
3 Chief, National Security Division
ANTHONY J. LEWIS (Cal. Bar No. 231825)
4 Assistant United States Attorney
Deputy Chief, Terrorism and Export Crimes Section
5 ANIL J. ANTONY (Cal. Bar No. 258839)
Assistant 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 FOR THE CENTRAL DISTRICT OF CALIFORNIA

14 IN RE: BOTNET OF COMPROMISED
15 COMPUTERS

No. 18-MJ-02739

~~PROPOSED~~ WARRANT AND ORDER

(UNDER SEAL)

16
17
18 Upon application by the United States of America, supported by
19 the law enforcement agent's affidavit, for a search warrant.

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

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

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

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

27

28

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

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

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

12 A. **PROPERTY TO BE SEARCHED**

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

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

28

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

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

13 **B. PROPERTY TO BE SEIZED**

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

- 17 a. The IP address of the connecting Peer;
- 18 b. The source port and destination port;
- 19 c. The commands used;
- 20 d. A pseudo-random string of text that is used for an
21 encrypted handshake to authenticate the two communicating computers
22 as Peers of the Joanap botnet;
- 23 e. The list of peers exchanged; and
- 24 f. Other ancillary information exchanged in order to
25 complete the commands, which information may include system times,
26 numerical values generated in the course of the exchange, whether the

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

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

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

11 6. Pursuant to Title 18, United States Code, Section 3123,
12 Special Agents of the FBI may use a trap and trace device on each FBI
13 IP anywhere in the United States to capture and record the incoming
14 electronic or other impulses that identify the originating numbers or
15 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.

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

26
27
28

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

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

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

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

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

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

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

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

14
15 ///

16
17
18
19
20
21
22
23
24
25
26
27
28

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

3
4 

5

UNITED STATES MAGISTRATE JUDGE
MICHAEL R. WILNER

6
7 DATE/TIME OF ISSUE: 10/18/2018 15:30 p.m.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28