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

I, Joshua A. Morton, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am Joshua A. Morton, a Special Agent with the Federal Bureau of Investigation operating within Chesapeake, Virginia. I have been working for the agency for about five years in the Chesapeake Field Office as a member of the Cyber Action Team / Cyber Squad. I have been investigating cyber and computer intrusion crimes for two years and specialize in the investigation of botnets facilitating distributed denial of service attacks (DDos),

2. I make this Affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41 to authorize a search and seizure warrant for the premises located at:

6428 Tappahannock Drive, Norfolk Virginia, 23509

The listed address is the suspected residence of Juan Pablo Erb, a suspected criminal hacker, known under the alias as C0alMiner. Erb has been suspected of running a botnet operation out of his home which is used in a DDos-For-Hire business operation targeting businesses, organizations, and individuals with distributed denial of service attacks in exchange for cryptocurrency pay.

3. As set forth in the Probable Cause section, the computers, servers, and technical equipment used to solicit the DDos-For-Hire attacks and conduct botnet organized DDos attacks have probable cause to be in violation of Title 18, United States Code, Sections 1030 (a)(5)(A) (Intentionally causing damage to a protected computer), 1030(b) (Conspiracy to commit Computer Fraud), and 1343 (Conspiracy to commit Wire Fraud).

PROBABLE CAUSE

1. Through investigation with the FBI Cyber Action Team in coordination with the Norfolk Police Department & Old Dominion Campus Police Department have probable cause to believe that Juan Pablo Erb is responsible for coordinating a illegal DDos-For-Hire operation responsible for disrupting critical infrastructure of educational institutions and private businesses within the Eastern District of Virginia.

2. Between the dates of February 8th and March 17th, multiple DDos attacks suspected to be caused by a botnet run by Juan P. Erb targeted:

    1. Old Dominion University Campus Network & Wi-Fi Services, preventing the use of campus wi-fi services which led to the shutdown of many computers needed for instruction and campus operations as well as the many businesses that run on the same University Wi-Fi network for their Point-of-Sale Computers.

3. It has been determined by the local departments and I, that Erb is running a botnet, whose purpose is to flood target servers, networks, or websites with high volumes of traffic to make services unavailable, install malicious programs, such as ransomware, and harvest user credentials. All of the included purposes are conducted for the financial benefit of Erb and other associated cybercriminals.

4. Based upon the investigation described below, I believe that the botnet responsible for the Old Dominion University Campus Wi-Fi DDos attack is operated and controlled by an individual identified as Juan P. Erb from his home in Norfolk Virginia and Erb has used the botnet for financial gain.

EVIDENCE FOR PROBABLE CAUSE

1. While Undercover I messaged Erb (Alias: C0alMiner) in a discord server to which he had posted the following advertisement on a discord server known as CoalMine:

"Am running some crazy stuff. Can take whole servers down real quick. Tap In!"

2. C0alMiner instructed to add me to a Telegram chat and message the following conversation in which I asked for an attack to an FBI dummy server to which Erb accepted and agreed to a $250 dollar bitcoin transaction:

C0AlMiner: Hey. I saw ur message on discord.

Agent Morton: Yea what do you do.

C0AlMiner: I do DDos for cheap just lemme know what you want.

Agent Morton: Can you target a certain server for me?

C0AlMiner: Yea man it'll be $250, crypto only. U got bitcoin?

Agent Morton: Yea sure let me send it to you and you can get to work.

3. FBI forensic analysis determined that the Command-and-control server hosting the botnet and harboring traffic related to the DDos attacks was issued from an IP registered to 6428 Tappahannock Drive, Norfolk Virginia, 23509.

4. On March 25, 2025, at 3:15 AM, a single server rack and multiple networking devices were observed by officers through Erb's residence basement window.

On March 27, 2025 at 2:43 PM. a delivery from NetGear Inc.was accepted by Erb. This delivery is suspected to be high-speed routers used for botnet management.

ITEMS TO BE SEIZED

1. Computers, servers, networking equipment (routers, switches, VPS logins) used in DDoS attacks
2. Cryptocurrency wallets (Ledger, Trezor, paper backups) containing proceeds from illegal services.
3. DDoS-for-hire transaction records, customer lists, and communication logs.
4. Telegram, Discord, and encrypted messaging apps related to cybercrime operations.
5. USB drives, SD cards, and hidden storage media that could contain attack scripts or stolen credentials.

JURISDICTION

1. With probable cause this warrant for search and seizure complies with:
   a. Rule 41(e)(2)(a) of the Federal Rules of Criminal Procedure states that the warrant must be executed within a period no longer than 14 days and the proper identification of a seized suspect.
   b. Rule 41(e)(2)(b) of the Federal Rules of Criminal Procedure states that a warrant under rule Rule 41(e)(2)(a) may authorize the seizure of an electronic storage or the seizure of electronically stored information and that the warrant authorizes a review of the media or information consistent with the warrant.
   c. 18 U.S. Code § 2703 stating the required disclosure of customer communications or records.
   d. 18 U.S. Code § 1030 (a)(5)(A) states that knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally

causes damage without authorization, to a protected computer, to which C0alMiner has been in violation of.

References:

Cornell Law School. (n.d.). 18 U.S. Code § 1030 - Fraud and related activity in connection with computers. LII / Legal Information Institute.

https://www.law.cornell.edu/uscode/text/18/1030

18 U.S. Code § 2703 - Required disclosure of customer communications or records. (n.d.). LII / Legal Information Institute.

https://www.law.cornell.edu/uscode/text/18/2703

Legal Information Institute. (2016, November 30). Rule 41. Search and Seizure. LII / Legal Information Institute.

https://www.law.cornell.edu/rules/frcrmp/rule_41

UNITED STATES DISTRICT COURT. (n.d.). Retrieved April 4, 2025, from https://ia800905.us.archive.org/10/items/gov.uscourts.moed.167076/gov.uscourts.moed.167076.2.0.pdf

https://www.justice.gov/opa/page/file/976846/dl?inline