DMP/JAM:AFM/EHS/AA
F. #2022R00315

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

SAGAR STEVEN SINGH ,
also known as "Weep," and
NICHOLAS CERAOLO,
also known as "Convict," "Anon"
and "Ominous,"

Defendants.

AFFIDAVIT AND COMPLAINT IN SUPPORT OF AN APPLICATION FOR AN ARREST WARRANT

(T. 18, U.S.C., §§ 1030(b), 1349 and 3551 et seq.)

No. 23-M-213

- X

EASTERN DISTRICT OF NEW YORK, SS:

JUSTIN GETZ, being duly sworn, deposes and states that he is a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations, duly appointed according to law and acting as such:

Conspiracy to Commit Computer Intrusion

In or about and between April 2022 and May 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SAGAR STEVEN SINGH , also known as "Weep," and NICHOLAS CERAOLO, also known as "Convict," "Anon" and "Ominous," together with others, did knowingly and intentionally conspire to intentionally access a computer, without and in excess of authorization, and thereby obtain information from a department or agency of the United States, and the offense was committed in furtherance of criminal or tortious acts, in

violation of Title 18, United States Code, Sections 1030(a)(2)(B) and 1030(c)(2)(B)(ii).

(Title 18, United States Code, Sections 1030(b) and 3551 et seq.)

Wire Fraud Conspiracy

In or about and between February 2022 and May 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant NICHOLAS CERAOLO, also known as "Convict," "Anon" and "Ominous," together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud electronic service providers, and to obtain information by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, as well as emails and other online communications, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI") and have been since November 2018. I

[1] Because the purpose of this complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for cybercrime, financial crime and money laundering. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information.

2. I am familiar with the facts and circumstances set forth below from my participation in the investigation, from my review of documents obtained pursuant to the investigation and from reports of other law enforcement officers involved in the investigation. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

I. THE DEFENDANTS

3. The defendant SAGAR STEVEN SINGH, also known as "Weep" ("SINGH"), is 19 years old and resides in Pawtucket, Rhode Island.

4. The defendant NICHOLAS CERAOLO, also known as "Convict," "Anon" and "Ominous" ("CERAOLO"), is 25 years old and resides in Queens, New York.

II. BACKGROUND REGARDING ViLE

5. As set forth in detail below, SINGH and CERAOLO are members of a group of cybercriminals, known to its members as "ViLE," who specialize in obtaining personal information about third-party victims, which they then use to harass, threaten or extort the victims, a practice known as "doxing." ViLE is collaborative, and the members routinely share tactics and illicitly obtained information with each other.

6. SINGH, CERAOLO and other members of ViLE use various methods to obtain victims' personal information, including tricking customer service employees;

submitting fraudulent legal process to social media companies to elicit users' registration information; coopting and corrupting corporate insiders; searching public and private online databases; and, as charged herein, accessing a nonpublic United States government database without authorization and unlawfully using official email accounts belonging to other countries.

7. Once they have obtained a victim's information, SINGH and CERAOLO post the information in an online forum, hereinafter referred to as Forum-1, that is administered by the leader of ViLE ("CC-1"). Victims are extorted into paying CC-1 to have their information removed from Forum-1. SINGH also uses the threat of revealing personal information to extort victims into giving him access to their social media accounts, which SINGH then resells.

8. SINGH is also known as "Weep," and CERAOLO is also known as "Convict," "Anon" and "Ominous." SINGH and CERAOLO use their online nicknames (or "handles") to post on Forum-1 and in chatrooms on various social media platforms. SINGH and CERAOLO regularly use those chatrooms to talk with CC-1 and other members of ViLE. SINGH and CERAOLO have also been listed (under the respective handles "Weep" and "Ominous") on a membership roster of ViLE that is available online. The names on the roster appear below an image of the hanging body of a young girl, depicted below, which appears to be a calling card used by ViLE on websites with which it is affiliated:

III. SINGH AND CERAOLO ACCESS A U.S. GOVERNMENT DATABASE WITHOUT AUTHORIZATION

9. A United States federal law enforcement agency (the "Federal Law Enforcement Agency") maintains a nonpublic website (the "Portal") whose purpose is to share intelligence from government databases with state and local law enforcement agencies. Data available through the Portal is not classified but is sensitive and includes detailed, nonpublic records of narcotics and currency seizures, as well as law enforcement intelligence reports.

10. The Portal is password-protected, and access to the Portal is restricted to law enforcement officials. A user who enters the Portal must view and click through multiple warning screens. One such screen warns that "unauthorized use or access to this system may subject you to criminal and/or civil prosecution and penalties." Another screen repeats this warning and adds that the Portal is "only for authorized U.S. government and law enforcement use" and that "[e]vidence of unauthorized use" may lead to "criminal or other

adverse action." These warnings were shown to anyone logging into the Portal at all times relevant to this Complaint.

11. On or about May 7, 2022, SINGH used a username and password belonging to a local police officer (the "Stolen Credentials") to log in to the Portal without authorization. SINGH connected to the Portal from an IP address[2] that had, in turn, previously been used to access a social media account registered to SINGH. Records from SINGH's computer and the Federal Law Enforcement Agency's servers indicated that SINGH accessed various portions of the Portal, including multiple guides to using the Portal and law enforcement databases that track narcotics seizures in the United States. SINGH also clicked on links within the Portal that led to other Federal Law Enforcement Agency databases, but was unable to access those databases because they required separate credentials.

12. Records obtained from a social media platform ("Platform-1") show that on or about May 7, 2022, while still logged in to the Portal, SINGH wrote in a chat on Platform-1 that he "got access to this gov website." SINGH shared a screenshot of the Portal, and described it as "a portal that allows the user to obtain essentially any piece of info." SINGH shared an image of a previously downloaded guide to using the Portal, and also shared the Federal Law Enforcement Agency-operated telephone number and email address for the Portal, stating that he could "get any of that [information] just by calling this number or emailing them to request for information." SINGH also shared other guides to

---

[2] An Internet Protocol (or "IP") address is a unique numerical indicator designating a point of connection to the internet, such as a residential router.

using the Portal, including a PowerPoint presentation that detailed the purpose and some of the capabilities of the modules hosted in the Portal.

13. On or about May 8, 2022, SINGH and CERAOLO communicated on Platform-1. CERAOLO asked SINGH if he could acquire more login credentials. SINGH told CERAOLO, "no i literally just got a login [for] it…but ill give u login as well if u wana scope it out." SINGH sent the Stolen Credentials to CERAOLO. Immediately afterwards, CERAOLO responded: "it worked." CERAOLO added, "This is an [Federal Law Enforcement Agency] agent pretty sure . . . were all gonna get raided one of these days i swear." Based on my knowledge, training and experience, I assess that CERAOLO meant that the Stolen Credentials likely belonged to a law enforcement officer employed by the Federal Law Enforcement Agency, and that SINGH and CERAOLO could face criminal penalties as a result.

14. On or about May 8, 2022, according to records obtained from Platform-1, SINGH wrote to a contact that the "portal shit i accessed i was not supposed to be there not one bit." SINGH said he had, "jacked into a police officer's account" and "that portal had some fucking potent tools." SINGH continued: "it gave me access to gov databases," followed by the names of five search tools accessible through the Portal.

15. On or about May 9, 2022, based on information provided by Platform-1, SINGH sent a friend screenshots of text messages between himself and an individual whom SINGH was extorting ("Victim-1"). In the messages, SINGH sent Victim-1 an extensive set of personal details associated with Victim-1, including Victim-1's social security number, driver's license number, cellphone number, and home address. SINGH asked: "look familiar?" SINGH then advised Victim-1: "you're gonna comply to me if you

don't want anything negative to happen to your parents. . . I have every detail involving your parents . . . allowing me to do whatever I desire to them in malicious ways." SINGH demanded the credentials to Victim-1's Instagram accounts and added: "leave the details here and I won't harm anyone."

16. During the conversation, SINGH told Victim-1 that he had "access to [] databases, which are federal, through [the] portal, i can request information on anyone in the US doesn't matter who, nobody is safe."[3] SINGH ultimately directed Victim-1 to sell Victim-1's account credentials and send the proceeds of the sale to SINGH.

17. Records obtained from online platforms show that after his initial access, CERAOLO shared the Stolen Credentials with online associates, including a fellow member of ViLE ("CC-2") and another individual who is not a member of ViLE ("CC-3"). CERAOLO and CC-3 discussed how to "scrape" data from the Portal. Scraping data means using automated tools to export voluminous information from a website into a local file which is saved to a computer's hard drive. CERAOLO described the Portal to CC-3 as "some sort of intel center for [Federal Law Enforcement Agency]."

18. On or about September 8, 2022, I and other Homeland Security Investigations agents executed a search warrant at SINGH's residence and seized evidence, including SINGH's cellular phone and laptop. Both devices contained extensive evidence of access to the Portal. For example, SINGH's cellphone contained images he had captured

---

[3] In his communication, SINGH named two databases that are accessible through the Portal. The names of those databases have been redacted from the quotation in this Complaint.

of the Portal, including a video of the Portal's homepage, a screenshot of a message from the Portal confirming successful login, and an annotated screenshot of the Portal's homepage, with an arrow pointing to a portion of the Portal and the annotation "DBs." Based on my training and experience, I know that "DB" is the abbreviation for "database." In the background of the annotated image, there appears an internet browser with several tabs open. One of the open tabs reads "Ominous" – CERAOLO's online handle.

IV. CERAOLO POSES AS A POLICE OFFICER TO OBTAIN PRIVATE SUBSCRIBER INFORMATION AND OTHER THINGS OF VALUE FROM ONLINE SERVICE PROVIDERS

19. On or about and between February 2022 and May 2022, CERAOLO accessed without authorization an official email account belonging to a Bangladeshi police official. CERAOLO used the account to pose as a police officer in communication with U.S.-based social media platforms. In these communications, CERAOLO requested personal information about users of these platforms, under the false pretense that the users were committing crimes or in life-threatening danger.

20. By these means, CERAOLO induced and attempted to fraudulently induce the platforms to provide their users' information, which they would not otherwise have provided.

A. Ceraolo Obtains Victim Subscriber Information From Platform-1

21. On or about February 22, 2022, Platform-1 received a message from an email address belonging to a Bangladeshi law enforcement official (the "Bangladeshi Police Account"). The purported police officer requested personal details about one of Platform-1's users ("Victim-2"), including Victim-2's IP address, email address and telephone

number. The purported police officer asserted that Victim-2 had participated in "child extortion" and blackmail and had threatened officials of the Bangladeshi government.

22. Later that day, Platform-1 emailed Victim-2's telephone number, email address and IP address to the Bangladeshi Police Account. Beginning approximately three hours later, in a conversation on a messaging app, CC-1 wrote to SINGH that he was "talking to ominous" (referring to CERAOLO) and then sent Victim-2's IP address, email address and telephone number to SINGH. The victim information sent by CC-1 to SINGH, and attributed by CC-1 to CERAOLO, matched the information that Platform-1 had provided to the Bangladeshi Police Account shortly beforehand.

B. Ceraolo Targets Platform-2 and its Subscribers

23. On or about March 13, 2022, a social media company that operates a popular online game ("Platform-2") received an email message from the Bangladeshi Police Account. The purported police officer requested personal details about one of Platform-2's users ("Victim-3"), such as the user's IP address and messages sent by Victim-3 within Platform-2. The purported police officer asserted that Victim-2 had sent "bomb threats," distributed child pornography and threatened officials of the foreign government.

24. Platform-2 declined to provide the information, and later posted on Twitter touting its success in identifying the fraudulent approach.

25. On or about May 11, 2022, I and other Homeland Security agents executed a search warrant at CERAOLO's residence and seized evidence, including CERAOLO's mobile phone. Examination of the phone revealed that after Platform-2

posted about the scam, CERAOLO used a chat application to share a screenshot of the post with CC-3. CERAOLO wrote: "lmao was literally me loool."[4]

26. After Platform-2 advertised its success in thwarting CERAOLO's attempted fraud, CERAOLO attempted to take revenge on Platform-2 by posing as a U.S. police officer to obtain the personal information of Platform-2's administrators. According to data recovered from CERAOLO'S mobile phone, CERAOLO wrote to a co-conspirator that he wanted to "hack [Platform-2] . . . I wanna hack these faggots for acting like their [sic] untouchable." CERAOLO added that he would "handle dumping and defacing everything for trying to snitch to homeland security" and that he could "easily get 6 figs" for selling Platform-2's information "on one of the dark web markets." Accordingly, in and around May 2022, CC-3, at CERAOLO's behest, used an internet domain that fraudulently appeared to belong to a local police department to send an email to an online infrastructure company ("Vendor-1") whose services are used by Platform-2. The email claimed that an IP address belonging to Platform-2 was being used to threaten someone's life and induce minors to commit suicide. Attached to the email was a forged subpoena seeking subscriber details about Platform-2's account with Vendor-1. Vendor-1 requested additional information, and ultimately did not provide the subscriber details for Platform-2.

C. Ceraolo Targets Platform-3

---

[4] Based on my knowledge, training and experience, "lmao" is an abbreviation for "laughing my ass off," and "lol" and variants thereof are abbreviations for "laughing out loud."

26. On or about March 15, 2022, CERAOLO used Platform-1 to write to another member of ViLE that he was "working on getting us" an account with a U.S. company ("Platform-3") that provides facial recognition software to law enforcement, government employees and contractors. Platform-3's products are not available to the general public. CERAOLO added that Platform-3's product was "the best facial recognition out rn [right now]." That same day, Platform-3 received an email from the Bangladeshi Police Account, asking to purchase Platform-3's software on behalf of the Bangladeshi police, and requesting a discount for a "rather large team of law enforcement officers." Platform-3 ultimately denied the request.

WHEREFORE, your deponent respectfully requests that arrest warrants be issued for the defendants SAGAR STEVEN SINGH , also known as "Weep," and NICHOLAS CERAOLO, also known as "Convict," "Anon" and "Ominous," so that they may be dealt with according to law.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this Affidavit and any arrest warrants issued. Based on my training and experience, I have learned that criminals actively search for criminal affidavits on the Internet and disseminate them to other criminals as they deem appropriate, such as by posting them publicly through online forums. Premature disclosure of the contents of this Affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee

or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior and notify confederates.

JUSTIN GETZ
Special Agent
United States Department of Homeland Security,
Homeland Security Investigations

telephonically

Sworn to before me this
10 th day of March, 2023

Marcia M. Henry

THE HONORABLE MARCIA M. HENRY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK