UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. ANGEL MANUEL COLON, JR., aka "Anonghost720," aka "Anonghost1337," Defendant.	No. CR 2:22-cr-00579-JFW I N F O R M A T I O N [18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)(i), (c)(4)(A)(i)(VI): Unauthorized Impairment of a Protected Computer]

The United States Attorney charges:

COUNT ONE

[18 U.S.C. § 371]

A. OBJECT OF THE CONSPIRACY

Beginning no later than August 2017 and continuing to on or about November 17, 2021, in Los Angeles County, within the Central District of California, and elsewhere, defendant ANGEL MANUEL COLON, JR. ("COLON"), and others known and unknown to the United States Attorney, knowingly conspired and agreed with each other to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally cause damage without

authorization to protected computers, and specifically to cause such damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI).

B. MEANS BY WHICH THE OBJECT OF THE CONSPIRACY WAS TO BE ACCOMPLISHED

The object of the conspiracy was to be accomplished, in substance, as follows:

1. Defendant COLON would offer services via the website SecurityTeam.io that would allow his subscribers, for a fee, to cause floods of Internet traffic to be directed to victim computers, an online attack technique known as "Distributed Denial of Service" or "DDoS," for the purpose of degrading or disrupting the victim computers' access to the Internet.

2. Defendant COLON would construct these DDoS attacks to use a practice known as "amplification," meaning that brief commands sent to third-party computers and devices would cause much longer strings of data to be sent to the victim in response.

3. Defendant COLON would construct the attacks in such a manner as to disguise the true origin of the electronic queries sent to such computers and devices, so that the computers and devices sending the floods of Internet traffic perceived the queries to be coming from the victim computers rather than COLON or his subscribers, a practice known as "spoofing."

4. Defendant COLON would maintain and improve the SecurityTeam.io website and services, respond to requests for attacks, subscriptions, or assistance from potential or current customers, and market the SecurityTeam.io website in an attempt to

draw subscribers to SecurityTeam.io and away from other competitor websites.

C. OVERT ACTS

In furtherance of the conspiracy and to accomplish its object, defendant COLON and others committed various overt acts within the Central District of California, and elsewhere, including but not limited to the following:

Overt Act No. 1: On an unknown date in 2017 or 2018, defendant COLON defaced a competitor DDoS-for-hire website by posting "HACKED BY ANONGHOST720" on its landing page.

Overt Act No. 2: On an unknown date between August 2017 and November 17, 2021, in response to a customer question about recommended methods available to cause floods of data to be sent to different types of victim computers, defendant COLON posted on the SecurityTeam.io website that the "DNS-SIG method" had the biggest "amplification power" and was therefore recommended for attacking "home connection unprotected servers."

Overt Act No. 3: On an unknown date between August 2017 and November 17, 2021, defendant COLON posted to the SecurityTeam.io website that the "VIP" plan was only needed for attacking VPNs because "home connections are super easy to take down [] and it only takes about 50Mbps to take down a home connection so [it] is pointless to use VIP on a home connection."

Overt Act No. 4: On an unknown date between August 2017 and November 17, 2021, in response to a customer question about why an attack had been unsuccessful against a particular target, defendant COLON posted on the SecurityTeam.io website that "you probably just

need to use a different method or hit with a p[o]rt that's open on the server."

Overt Act No. 5: On an unknown date between August 2017 and November 17, 2021, defendant COLON posted an explanation on the SecurityTeam.io website under the heading "What is the difference between Layer 4 DDoS and Layer 7 DDoS," writing, "Layer 4 DDoS attacks refer to the attacking of the actual network. It requires a lot of bandwidth. Picture a store and its customers entering/leaving. We will say that the store is the host you are wanting to attack and the people are the packets you are sending to the host. What a DDoS does is literally push in a lot of people fast. This causes everything to become slower and eventually the store will become unavailable due to no one being able to enter."

Overt Act No. 6: On or about November 9, 2017, defendant COLON posted on the SecurityTeam.io website "I have created an insta boot API that you can use any link to create a short link and whoever you send it to when they click on it they will get booted for 100 seconds."

Overt Act No. 7: On May 11, 2021, an unindicted co-conspirator who was a customer of SecurityTeam.io used the SecurityTeam.io service to conduct a DDoS attack on victim L.D., located in Los Angeles, California.

COUNT TWO

[18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)(i), (c)(4)(A)(i)(VI)]

Beginning no later than August 2017 and continuing to on or about November 17, 2021, in Los Angeles County, within the Central District of California, and elsewhere, defendant ANGEL MANUEL COLON JR. knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage and attempted to cause damage by impairing the integrity and availability of data, programs, systems, and information on protected computers, as that term is defined in Title 18 United States Code, Section 1030(e)(2)(B), thereby causing and attempting to cause damage affecting ten or more protected computers during a one-year period beginning on or about November 17, 2020.

FORFEITURE ALLEGATION

[18 U.S.C. § 1030]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 1030, in the event of the defendant's conviction of the offenses set forth in any of Counts One and Two of this Information.

2. The defendant so convicted shall forfeit to the United States of America the following:

a. All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

b. Any property used or intended to be used to commit the offense; and

c. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i), the defendant, if so convicted, shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has

been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

E. MARTIN ESTRADA
United States Attorney

ANNAMARTINE SALICK
Assistant United States Attorney
Chief, National Security Division

CAMERON L. SCHROEDER
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

AARON FRUMKIN
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section