BRYAN SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: adam.alexander@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID BUKOSKI, Defendant.	)	Case No. 3:18-cr-00154-TMB

GOVERNMENT'S SENTENCING MEMORANDUM

SUMMARY OF SENTENCING RECOMMENDATIONS

TERM OF IMPRISONMENT ..... 12 Months

SUPERVISED RELEASE ..... Three Years

PROBATION ..... N/A

RESITUTION ..... TBD

COMES NOW the United States of America, by and through undersigned counsel, and hereby files this Sentencing Memorandum. For the reasons stated herein, the United States respectfully asks the Court to impose a sentence of 12 months and one day of imprisonment, followed by a three-year term of supervised release.

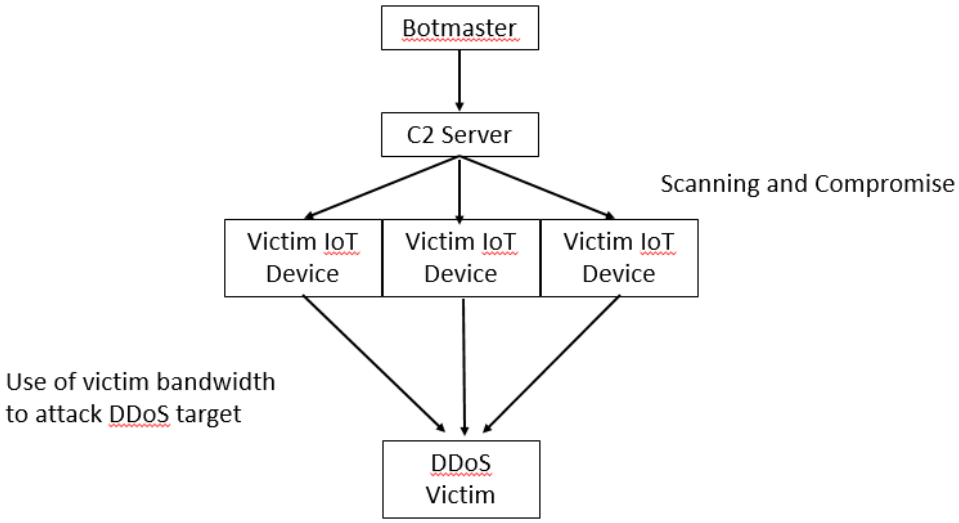
I. INTRODUCTION

a. Summary

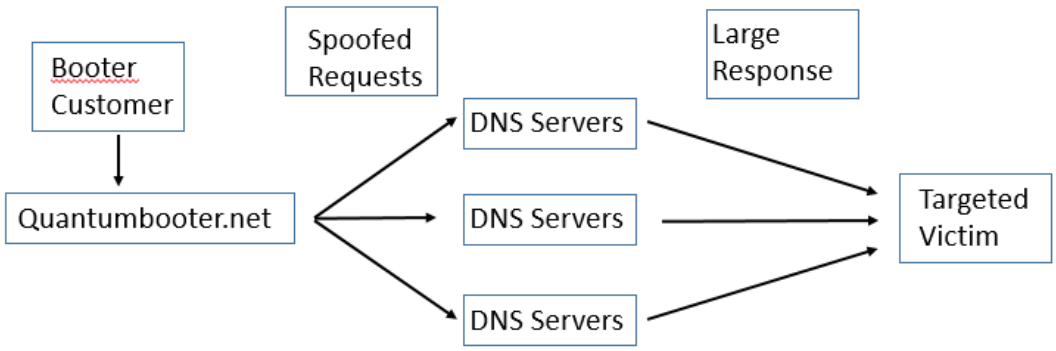
The defendant has pleaded guilty to operating a DoS for-hire service, commonly known as a "booter" or "stressor." Denial of service attacks (DoS) are a mechanism by which criminals can manipulate (in most cases stolen) bandwidth and architecture for the purpose of damaging the targeted victim's access to the internet by flooding them with internet traffic with the intent of causing damage or financial loss. Such attacks can range in scale and scope from those executed using the "Mirai" botnet, which channeled sufficient distributed bandwidth that they were capable of threatening not just individual devices or networks, but the upstream internet service providers as well, to those executed using amplification techniques common to less sophisticated booter services such as those operated by the defendant.

This court has previously imposed sentence on three individuals responsible for developing and deploying the Mirai botnet. PSR ¶9. That botnet was an assembly of thousands of hijacked Internet of Things (IoT) devices that were collectively compromised by that criminal group, and then used to target victims such as videogame servers with occasionally disastrous consequences for adjacent network infrastructure and the ISPs themselves, even those that had access to sophisticated DDoS mitigation.

After becoming aware of the FBI investigation into the Mirai botnet, those same defendants also created a successor botnet that was leased to other criminal groups for the purposes of conducting pervasive online advertising fraud. A simplified diagram depicting an IoT DDoS botnet is depicted below, illustrating a criminal's use of C2 server (or domain) to direct a botnet comprised of tens or hundreds of thousands of hijacked IoT devices to conduct a distributed denial of service attack on a victim device or network.



The purpose of this defendant's enterprise, by contrast, was to provide the ability to conduct wide-scale, if lower-level DoS attacks to paying customers who were not sufficiently sophisticated to develop their own DoS architecture, and who sought to target victims that did not have access to sophisticated DoS mitigation services. Lacking the technical skill necessary to scan the internet for vulnerable devices and compromise them at scale for the purposes of developing an IoT botnet, individuals like the defendant in this case use different techniques that capitalizes on existing architecture to conduct DoS attacks, such as that depicted below.



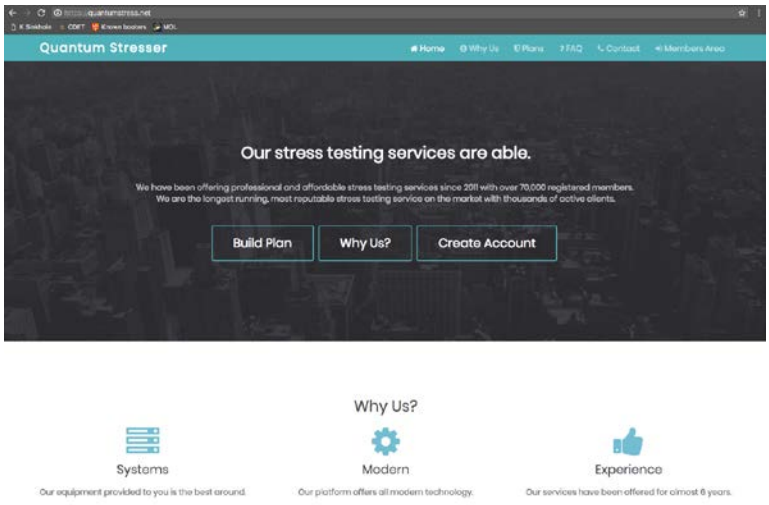
In this model, booter services such as Quantum use techniques such as DNS amplification, depicted in the simplified diagram above, to steal bandwidth in order to provide paying customers to conduct DoS attacks against third-party victims. This technique involves the use of an attack server to send UDP packets with spoofed IP addresses to DNS recursors that point to the victim device. This causes the DNS resolver to send a high volume of otherwise innocuous data to the victim device, which can overwhelm not only the victim but network adjacent infrastructure as well, resulting in a denial of service. This technique victimizes not only the DoS target but the servers providing the bandwidth to conduct the attacks based on the spoofed requests generated by the booter service. In simple terms, these attacks are analogous to a prank caller directing an innocent third-party to call the victim's telephone and leave a long voicemail, thus preventing the victim from receiving phone calls during that period.

Such attacks have become a persistently problematic feature of the contemporary internet landscape, as each attack individually may not be sufficiently significant to gain law enforcement attention, but when taken as a whole represent a significant threat to victims in the United States and abroad. The United States provides the summary below

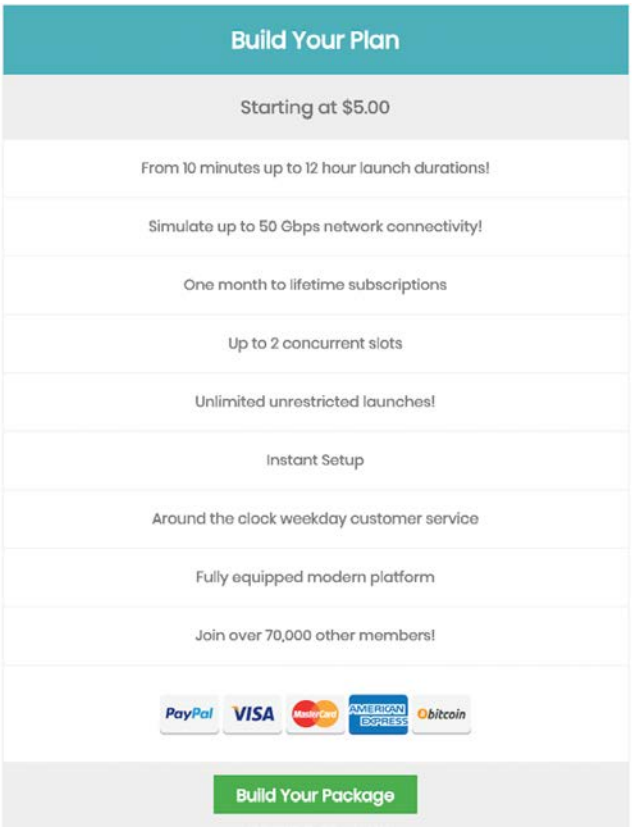
of both the nature of the offense conduct and the steps undertaken in the investigation to complement the information provided in the pre-sentence report and supplement the undisputed factual basis of the plea agreement. All of the information discussed below was previously shared with the defendant through his counsel.

b. Features and Purpose of QuantumStress.net

As part of a coordinated and ongoing inter-District operation, FBI agents began investigating individuals in the United States and abroad operating what were suspected to be the longest running and most prevalent "booter" services. The Defendant is one such individual, and during the period in question operated a website (or domain) operating under different names, but most recently "quantumstress.net." A screen capture of the Defendant's booter service operated through the domain "quantumstress.net." In the course of investigating the defendant's booter service, the FBI subscribed in an undercover capacity and conducted test attacks in order to verify that the defendant was in fact providing the services that he advertised, as seen below.



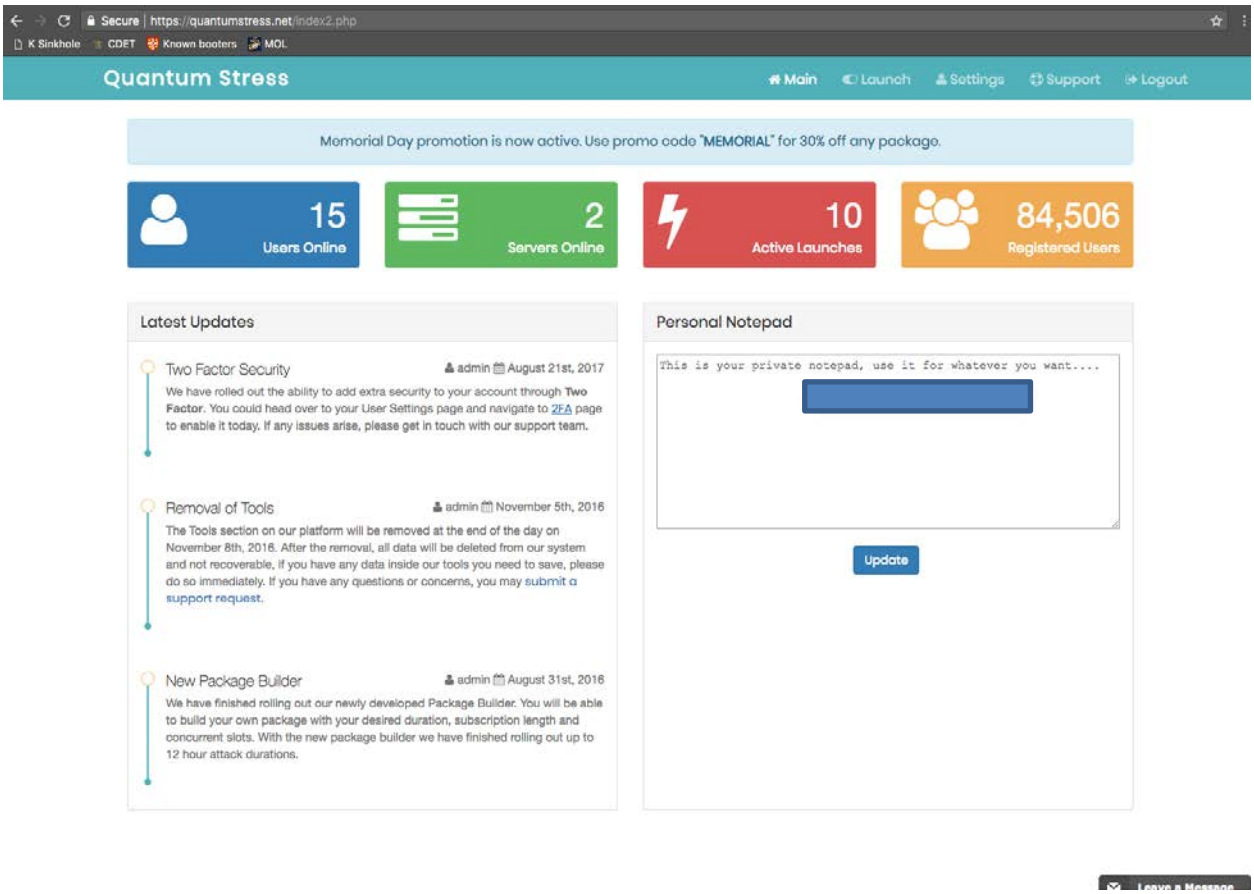
The defendant made a number of different subscription plans available to his approximately 70-80,000 subscribers, all of which entailed payment by the subscriber in exchange for some period of access to the attack infrastructure controlled by the defendant. An example of the defendant's advertisement of the features available to his subscribers is reflected in the following screen capture from the service:



Those features reference "launch duration," "network connectivity," "unlimited unrestricted launches" and "instant setup." Those terms are euphemisms for the type, volume, and duration of the criminal DDoS attack services the defendant provided to his paying customers.

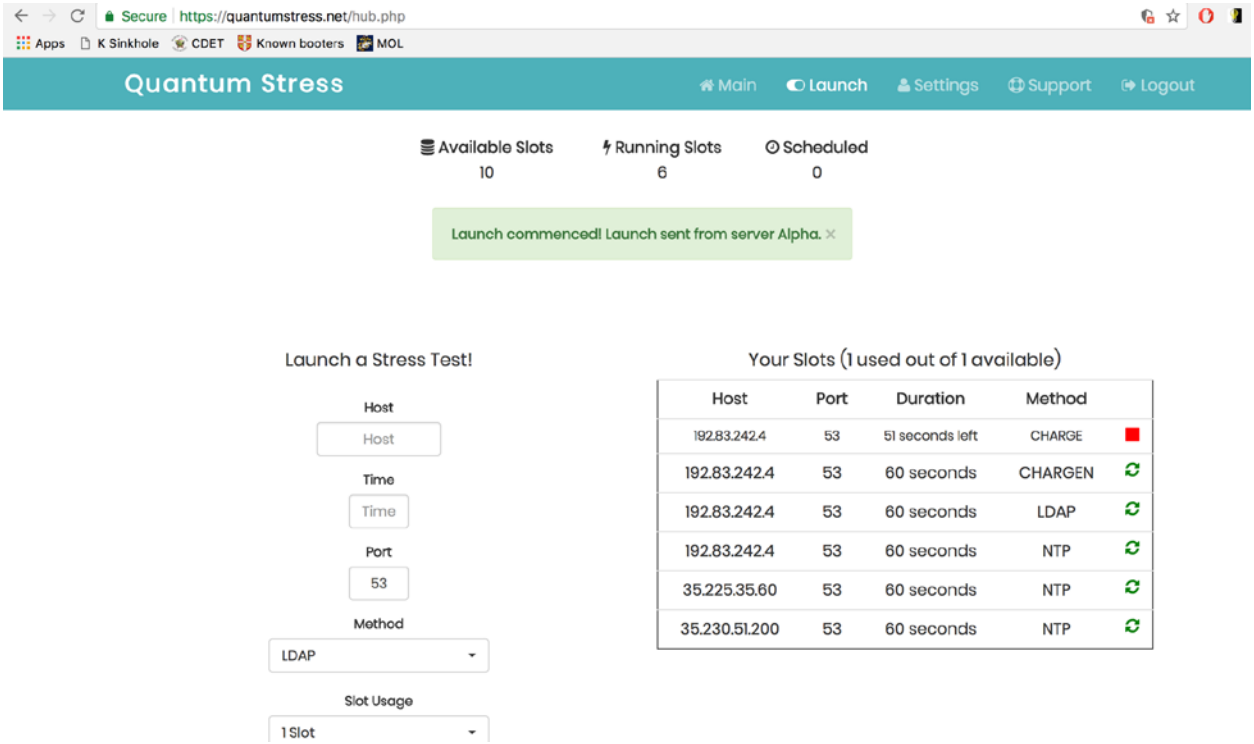
Paying subscribers would gain access to a private web accessible dashboard, depicted below. That dashboard would allow users to configure settings and launch

DDoS attacks against victims of their choosing using the architecture made available by the defendant in exchange for subscription fees that varied base on the type, magnitude and duration of the attacks purchased.



Several features of the defendant's dashboard depicted above are significant. The dashboard at the time the FBI took the snapshot referenced 15 other users being online at that time, with two servers available to conduct attacks, and 10 attacks underway. The defendant also configured his service to reference a tally of the number of registered (although not necessarily current) users of his service, numbered here at over 80,000. The defendant also references in the August 31, 2016 admin note that he has developed the capacity for his customers to launch attacks lasting as long as 12 hours.

The defendant configured the subscriber dashboard of his booter website to allow his customers to manually configure the settings to best tailor DoS attack types to their individual needs. An example of the customer dashboard is copied below.



As seen above, "stress test" is a euphemism for "DoS attack," and the defendant configured his service to allow subscribers to manually enter the desired target for their attacks, along with the attack duration, port targeted, and attack method.

c. Identifying the Defendant as the Operator of Quantumstress.net

Having determined that the booter quantumstress.net did in fact provide the criminal services advertised, the FBI then undertook an investigation that ultimately resulted in the identification of the defendant as the individual operating and profiting from the service. One of the first steps taken by the FBI was straightforward – performing a so-called "whois" query to determine basic information about the domain

itself. The results of that query are depicted below, and alerted investigators to the fact that the defendant was using a prominent internet service provider.

Address lookup

canonical name **quantumstress.net.**

aliases

addresses **104.27.132.250**
104.27.133.250
2606:4700:30::681b:85fa
2606:4700:30::681b:84fa

Domain Whois record

Queried **whois.internic.net** with "**dom quantumstress.net**"...

```
   Domain Name: QUANTUMSTRESS.NET
   Registry Domain ID: 2105005520_DOMAIN_NET-VRSN
   Registrar WHOIS Server: whois.name.com
   Registrar URL: http://www.name.com
   Updated Date: 2018-07-08T22:04:38Z
   Creation Date: 2017-03-14T21:06:15Z
   Registry Expiry Date: 2019-03-14T21:06:15Z
   Registrar: Name.com, Inc.
   Registrar IANA ID: 625
   Registrar Abuse Contact Email: abuse@name.com
   Registrar Abuse Contact Phone: 7202492374
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: BRIT.NS.CLOUDFLARE.COM
   Name Server: VERN.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-12-05T04:36:29Z <<<
```

Records associated with that internet service provider received in response to legal process gave investigators a number of email addresses that the defendant intended to be anonymous, but in fact allowed the FBI to work backwards and ultimately establish that the defendant was the owner and operator of the quantumstress.net booter service. By using additional process issued in the District of Alaska, the FBI was able to review records associate with internet accounts used by the defendant while operating quantumstress.net, including some of the defendant's internet browsing history. An excerpt of that history is copied below.

```
2017-12-10 22:12:16 UTC: Visited https://krebsonsecurity.com/2017/11/ddos-for-hire-service-launches-mobile-app/ (https://
krebsonsecurity.com/2017/11/ddos-for-hire-service-launches-mobile-app/)
2017-12-10 22:11:37 UTC: Visited https://krebsonsecurity.com/2017/11/ddos-for-hire-service-launches-mobile-app/ (https://
krebsonsecurity.com/2017/11/ddos-for-hire-service-launches-mobile-app/)
2017-12-10 22:11:29 UTC: Searched for quantumservicesweb@gmail.com (https://www.google.com/search?q=quantumservicesweb%40gmail.com
```

That excerpt of the defendant's web browsing history was significant to investigators for a number of reasons, including the fact that it shows that the defendant browsed an article written by a prominent security researcher referencing both the defendant's enterprise along with a competing service, including a link provided by the researcher in the article to an advisory posted by the FBI warning that the operation of booter services was potentially punishable under federal law.

09 DDoS-for-Hire Service Launches Mobile App

NOV 17

In May 2013 KrebsOnSecurity wrote about **Ragebooter**, a service that paying customers can use to launch powerful distributed denial-of-service (DDoS) attacks capable of knocking individuals and Web sites offline. The owner of Ragebooter subsequently was convicted in 2016 of possessing child pornography, but his business somehow lived on while he was in prison. Now just weeks after Poland made probation, a mobile version of the attack-for-hire service has gone up for sale on the **Google Play** store.

In the story Ragebooter: 'Legit' DDoS Service, or Fed Backdoor, I profiled then 19-year-old **Justin D. Poland** from Memphis — who admitted to installing code on his Ragebooter service that allowed FBI investigators to snoop on his customers.

Rageservices[dot]net advertises itself as a store for custom programming and Web site development. Its content is identical to a site called QuantumServices. A small purchase through the rageservices[dot]net site for a simple program generated a response from Quantum Services and an email from quantumservicesweb@gmail.com. The person responding at that email address declined to give his or her name, but said they were not Justin Poland.

Figures posted to the home page of ragebooter[dot]net claim the service has been used to conduct more than 310,000 DDoS attacks. Memberships are sold in packages ranging from $3 per day to $300 a year for an "enterprise" plan. Ragebooter[dot]net includes a notice at the top of the site indicating that rageservices[dot]net is indeed affiliated with Ragebooter.

If Poland still is running Ragebooter, he may well be violating the terms of his parole. According to the **FBI**, the use of DDoS-for-hire services like Ragebooter is illegal.

In October the FBI released an advisory warning that the use of booter services — also called "stressers" — is punishable under the Computer Fraud and Abuse Act, and may result in arrest and criminal prosecution.

"Booter and stresser services are a form of DDoS-for-hire— advertised in forum communications and available on Dark Web marketplaces— offering malicious actors the ability to anonymously attack any Internet-connected target. These services are obtained through a monetary transaction, usually in the form of online payment services and virtual currency. Criminal actors running booter and stresser services sell access to DDoS botnets, a network of malware-infected computers exploited to make a victim server or network resource unavailable by overloading the device with massive amounts of fake or illegitimate traffic."

The portions of the defendant's web browsing history reviewed by the FBI also showed his own use of the quantumstress.net booter:

```
2018-01-28 22:31:59 UTC: Visited Quantum Stress (https://quantumstress.net/launches?do=stop&id=452603)
2018-01-28 22:31:53 UTC: Visited Quantum Stress (https://quantumstress.net/launches?do=stop&id=452615)
2018-01-28 22:31:49 UTC: Visited Quantum Stress (https://quantumstress.net/launches?do=stop&id=452617)
2018-01-28 22:31:45 UTC: Visited Quantum Stress (https://quantumstress.net/launches?do=stop&id=452620)
2018-01-28 22:25:46 UTC: Visited Quantum Stress - Hub (https://quantumstress.net/hub.php)
2018-01-28 22:24:44 UTC: Visited Quantum Stress (https://quantumstress.net/launches?do=stop&id=452564)
2018-01-28 22:24:39 UTC: Visited Quantum Stress (https://quantumstress.net/launches?do=stop&id=452580)
2018-01-28 22:24:33 UTC: Visited Quantum Stress (https://quantumstress.net/launches?do=stop&id=452568)
2018-01-28 22:24:25 UTC: Visited IP-API.com - Free Geolocation API (http://ip-api.com/#65.96.167.141)
```

The defendant's administration of his booter service resulted in so-called 'terms of service' ("ToS") violation notices from a variety of platforms that did not wish to be associated with criminal DDoS for hire enterprises such as quantumstress.net. For example, the prominent e-commerce platforms such as PayPal and FastSpring, as well as the chat platform Discord all terminated the defendant's accounts as a result of the criminal conduct that came to their attention through his administration of quantumstress.net. Examples of those notices to the defendant are copied below:

From service@paypal.com ☆
Subject **Your account has been limited**
To d427pp@gmail.com <d427pp@gmail.com> ☆

Dear David Angrego,

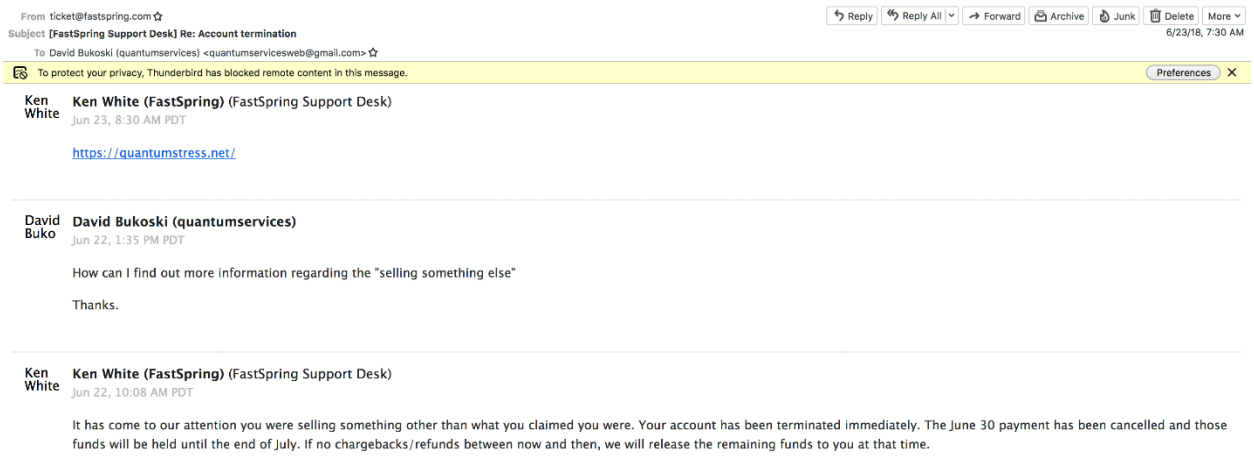
A recent review of your account activity identified products/services on your website violate PayPal's Acceptable Use Policy. Specifically, DDOS stressors that are associated with https://quantumstress.net and are not permitted on our platform.

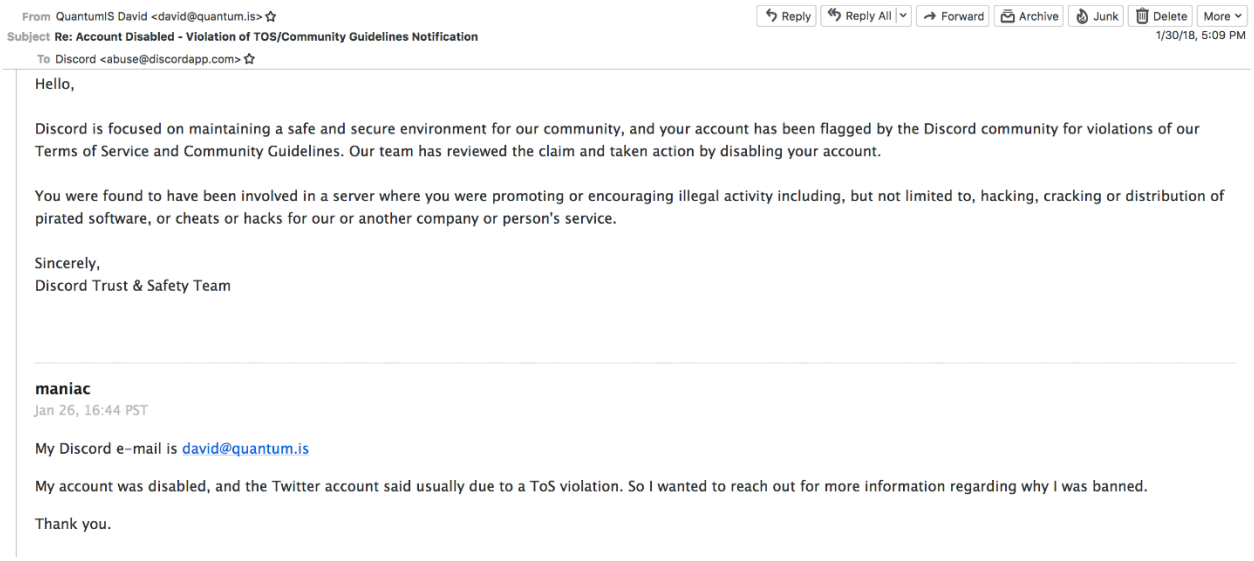
Please remove all references to PayPal from your website/s and/or auction/s. This includes not only removing PayPal as a payment option, but also the PayPal logo and PayPal shopping cart.

Please refer to:
- Transaction 8LT90027U6417631V

After a recent review of your account activity, it has been determined that you are in violation of PayPal's Acceptable Use Policy. Therefore, your account has been permanently limited.

Please remove all references to PayPal from your website/s and/or auction/s. This includes not only removing PayPal as a payment option, but also the PayPal logo and PayPal shopping cart.





From QuantumIS David <david@quantum.is>
Subject Re: Account Disabled - Violation of TOS/Community Guidelines Notification
To Discord <abuse@discordapp.com>

Reply | Reply All | Forward | Archive | Junk | Delete | More
1/30/18, 5:09 PM

Hello,

Discord is focused on maintaining a safe and secure environment for our community, and your account has been flagged by the Discord community for violations of our Terms of Service and Community Guidelines. Our team has reviewed the claim and taken action by disabling your account.

You were found to have been involved in a server where you were promoting or encouraging illegal activity including, but not limited to, hacking, cracking or distribution of pirated software, or cheats or hacks for our or another company or person's service.

Sincerely,
Discord Trust & Safety Team

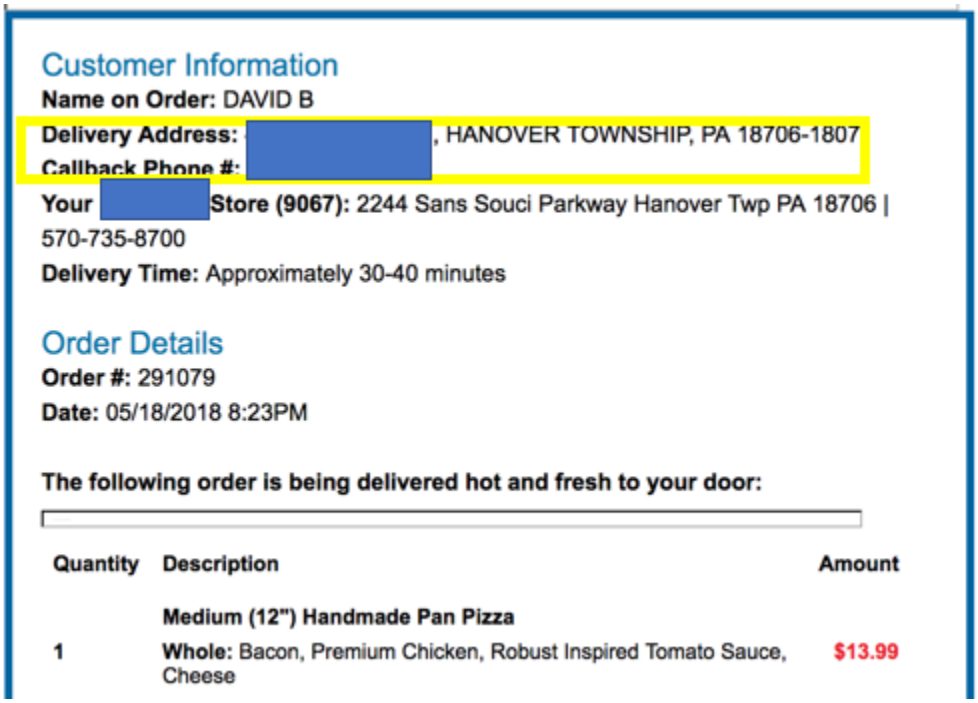
maniac
Jan 26, 16:44 PST

My Discord e-mail is david@quantum.is

My account was disabled, and the Twitter account said usually due to a ToS violation. So I wanted to reach out for more information regarding why I was banned.

Thank you.

In addition to evidence relevant to the defendants state of mind and knowledge regarding the activities of the quantumstress.net booter, the review of his internet accounts yielded the identifying information necessary for the FBI to apply for and execute a search warrant at the defendant's residence, including emailed receipts for pizzas that the defendant would have delivered to his home address:



Customer Information

Name on Order: DAVID B
Delivery Address: [redacted], HANOVER TOWNSHIP, PA 18706-1807
Callback Phone #: [redacted]
Your [redacted] **Store (9067):** 2244 Sans Souci Parkway Hanover Twp PA 18706 | 570-735-8700
Delivery Time: Approximately 30-40 minutes

Order Details

Order #: 291079
Date: 05/18/2018 8:23PM

The following order is being delivered hot and fresh to your door:

Quantity	Description	Amount
	Medium (12") Handmade Pan Pizza	
1	**Whole:** Bacon, Premium Chicken, Robust Inspired Tomato Sauce, Cheese	$13.99

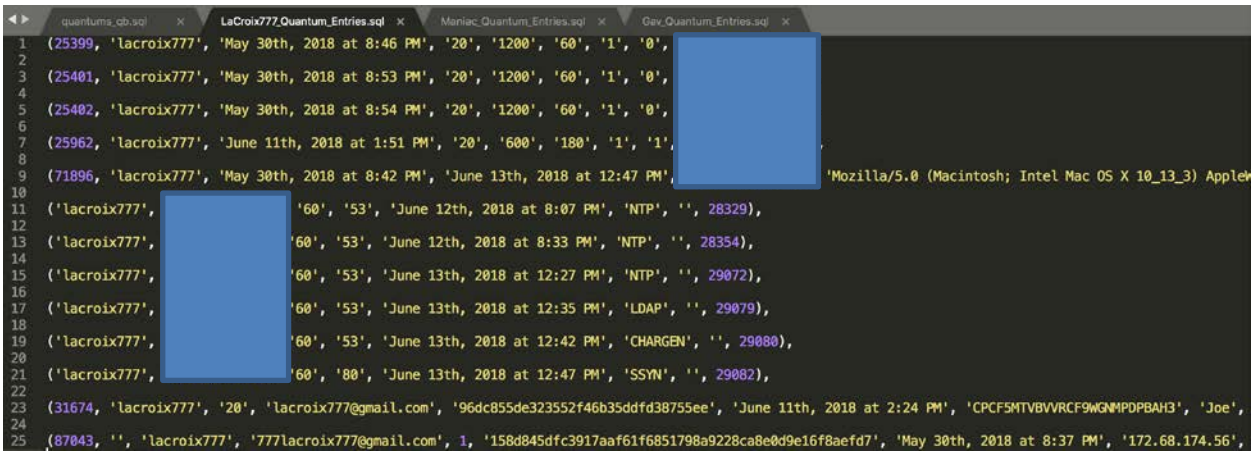
d. Interview and Search of the Defendant

In November, 2018 the FBI executed a search warrant at the defendant's residence in Hanover Township, Pennsylvania. In a recorded interview, the defendant, to his credit, was largely straightforward with investigators, admitting that he was the administrator of the booter service quantumstress.net; that he operated the booter service for profit for approximately seven years; and that he understood that the majority of his subscribers used the service to attack victims using DoS attacks facilitated by the architecture he provided. During the course of the search, the FBI seized and imaged devices including the defendant's primary cell phone and computers. The defendant also provided a copy of recent database entries associated with the operation of quantumstress.net to the FBI.

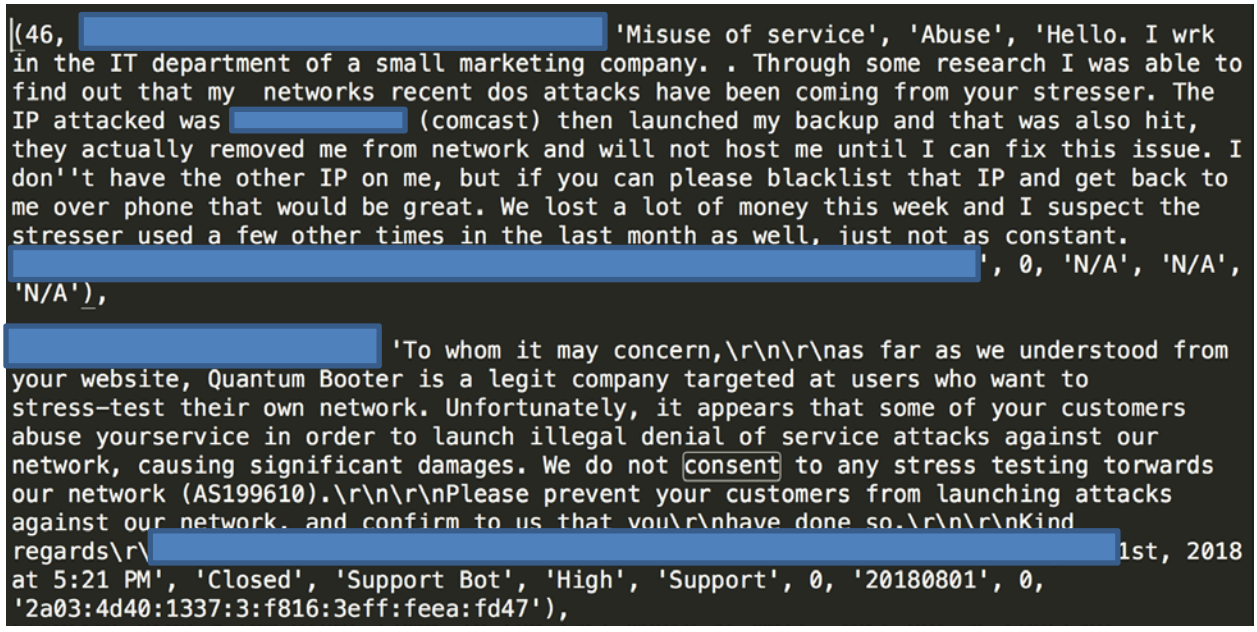
Those database records further corroborated the FBI's understanding of the operation of the quantumstress.net and the various pseudonyms used by the defendant during his administration of the booter service. The database included customer service tickets, or communications between the defendant and other individuals regarding the service.

In addition to records establishing that the defendant's quantumstress.net booter service had been used both by individuals outside of Alaska to attack Alaskan victims and individuals in Alaska to attack others outside, the database also contained records associated with the test attacks launched by the FBI using their undercover account ("lacroix777"), as seen below. It should be noted that the test attacks conducted by the FBI targeted safe IP ranges that would not actually be damaged, although the defendant

had no reason to know that was the case when the attacks were executed using his service.



The database provided by the defendant during the search of his residence also yielded communications to quantumstress.net from *victims* of attacks conducted by subscribers to the defendant's booter service. Two such communications asking the defendant to stop the attacks launched via quantumbooter.net by his paying customers are excerpted below:



II. Procedural History and Sentencing

a. Procedural History

The defendant was charged by indictment in the District of Alaska on December 12, 2018. Doc. 2. He was arraigned on the indictment on January 3, 2019. Doc. 11. The defendant pleaded guilty as charged on August 13, 2019, pursuant to the terms of the plea agreement filed at Docket 62. Doc. 73.

b. Pre-Sentence Report

The pre-sentence report filed at Docket 82 (PSR) accurately calculates the defendant's adjusted offense level as follows: base offense level of six for a violation of 18 U.S.C. § 1030(a)(5)(A) pursuant to U.S.S.G. §2B1.1; with a two-level enhancement for an offense involving 10 or more victims pursuant to §2B1.1(b)(2)(A); a four-level enhancement for sophisticated means pursuant to §2B1.1(b)(10)(C); and a four-level offense-specific enhancement resulting from the offense of conviction pursuant to 2B1.1(b)(19)(A)(ii), resulting in an adjusted offense level of 16, less three levels for acceptance of responsibility pursuant to U.S.S.G. §3E1.1 for a total offense level of 13. PSR ¶22. Given the fact that the defendant does not have any juvenile or adult criminal convictions in the United States, his guideline sentencing range as noted in the PSR is 12 to 18 months incarceration.

c. Probations' Sentencing Recommendation

Probations recommends a substantially below guideline sentence of five years' probation, largely based on the sentences imposed by this court in the matters related to

the Mirai botnet. For reasons the court is aware of, those cases are not analogous to this matter.

d. Sentencing Recommendation of the United States

Consistent with the terms of the plea agreement filed at Docket 61, the United States recommends that the court impose a sentence at the low end of the applicable advisory guideline range of 12 months (or 12 months and a day).

In the context of the nature and circumstances of the offense of conviction as well as the history and characteristics of the defendant himself, this recommended sentence is consistent with the imperatives of 18 U.S.C. § 3553(a), prioritizing the need for the sentence to imposed to afford adequate deterrence; protect the public from further crimes of the defendant; and provide the defendant with needed educational or vocational training as well as medical care or other treatment in the most effective manner.

The defendant made a modest but consistent income of, at times, between $1,500 and $2,500 monthly and totaling at least $101,273 during the time he operated the quantumstresser.net booter service. Doc. 62 ¶ 10-12 (Plea Agreement). That income was derived from the fact that he aided and abetted a substantial number of comparatively low-level DoS attacks committed by the approximately 84,000 individuals subscribing to his service at various times. Doc. 62 ¶16. As illustrated in the service tickets excerpted above, even these comparatively low level DoS attacks facilitated by the defendant's booter service had substantial effects on the targeted victims, which included personal computers on home networks as well as schools, universities, public utilities, and internet service providers. Doc. 62 ¶17.

While he took some steps to obscure his identity while operating his booter service, the defendant likely acted with impunity under the assumption that no single instance of criminal conduct he aided and abetted for profit would rise to the threshold of triggering a federal investigation and his subsequent prosecution in the District of Alaska. That assumption is not necessarily uncommon among individuals like the defendant who seek to profit by victimizing others.

It is appropriate for the court to take into consideration the defendant's poor health, comparative youth, and lack of prior criminal convictions, but those mitigating considerations should be weighed against the significant universe of those victims harmed by the defendant's actions and the concurrent need to not only specifically deter him from engaging in such conduct in the future, but also to serve as a deterrent to equally situated individuals and protect the public from this type of comparatively low-level but nevertheless persistent and wide-spread criminal activity.

III. CONCLUSION

For the above stated reasons, the United States respectfully recommends a sentence of no less than 12 months and a day, to be followed by three years of supervised release.

RESPECTFULLY SUBMITTED this 8th day of November, 2019, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Adam Alexander
ADAM ALEXANDER
Assistant U.S. Attorney

//

//

CERTIFICATE OF SERVICE

I hereby certify that on November 8, 2019, a copy of the foregoing was served electronically on:

Michelle Nesbett, Esq.

s/ Adam Alexander
Office of the U.S. Attorney