AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

MATTHEW GATREL and
JUAN MARTINEZ,

Defendants

Case No. MJ 18-3344

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief:

From an unknown date but no later than October 10, 2014, and continuing to November 19, 2018, in the County of Los Angeles, in the Central District of California, and elsewhere, defendants MATTHEW GATREL and JUAN MARTINEZ violated:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy to commit unauthorized impairment of protected computers, in violation of 18 U.S.C. § 1030(a)(5)(A)

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

ELLIOTT PETERSON, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/19/18

Judge's signature

City and state: Los Angeles, California

Hon. Michael R. Wilner, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Elliott Peterson, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since 2011. I am currently assigned within the Anchorage Field Office to the Counter Intelligence/Cyber Squad. I perform and have performed a variety of investigative tasks, including functioning as a case agent on computer crime cases. Since becoming a Special Agent of the FBI, I have received many hours of specialized cyber training, including on the topic of computer networking, online attribution techniques, and malware analysis. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I specialize in the investigation of botnets, Distributed Denial of Service ("DDoS") attacks, and crimes involving embedded devices, also known as the "Internet of Things."

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against, and summons for, MATTHEW GATREL ("GATREL") and JUAN MARTINEZ ("MARTINEZ") for a violation of 18 U.S.C. § 371 (Conspiracy to Commit Unauthorized Impairment of a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A)).

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

4. As described in detail below, GATREL has been operating two websites, downthem.org ("Downthem") and ampnode.com ("Ampnode"), both of which facilitate the conduct of Distributed Denial of Service, or "DDoS," attacks. MARTINEZ has been assisting GATREL in the operation of Downthem. Downthem is a DDoS service traditionally known as a "booter" or "stresser," essentially a website through which subscribers can attack unwitting victims for the express purpose of preventing the victims from properly using and/or accessing the Internet. Ampnode is a server subscription service in which GATREL provided servers suitable for subscribers to operate their own DDoS services, independent of an intermediary service or website such as Downthem.

5. As part of this investigation, I have reviewed records associated with the operation and workings of Downthem and Ampnode. This includes the records of a web service known as

"Cloudflare"[1] which provides DDoS defense solutions for Downthem's website. The Cloudflare records for Downthem indicated that email accounts associated with GATREL were used to register for the service. The records further indicated that IP addresses associated with GATREL were similarly used to access the Cloudflare service and perform administrative functions relative to the Downthem domain. During an interview of MARTINEZ on December 17, 2018, FBI agents also observed MARTINEZ log into the Cloudflare account tied to Downthem and Ampnode.

6. FBI agents obtained information about and content from email accounts used by GATREL to support and operate the Downthem and Ampnode services. These emails contained overlapping use of IP addresses associated with GATREL as well as high volumes of emails exchanged between GATREL and current and prospective customers, hosting providers, and others in furtherance of the operations of these websites. Within the accounts there were also references to GATREL's identity and physical address. The contents of the email accounts reflect that GATREL was extensively involved in the day-to-day operation of both the Downthem and the Ampnode DDoS services.

7. On November 19, 2018, GATREL was interviewed, and an image of his computer was taken. During the interview, GATREL admitted that he was the user of the email accounts reviewed by

[1] Cloudflare is a "Content Delivery Network" (CDN) provider, and as such will offer its services to host a given website at multiple locations across the globe so as to ensure speedy website access to end users regardless of the users' own locations.

the FBI, and that he was the administrator of both the Downthem and Ampnode services. GATREL also indicated that another individual, who he knew only as "Severon," was helping him administer the Downthem site. GATREL stated that "Severon" utilized the email severon[*redacted*]@gmail[.]com. GATREL provided interviewing agents with two databases containing logs related to Downthem and Ampnode. A review of the database associated with the Downthem site indicated that it had been used to conduct or attempt to conduct over 200,000 DDoS attacks since 2014.

8. On December ~~18~~ 17 EPP, 2018, MARTINEZ was interviewed. During the interview, MARTINEZ stated that he utilized the email severon[*redacted*]@gmail[.]com and had been assisting with the operation of the Downthem website for a number of months. MARTINEZ accessed the Downthem website and downloaded a copy of the database. The database appeared to be a more recent version of the database provided by GATREL.

IV. SUMMARY OF RELEVANT COMPUTER AND INTERNET CONCEPTS

9. The information provided below regarding relevant computer and internet concepts is based on my training and experience:

a. "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard[2] format for IP addressing consists of

[2] IP version 4, or "IPv4", is the version of IP most commonly used today, and is the version described above. A newer version of the protocol, "IPv6", wholly different in

four numbers between 0 and 255 separated by dots, *e.g.*, 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet Service Providers ("ISPs") assign IP addresses to their customers' computers. ISPs typically log their customers' connections, allowing them to identify which of their customers was assigned a specific IP address during a particular session.

b. "Domain Names" serve to identify Internet resources, such as computers, networks, and services, with a text-based label that is easier to memorize than an IP address. A domain name consists of one or more parts (or "labels") that are conventionally concatenated and delimited by dots, such as *example.com*. The right-most label conveys the top-level domain; for example, the domain name *www.example.com* belongs to the top-level domain *com*.

c. "Server" is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes called "clients." Server computers can be physically located

appearance to IPv4, is sometimes used, but does not pertain to this request, and will not be referred to further.

anywhere. For example, it is not uncommon for a network's server to be located hundreds, or even thousands of miles away from the client computers.

d. "Name Servers" are server applications which function like a phonebook. Name Servers will accept queries for domain names (such as example.com) and return an IP address associated with the domain, much as the name John Doe might be looked up in a telephone book to determine the corresponding telephone number.

e. "Distributed Denial of Service" attacks, or "DDoS" attacks, are a type of network attack in which multiple Internet-enabled devices are used to attack computers for the purpose of rendering them inaccessible to legitimate users or unable to communicate with the Internet.

V. STATEMENT OF PROBABLE CAUSE

A. Description of Booter and Stresser Services

10. "Booter" or "Stresser" services are a class of DDoS attack tool designed to flood a website or server with internet traffic, making the targeted website unable to be accessed by legitimate users or customers. These services are characterized by their accessibility and affordability, and require relatively little skill for the prospective attack customer to purchase and operate. Booter services are so named because the attacks they conduct result in the "booting" or "dropping" of the victim targeted website from the Internet. More recently, they have

also been called "stressers" in an attempt to suggest that they have a legitimate use in testing the strength of DDoS defenses. As discussed below, the services Downthem offers operate in the same manner common to most booter services, that is, they flood the victim with tremendously high volumes of unsolicited traffic, effectively preventing the victim from receiving or responding to normal traffic and therefore from properly using the Internet. Based on my training and experience, the name of GATREL's "Downthem" service likely refers to the act of "taking down" a target web service.

11. Based on my training and experience, booter-based DDoS attack tools represent an effective advance in Internet attack technology because they provide such a relatively low barrier to entry. These services accept common online payment methods such as PayPal, Google Wallet, and Bitcoin.[3] Previous work by law enforcement and private sector partners has reduced the ability of these booters to use payment services such as PayPal and Google Wallet as effectively, and so the most common payment method is now Bitcoin and other similar cryptocurrencies.

12. Based on my training and experience, the rates charged to customers by booter services vary according to the specific service, the desired "bandwidth" or attack size, the attack

[3] Bitcoin and similar cryptocurrencies are types of digital currency in which transactions are made without governance by any central bank, and encryption techniques are used to regulate the generation of units of currency and to verify the transfer of funds. Based on my training and experience, I know that this type of currency is often used to conceal the identities of the parties involved in a financial transaction.

type, and the number of "concurrent" attacks allowed. For example, a premium, "VIP" account on a given booter service might cost $100 a month and allow access to ten or more attack types, a peak attack bandwidth of 30 Gbit/s,[4] and the ability to attack up to four IP addresses at one time. A "basic" plan might cost $25 to $35 a month and provide a more limited number of attack types, while allowing the customer to attack only a single IP address at a time. As described in more detail below, the FBI has conducted testing of Downthem, and has found that it follows this basic pattern.

13. I have interviewed many of the preeminent experts in the field of Internet attack technology, including those at domestic Internet Service Providers (ISPs) who often observe thousands of attacks a day. From these interviews, I have learned that some domestic ISPs utilize a form of networking hardware known as an "aggregator" to bundle downstream customer accounts; that one common network implementation results in up to 10,000 domestic ISP customers downstream of a single aggregator; and that many aggregators can only sustain incoming Internet traffic volume of 40 Gigabits per second (Gbit/s) and below. Other ISPs may employ different technologies or procedures that still result in certain ceilings for peak bandwidth received, after which a DDoS attack can affect more than just the intended target; for example, a very large attack

[4] Gbit/s, or Gigabits per second, is a volumetric measure of network data. An average US domestic cable Internet subscriber might experience speeds of 10-50 Megabits per second (Mbit/s). One Gigabit is equivalent to 1000 Megabits.

could result in an outage affecting an aggregator or similar device, resulting in Internet degradation or disruption for associated customers.

14. Therefore, Internet traffic exceeding 40 Gbit/s can result in the inability of an aggregator to route any further traffic. Larger attacks can have even more severe effects. The FBI's testing of various booter services showed that some services achieved attack volumes of up to 30 Gbit/s for their more basic plans; many, including Downthem, advertised the ability to achieve substantially higher attack volumes, up to 200 Gbit/s in Downthem's case (the FBI did not purchase or verify these higher-volume plans). Therefore, even at the lower volumes verified, the simultaneous use of two such services, at a combined cost of under $50 month, could result in an Internet outage for up to 10,000 ISP customers, for as long as the attacker was capable of implementing the attack. These booter services thus represent a distinct and growing threat to reliable access to Internet services.

15. Booter services advertise their attack capabilities publicly, on web pages, criminal forums, chat platforms, or with video services such as YouTube. In some cases, what appear to be distinct booter services (with different names and branding) are merely different front ends for the same underlying attack architecture. In some cases, booter operators rely on third parties, such as GATREL's Ampnode service, to provide the attack infrastructure that their services require in order to provide these DDoS attacks.

16. Based upon my training and experience, I know that of the many types of DDoS attacks offered by booter sites, among the largest, in terms of sheer volume, tend to be Reflective Amplification Attacks ("RAA"). RAA DDoS attacks function as follows:

a. First, the attacker learns the victim's IP address. This can be done through a variety of methods, including "resolvers" offered by the DDoS-for-hire sites themselves. These resolvers can, for example, discover the true IP address associated with a web server so that an attack can bypass anti-DDoS defenses such as Cloudflare, determine on which IP address a given website or domain is hosted, or determine an IP address associated with a given Skype username.

b. Second, the attacker chooses a "protocol," i.e., a type of communication between computers, which enables the attacker to send a very small request to a neutral third party and get a very large response. There are several Internet services which - though created for legitimate purposes - are commonly misused by booter services to craft large RAA DDoS attacks. Examples include SSDP, also known as Simple Service Discovery Protocol, which allows for the advertisement and discovery of network services; NTP, or Network Time Protocol, which allows clock synchronization between computer systems; DNS, or Domain Name System, which facilitates the translation of domain names to IP addresses; and Chargen, or Character Generation Protocol, which facilitates testing and debugging.

c. Third, the attacker crafts and sends such a request, but in doing so "spoofs" the request's origin: rather than using the attacker's own IP address, the attacker falsifies the victim's IP address as the source, thus ensuring that the victim, rather than the attacker, receives the resulting flood of data from the protocol request.

d. Fourth, the neutral third party receives the request, and is tricked by the "spoofed" origin IP address - the third party returns its much larger response not to the attacker, but to the victim.

e. The attacker then replicates this process many times a second, often using many different third parties to reflect and amplify the attack, hence the name "Reflective Amplification Attack."

f. As a result, the victim receives an overwhelming amount of unsolicited Internet traffic, saturating its ability to communicate, and effectively taking it offline for the duration of the attack.

17. RAA DDoS attacks, as described above, are characterized by amplification factors - the size of the response data relative to the given query. For example, issuing the command "dig ns fbi.gov," a single line of query, results in approximately 20 lines of text returned from the third-party "reflector" service. This command/query can thus be said to have an amplification factor of approximately 20. Using similar procedures, RAAs magnify the bandwidth available for attack by factors of 10, 20, 100, and even more. By doing so, RAAs

appropriate bandwidth resources from the third-party reflectors, resources that the attacker does not pay for, and which far exceed "normal" use of those third parties, offloading the costs of RAAs to those third-party servers and their upstream providers.

18. Further, as described above, an additional essential component of RAA is fraudulent misdirection. It does the attacker no good if the requested data is directed back to the attacker. The "spoofing" of the victim IP address is a central component of the attacks conducted by the booter services investigated by the FBI. There are also legitimate uses for "spoofing" the source IP address of outbound Internet traffic, including research, application testing, and anonymity functions, but it is becoming less and less common for ISPs to allow customers to use spoofing, given the prevalence of abuse and crime associated with spoofing.

19. The last component of an RAA is one of distribution. Instead of issuing the query to a single third-party reflector, the query may be issued to hundreds or thousands of such third-party reflectors simultaneously, each of which returns with "amplified" responses. The resulting deluge of attack data saturates the network connection of the victim target website, and often negatively affects many other Internet users or servers that stand between the attacker and the victim.

20. It should be noted that most, though not all, booter services that I have reviewed will offer some token language within their Terms of Service which attempts to absolve the

booter service from responsibility for attacks launched by their customers. This language may include statements such as "Under this license you may not intentionally send a DDoS flood to an IP address not owned by yourself." Based on my training and experience, I believe this language is essentially a pretense. Because RAA DDoS attacks by definition rely upon external services to act as "amplifiers," they must flood traffic to those external services en route to the victim, impairing and degrading the capacity of those services, for which they have received no permission. Furthermore, many of the booter services I studied, including Downthem, offered services known as "resolvers" - the purpose of which is to obtain the IP address of a victim; such resolvers would be entirely unnecessary if any customer was targeting their own infrastructure.

21. During the course of this investigation I have studied the effects of these attacks, as well as those targeted by DDoS attacks. Over the last several years, databases from booter services have been leaked online, and/or have in other instances been obtained lawfully by law enforcement, including, as described below, a database associated with Downthem in particular. These databases can contain data on attack targets and the individuals that ordered them, as well as the subjects involved in the day-to-day operation of the services. I have examined several leaked and/or seized booter databases. The data contained within those databases indicates that DDoS attacks affect every district in the United States, and that

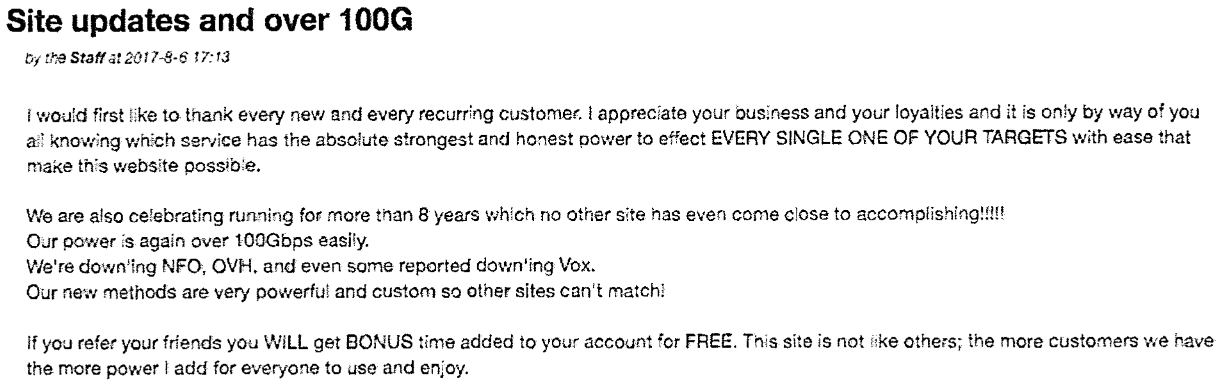
customers of these services exist all over the United States and in other countries. I have also learned through my investigation and review of these databases that booter services are responsible for attacking large numbers of sensitive targets, among them websites belonging to federal, state, and municipal government entities, military websites, websites belonging to the media, and websites belonging to universities and secondary schools. My review of the database showed that Downthem was used to attack or attempt to attack all of these types of targets.

22. Accordingly, I and my FBI colleagues, in collaboration with private sector subject matter experts investigating DDoS attacks, prioritized from among the dozens of known booter services a shortlist of those booters believed to be most egregious, according to criteria such as the number of purported attacks, DDoS attack strength, accessibility, or other factors. Downthem was one of the services so targeted.

B. Downthem and Ampnode Service and FBI Testing

23. On May 30, 2018, I accessed the site downthem.org. Agents observed that the site was designed to offer DDoS attacks for sale, and further found it to contain a list of messages from administrators to users. One such announcement, depicted below, referenced the attack power of Downthem and claimed to

offer the "absolute strongest and honest power to effect [sic] EVERY SINGLE ONE OF YOUR TARGETS with ease":



Site updates and over 100G

by the ***Staff*** *at 2017-8-6 17:13*

I would first like to thank every new and every recurring customer. I appreciate your business and your loyalties and it is only by way of you all knowing which service has the absolute strongest and honest power to effect EVERY SINGLE ONE OF YOUR TARGETS with ease that make this website possible.

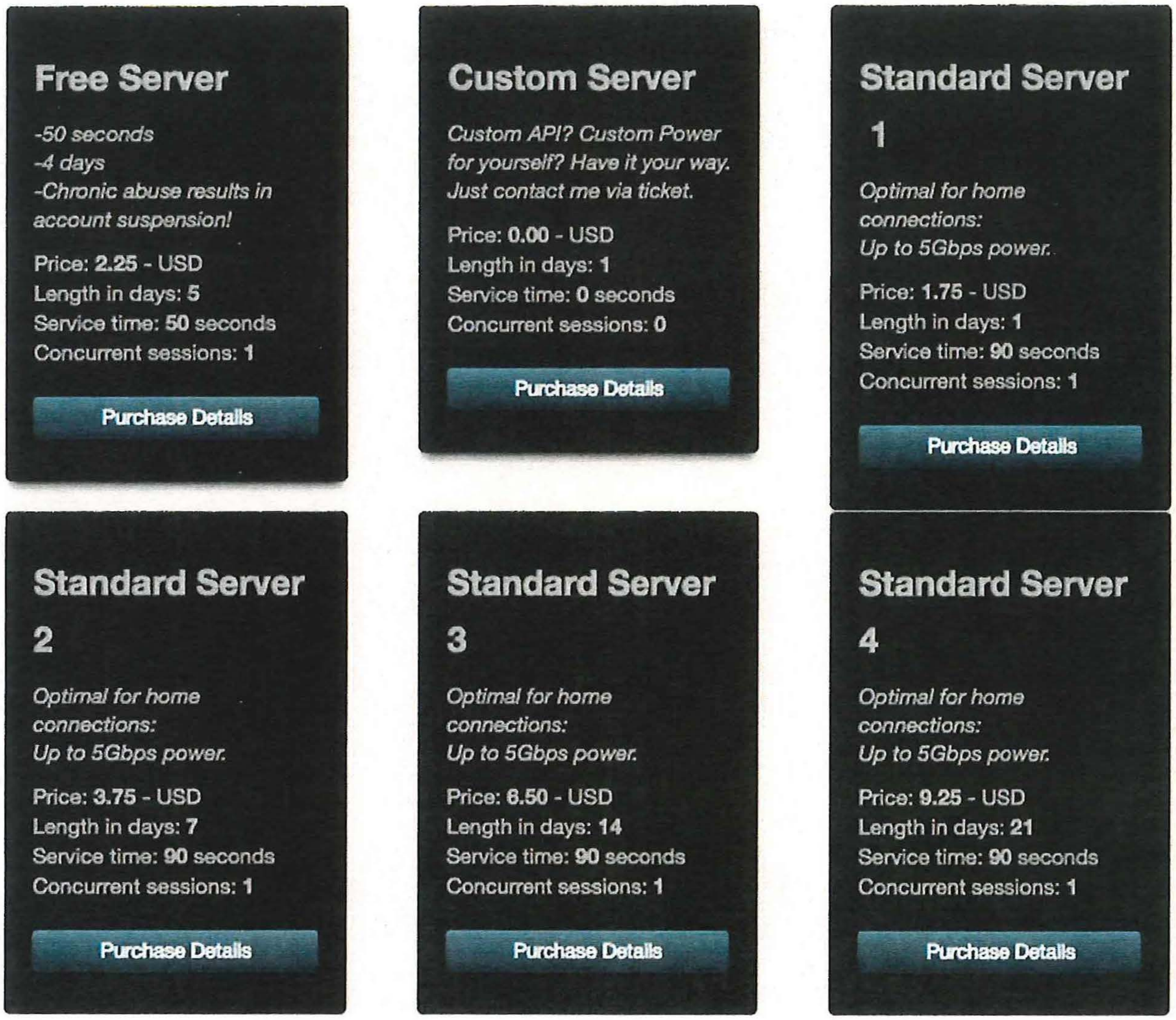
We are also celebrating running for more than 8 years which no other site has even come close to accomplishing!!!!!
Our power is again over 100Gbps easily.
We're down'ing NFO, OVH, and even some reported down'ing Vox.
Our new methods are very powerful and custom so other sites can't match!

If you refer your friends you WILL get BONUS time added to your account for FREE. This site is not like others; the more customers we have the more power I add for everyone to use and enjoy.

24. This message also notes that the service had been "running for more than 8 years which no other site has even come close to accomplishing!!!!! Our power is again over 100Gbps easily." This same post referenced the ability to "down" NFO, OVH, and Vox. Based upon my training and experience, I know NFO, OVH, and Vox to be web hosting platforms that are frequently victims of DDoS attacks, and also platforms that host numerous U.S. and international business websites. I also know that they are very large and robust Internet services designed with DDoS defense in mind, and that for a booter service to reliably "down" a server at one of these web hosting platforms would require very large attacks, much larger than what is required to disrupt internet access at most homes and businesses.

25. Downthem advertises to customers that it can conduct DDoS attacks, as described above, capable of severely disrupting home and small business Internet connections for prices of around $1.75 per day, with prices decreasing with longer

duration subscriptions. Below is a screenshot representing the first six tiers of DDoS subscription plans offered by Downthem, of which there are more than ten, the largest of which purports to offer 200 Gbit/s of DDoS attack bandwidth. This screenshot was taken on May 30, 2018:



Free Server

-50 seconds
-4 days
-Chronic abuse results in account suspension!

Price: **2.25** - USD
Length in days: **5**
Service time: **50** seconds
Concurrent sessions: **1**

Custom Server

Custom API? Custom Power for yourself? Have it your way. Just contact me via ticket.

Price: **0.00** - USD
Length in days: **1**
Service time: **0** seconds
Concurrent sessions: **0**

Standard Server 1

Optimal for home connections:
Up to 5Gbps power.

Price: **1.75** - USD
Length in days: **1**
Service time: **90** seconds
Concurrent sessions: **1**

Standard Server 2

Optimal for home connections:
Up to 5Gbps power.

Price: **3.75** - USD
Length in days: **7**
Service time: **90** seconds
Concurrent sessions: **1**

Standard Server 3

Optimal for home connections:
Up to 5Gbps power.

Price: **6.50** - USD
Length in days: **14**
Service time: **90** seconds
Concurrent sessions: **1**

Standard Server 4

Optimal for home connections:
Up to 5Gbps power.

Price: **9.25** - USD
Length in days: **21**
Service time: **90** seconds
Concurrent sessions: **1**

26. Based on my training and experience, the above screenshot advertised some of the different DDoS service plans offered by Downthem. For example, the "Standard Server 2" plan description described a DDoS attack plan in which the attacker

would be able to launch an unlimited number of attacks on a website or server during the seven-day subscription period, provided the length of those attacks did not exceed 90 seconds in length. The cost of this plan was $3.75. At the time of FBI testing in May of 2018, Downthem appeared to accept cryptocurrency and Paypal as forms of payment for its offered services.

27. Downthem also advertised that they provide RAA-type attacks.[5] The FBI's testing indicated that Downthem in fact delivered RAA DDoS attacks, and in sufficient volume to interrupt the Internet activity of almost any normal user.

28. Based on my review of their respective websites, as well as email messages and email accounts pertaining to their operation (described below), Ampnode and Downthem appear to be distinct services without obvious overlapping architecture. Ampnode presents more complexity for use by a given customer to conduct DDoS attacks. That is because instead of simply navigating to a website and entering an IP address, as with the Downthem service, with Ampnode, the administrator establishes a server on which the customer must perform additional configuration in order for the server to be capable of performing DDoS attacks. The advantage of such an arrangement is that the customer can then use this architecture to create

[5] Downthem does not use the term "RAA" on its website and instead uses terms such as "chargen," "NTP," and "UDP," which I know based on my training and experience to be internet protocols that are abused to function as RAA-type attacks. Further, the FBI's testing confirmed that Downthem conducted DDoS attacks using RAA methods.

their own distinct booter service, potentially allowing for attacks with even higher bandwidth than might otherwise be available using Downthem. Further, based on the review of email messages associated with the administration of the Ampnode service, and my interview with GATREL (described below), GATREL was not merely establishing the architecture for a given customer. GATREL also provided "amp lists," or amplification lists of vulnerable servers which he would sell to Ampnode customers in order for them to conduct the most powerful attacks possible. When GATREL was interviewed, he stated that these lists were available for purchase directly from the Ampnode website.[6] Based on my training and experience, I know that most customers intending to run their own DDoS services from Ampnode servers would need to buy or generate such amplification lists on a regular basis in order to ensure that they were communicating with the largest possible number of vulnerable servers. This relates directly to the amplification factor that their service can achieve with a given attack method, as described above.

29. As part of the investigation, the FBI purchased packages at downthem.org to evaluate the service and determine if it was actually functioning (with the permission of the targeted "victims").[7] As a result of law enforcement testing,

[6] During the interview, GATREL stated that he would immediately remove such lists from the website and would no longer offer them for sale to prospective customers.

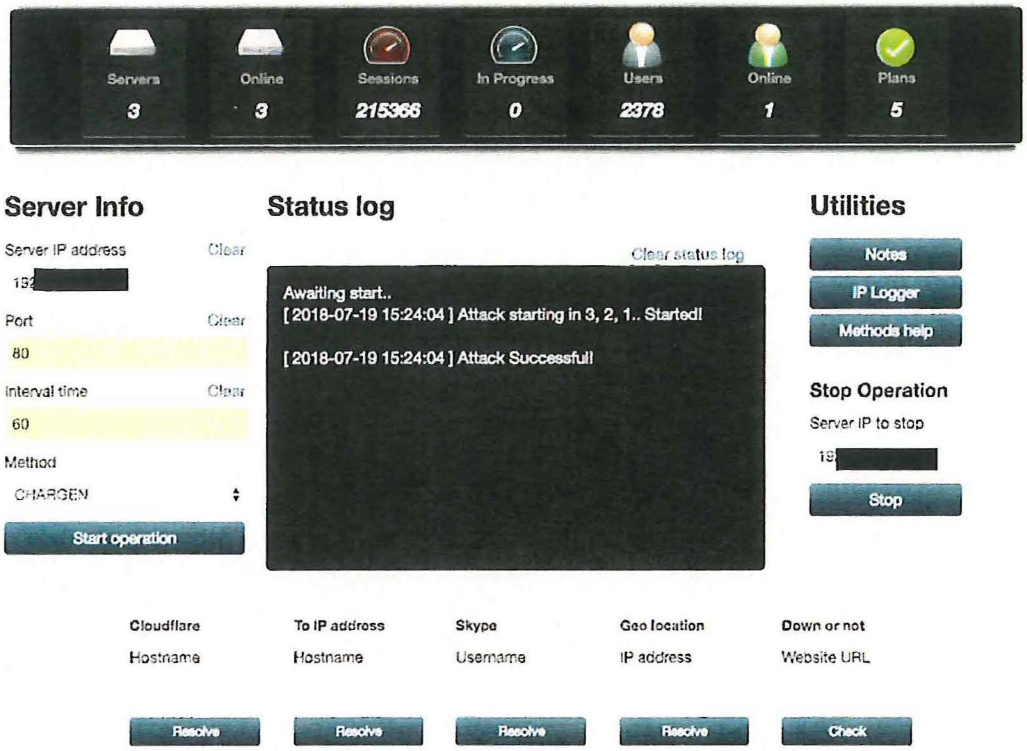
[7] I know from previous investigation and consultation with other agents and Internet security experts who specialize in

conducted in June and July of 2018 for Downthem, the FBI determined that many of the offered DDoS attack types were functioning, and were capable of delivering sufficient attack volume to saturate a typical commercial Internet connection. This indicates a sizeable attack volume, as the bandwidth of a typical commercial Internet connection usually exceeds that of a residential connection. The FBI conducted its testing, and provided payment, from computers in Los Angeles, California, and Anchorage, Alaska, and directed the attacks to computers in the same areas.

30. While true volumetric testing of DDoS attacks can require highly specialized software and hardware, based upon my training and experience, and based on conversations with other FBI and private sector colleagues, I and other testing FBI agents judged that the majority of the functioning attacks easily consumed all available Internet bandwidth available to the test "victim" computers. That is to say that Downthem functioned as advertised, providing a vehicle with which to conduct illegal DDoS attacks. Below is a screenshot from one of the tests of the Downthem service which occurred on July 19, 2018. As an explanation for the screenshot below, the website was configured such that a user entered the IP address of the intended victim, in this case identified by the "Server IP

booter services that many services have poorly functioning Application Program Interfaces (APIs). As a result of the poorly functioning APIs, not all booter services function properly, or deliver the promised attack volumes and types. However, as described herein, Downthem appeared to function as advertised.

Address" field. The user then entered a port number ("Port"), duration ("Interval Time"), type of Internet Protocol to be used in the attack ("Method"), and then initiated the attack ("Start operation").



Server IP address: [redacted]

Port: 80

Interval time: 60

Method: CHARGEN

Server IP to stop: [redacted]

```
Awaiting start..
[ 2018-07-19 15:24:04 ] Attack starting in 3, 2, 1.. Started!

[ 2018-07-19 15:24:04 ] Attack Successful!
```

31. At the bottom of the screenshot are several "resolver" tools, which, as described above, are designed to better facilitate a user's ability to conduct DDoS attacks. The first such tool attempts to resolve Cloudflare IP addresses, that is, discover the true IP address associated with a web server so that the DDoS attack can bypass Cloudflare defenses. The second resolver takes a given website or domain and determines which IP address it is hosted on. The third attempts to determine an IP address associated with a given Skype username. I am familiar

with all of these resolving tools and know them to be part and parcel of criminal DDoS services. In particular, these types of resolvers are only necessary if the user of Downthem's services does not own or have permission to access the targeted computer; if they did so, they would reasonably already know the targeted IP address and would have no use for the resolvers. Thus, these resolving services are another indicator that the site is designed for unlawful purposes - that is, to target others' computers without authorization.

C. Ampnode Use by Other Booter Services

32. Based on review of email messages obtained via a search warrant and an interview of an individual named David Bukoski ("Bukoski"), as well as review of the Ampnode database provided by GATREL as described below, I have also learned that Bukoski was a customer of GATREL's Ampnode service. Bukoski has been charged in the District of Alaska for Aiding and Abetting Computer Intrusions, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 2, in case No. 18-CR-00154-TMB-DMS, for operating the QuantumStress.net booter service, which provided a DDoS subscription platform for customers.[8] Bukoski's booter service was one of the longest-running services targeted by the FBI, operating since at least 2012; it has operated under different names but is presently known as QuantumStress.net. Based on examination of a database for the QuantumStress service provided by Bukoski, as well as examination of the QuantumStress website,

[8] As of the date of this affidavit, changes have been made to the QuantumStress.net website so that customers are no longer able to conduct DDoS attacks.

I determined that QuantumStress.net has had over 80,000 customer subscriptions, including customers within the Central District of California and the District of Alaska. Based on examination of the database, I learned that during 2018, QuantumStress.net was used to conduct over 50,000 actual or attempted DDoS attacks, and that these attacks targeted victims worldwide, including victims in the Central District of California and the District of Alaska. These targets included U.S. university networks, state and local government networks, U.S. government networks, gaming platforms, and major Internet Service Providers, including residential, commercial, and mobile networks.

33. Based on review of the Ampnode database, email accounts tied to Bukoski, and statements made by Bukoski, it appears that he used GATREL's Ampnode service in order to facilitate the DDoS attacks provided by his service, QuantumStress.net. That is, one or more Ampnode servers, procured by Bukoski via GATREL, provided the backbone through which QuantumStress.net issued DDoS attacks on behalf of its customers. Review of the Ampnode database and emails associated with Bukoski revealed that Bukoski and GATREL negotiated Bukoski's procurement of servers via email and messaging on the Ampnode website.

D. Email Records Associated with Downthem and Ampnode

34. A federal search warrant was issued in the District of Alaska for records between July 17, 2014, and June 22, 2016, for email accounts believed to be associated with the Downthem

booter service, as well as the Ampnode service. A second federal search warrant was issued in the Central District of California on July 30, 2018, again for accounts associated with these services, for the time period January 1, 2016 to July 30, 2018. The FBI determined that these accounts were associated with the Downthem and Ampnode services through examination of login IP addresses and subscriber information, including email addresses, as well as other ways, and the content of the accounts confirmed this association. During an interview with law enforcement agents, described below, GATREL also admitted that each of the relevant email accounts belonged to him and that he administered both services. Review of the records provided by Google in response to this search warrant revealed that these accounts were used by GATREL to facilitate his operation of the Downthem and Ampnode services.

a. As an example, on July 10, 2017, an email was sent to ampnode[*redacted*]@gmail[.]com from the web service NameCheap. NameCheap is a company that provides domain registration services. The email stated "your WhoisGuard subscription is expiring soon." The email further stated that the domain referenced was "downthem.org." Based upon my training and experience, I know that WhoisGuard is a privacy protection service that allows website operators to mask the true registration details for a given domain. I further know that details such as website registration and hosting are usually handled by one or more administrative figures. Thus, this exchange indicates that Ampnode and Downthem were connected services with a common administrator (GATREL).

b. In another example, on September 14, 2017, the email account ampnode[*redacted*]@gmail[.]com was used to exchange a series of emails with a customer using the email account "wane[*redacted*]@yahoo[.]com." The email exchange began with "wane zane" asking for help determining how much to charge DDoS customers. Ampnode[*redacted*]@gmail[.]com replied, "It's part of their plan on my stresser. And yes, I have customers who email me or open tickets saying it down'ed their nfo." Based upon my training and experience, I understand the user of the ampnode[*redacted*]@gmail[.]com account, believed to be GATREL, was saying that he has had customers inform him that his stresser service was sufficiently powerful to temporarily take down servers at NFO, a major hosting provider. Additionally, I understood this exchange to mean that "wane zane" was explicitly telling GATREL that he intended to use the Ampnode service for the purpose of operating his own DDoS service. "Wane zane" then replied, "ooh mike has a stresser so i can test it from your stresser then u will tell meh a price lol." Ampnode[*redacted*]@gmail[.]com (GATREL) replied, "sure but you'd need a trial login." "Wane zane" then responded, "where do I sing [sic] up at?" to which ampnode[*redacted*]@gmail[.]com responded, "downthem.org." This email exchange thus further demonstrates the connection between GATREL's two services, Ampnode and Downthem, and his connection to both.

c. Within the email account ampnode[*redacted*]@gmail[.]com, reviewing agents found tens of thousands of emails related to the operation of the Ampnode DDoS service. These emails included client inquiries, sales, trouble-shooting, and requests for "lists," as described above. For example, in one such exchange on July 15, 2017, an email was sent to ampnode[*redacted*]@gmail[.]com com by a customer who said, "hey looking to buy 3 new lists again for dns/ntp/chargen." In response, ampnode[*redacted*]@gmail[.]com sent an email stating "sure just did chargen and ntp yesterday." Based upon my training and experience, and as described above, I know that DNS, NTP, and CHARGEN are some of the most frequently abused Internet protocols when it comes to amplifying DDoS attacks. I am aware of few legitimate purposes for anyone to assemble and sell lists of servers which respond to those protocols, and I believe that the predominant usage for the exchange of such lists would be to facilitate the conduct of DDoS attacks. I also know that the purpose of assuring the customer that the lists were just created the previous day was because fresh lists are the most valuable for the purposes of conducting the largest DDoS attacks. That is because owners of the abused services often receive notification that their servers are being used to conduct attacks and may implement controls to prevent further abuse, as well as the fact that some servers may change IP addresses every few days. This would mean that over days and weeks, an "amp list" would likely become progressively less accurate, and therefore, less powerful. For those reasons, DDoS operators intending to conduct large attacks have to constantly renew their lists of vulnerable servers.

d. As another example, on July 29, 2017, ampnode[*redacted*]@gmail[.]com was sent an email by "Bob Squad" via oexotic[*redacted*]@gmail[.]com stating, "Most people are really after hitting nfo and ovh. And it can be done man. I've done it myself. Power is lovely on your site, and the zudp is sexy af I don't even need destination port to hit hotspots lol..im not use to it being that powerful. But! If you could get your hands on a tcp or udp method that can time out nfo or ovh servers for at least like 5-10ticks to lag them out a game..and i can put that in a thread...you would have people all over your site. I haven't tested all methods on site against an nfo or ovh yet, what methods would you think would down them[?]"

i. Based upon my training and experience, I believe that in this exchange, "Bob Squad" was telling GATREL that most customer demand was currently focused on DDoS services that were able to take down the hosts NFO and OVH, two very large international hosting companies. "Bob Squad" was encouraging GATREL to invest in TCP or UDP attack methods able to "time out" the NFO and OVH servers, and noted that in doing so, GATREL would attract many additional customers. This is especially relevant to certain types of online gameplay in which a loss of connectivity for "5-10 ticks," or 5-10 seconds, can mean ejection from a game, or such a competitive disadvantage that the victim is likely to lose whatever game they are playing. I know, based on my training and experience and interviews I have conducted with representatives from many online gaming platforms, that certain types of online games, especially multiplayer games, are very lucrative, with the operators of the online game making money from fees paid by the online players. DDoS attacks against players in these types of games is growing increasingly common, creating an even bigger market for criminal DDoS operators like GATREL.

e. A response was sent by ampnode[*redacted*]@gmail[.]com com to "Bob Squad" on the same date, stating, "trigemini 1 and 2, essyn and sometimes security methods work well on those hosts just need ports for those hosts."

i. Based upon my training and experience, I understand that in this exchange, GATREL was telling "Bob Squad" to try to use different attack methods against NFO and OVH, so long as "Bob Squad" was able to determine the proper ports. By this he would likely mean the given port that a specific victim was using or on which a gaming service was operating.

35. GATREL was confirmed as the user of the relevant emails a variety of ways, even prior to his statements during the FBI's interview (described below). For example, according to records obtained from Google, on June 12, 2018, an email was sent from ampnode[*redacted*]@gmail[.]com to "Matthew D" at another email that Google records connected to GATREL, tank[*redacted*]@gmail.com. The email contained an attached image of an Illinois driver's license in the name of Matthew D GATREL, including a residence address that located GATREL within a

Chicago, Illinois suburb. I have separately conducted public records checks and confirmed that this license and its accompanying address match GATREL's issued driver's license. That same date, a second email was sent from ampnode[*redacted*]@gmail[.]com to tank[*redacted*]@gmail[.]com containing an image of a utility statement for the same suburb. That utility statement was in the name of Matthew D GATREL, with a service address of another address in that same city. Thus, it appeared that GATREL was sending himself copies of these records from one account to another.[9]

E. Interview of GATREL and Search of His Computer

36. On November 19, 2018, I, along with other agents, interviewed GATREL at his residence. During the interview, GATREL agreed to allow agents to create an image of his computer, and also provided a copy of the databases for the Downthem and Ampnode services.

37. During the interview, GATREL confirmed that he was the current administrator of both Downthem and Ampnode, had been running Downthem since at least 2014, and had been operating Ampnode for approximately four to five years. GATREL also confirmed he was the user of each of the email accounts previously referenced within this affidavit as belonging to GATREL.

[9] Sending such identification documents is something I and other FBI agents have commonly observed in previous investigations and is usually due to those documents being required by various hosting companies in order to initiate or maintain service.

38. GATREL stated that he had a co-administrator to whom he was hoping to sell the Ampnode site. GATREL said that the person helping administer the Downthem server went by the username "Severon," and used the email address severon[*redacted*]@gmail[.]com. GATREL also stated that he had had a different co-administrator for Downthem approximately two years ago. During the interview, GATREL stated that he currently averaged between 2-3 customers at a time, and that the highest number of simultaneous customers enrolled to the Downthem service at one time was around 10.

39. GATREL said that he estimated that at least 50 percent of his Ampnode customers were likely running DDoS services using his infrastructure, especially as his network allowed spoofing. GATREL also stated that he was working with an individual and company in Romania to run the Ampnode network.

40. After the interview, I reviewed the database for GATREL's Downthem service. Based upon my training and experience, the database showed over 2000 customer subscriptions, and over 200,000 DDoS attacks conducted, or attempted to be conducted, between October 10, 2014 and my interview with GATREL. Almost 1,000 attacks were initiated by users from IP addresses in the Los Angeles area. The test attacks conducted by the FBI were correctly captured in the database, contributing to my assessment of its veracity. Other attacks reflected in the database include more than 2,000

attacks directed at IP addresses that geolocate[10] to the Los Angeles area, and substantially more than that within the Central District of California as a whole. Among the targeted victims were the following:

a. Over 65 universities, both within the United States and in other countries, including at least one university within the Central District of California;

b. Federal, state, and municipal government or utility targets;

c. Commercial/banking targets; and

d. Online gaming companies and online gaming servers.

41. Review of the database also corroborated GATREL's description of his co-administrator, "Severon." Beginning at least as early as June 2018, I observed messaging entries in which user "Severon" and GATREL discussed improvements to the Downthem service. Beginning in October 2018, I observed messaging entries in which user "Severon" responded to customer requests in an administrator capacity. In addition, it appears from the database that "Severon" conducted approximately 174 attacks using the Downthem service. For example, on or about November 10, 2018, user "Severon" conducted, or attempted to conduct, eight DDoS attacks. He was directing the attacks at two targets, both of which are large-scale server and cloud hosting companies.

[10] Geolocation tables can be slightly out of date, but based on my training and experience, most of these will be accurate.

F. Interview of MARTINEZ in Pasadena, California

42. Through use of public, commercial, and law enforcement database tools, I was able to determine that the nickname "Severon" was associated with the name "Juan Martinez." Further investigation of public records indicated that the relevant "Juan Martinez" resided at an address in Los Angeles County, California.

43. On December 17, 2018, Special Agent Joshua Rongitsch and I interviewed MARTINEZ at that address in Los Angeles County. MARTINEZ initially professed to not use DDoS services, but when asked specifically about Downthem, MARTINEZ admitted that he was helping to maintain the Downthem website. I then observed MARTINEZ use his computer to access the Cloudflare accounts for both Downthem and Ampnode, and I separately observed MARTINEZ navigate to the Downthem website. At the website, MARTINEZ had access to administrative fields and actions I had not observed in my testing of the website, indicating that MARTINEZ had administrator-level access to the site. For instance, the website stated that there were three tickets that needed to be answered.

44. At my request, MARTINEZ downloaded the database from the Downthem website and emailed it to me using the same email identified by GATREL for his co-administrator, severon[*redacted*]@gmail[.]com. I have evaluated the database that MARTINEZ provided and found it to be identical to the database provided by GATREL, except that it also contained more recent log entries which had been made between GATREL's

production of the database and MARTINEZ's production of the database.

45. I asked MARTINEZ about his own DDoS attacks using the Downthem server. MARTINEZ claimed that these attacks were test attacks against OVH servers that he controlled. I asked MARTINEZ if he had OVH's permission to conduct such an attack and he asked me if OVH even gave permission for such a thing. Based on my training and experience, I do not believe that OVH would in fact give permission for a user to conduct DDoS attacks against its servers.

VI. CONCLUSION

46. For all the reasons described above, there is probable cause to believe that GATREL and MARTINEZ have committed a violation of 18 U.S.C. § 371 (Conspiracy to Commit Unauthorized Impairment of a Protected Computer).

ELLIOTT PETERSON, Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before
me this 19th day of December,
2018.

HONORABLE MICHAEL R. WILNER
UNITED STATES MAGISTRATE JUDGE