

FILED

NOV 15 2018

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY *CM* DEP CLK

No. 5:18-cr-00461-BO

UNITED STATES OF AMERICA)	
)	
v.)	<u>CRIMINAL INFORMATION</u>
)	
SERGIY PETROVICH USATYUK, a/k/a)	
"Sergio Usatyuk," "Andy,")	
"Andrew Quez," "Andy Quez,")	
"Brian Martinez," "GIFTEDPVP,")	
and "GIFTEDPV.P")	
_____)	

The United States Attorney charges that:

Defendant and Co-Conspirator

1. Defendant SERGIY PETROVICH USATYUK a/k/a "Sergio Usatyuk", "Andrew Quez," "Andy Quez," "Andy," "Brian Martinez," "GIFTEDPVP," and "GIFTEDPV.P" (collectively "USATYUK"), is a citizen of the United States who last resided in Hollywood, Florida. USATYUK used and/or controlled the accounts giftedpvp@gmail.com and tabbdev@gmail.com. USATYUK was also the Chief Executive Officer (CEO) of OkServers LLC, which was incorporated in the State of Delaware.

2. Co-Conspirator A is a citizen of Canada, and last resided in Regina, Saskatchewan.

Relevant Terms and Definitions

3. A "distributed denial of service" or "DDoS" attack is a type of network attack in which the perpetrators use multiple Internet-enabled devices to overwhelm a target computer system of another person with unrequested traffic and, in turn, interfere with or disrupt the ability of a targeted computer system to respond to legitimate Internet traffic. A DDoS attack may cause a targeted computer system to be slowed down, rendered inaccessible to some or all legitimate users, or even prevented from communicating with the Internet.

4. "Booters" are a class of publicly-available, web-based services that can be used by any cybercriminal to launch unauthorized DDoS attack(s) against a target computer system for a relatively small fee or no fee at all. The services are termed "booters" because the DDoS attacks they launch often overwhelm the Internet connection of a targeted computer system, and thereby "boot" or "drop" the victim from the Internet. Booter services are known for their accessibility and affordability. To launch a DDoS attack using a booter, a cybercriminal often needs only a web browser and online payment tool to subscribe to a booter, provide attack instructions via a booter's website, and deliver payment.

5. A "server" is a computer that provides services to other computers. Examples include web servers that provide content to

web browsers, and e-mail servers that act as a post office to send and receive e-mail messages.

6. A "domain name" is a simple, easy-to-remember way to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular Internet Protocol ("IP") address.

7. Domain names may be purchased through a "registrar," which acts as the intermediary between the registry and the purchaser of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant."

Overview of the Scheme

8. Beginning from at least as early as August 2, 2015, and continuing until approximately November 30, 2017, USATYUK and Co-Conspirator A devised and executed a scheme to unlawfully enrich themselves from the ownership, administration and support of a number of booter services. As part of the scheme, USATYUK and Co-Conspirator A facilitated millions of illegal DDoS attacks against victim computer systems on behalf of paying and non-paying subscribers to booters that they owned, administered, or supported, including ExoStress.in ("ExoStresser"), QuezStresser.com ("QuezStresser"), Betabooter.com ("Betabooter"), Databooter.com ("Databooter"), Instabooter.com ("Instabooter"), Polystress.com ("Polystress"), Decafestresser, and Zstress.net ("Zstress") (collectively, "the Subject Booters"). As part of the

scheme, USATYUK and Co-Conspirator A also profited from administering and supporting booter-affiliated websites, such as Bestipstressers.com and Ipstressers.org (the "Subject Booter Websites") that promoted the Subject Booters and advertised other booter services (collectively, the "Subject Booter Services").

9. In furtherance of the scheme, USATYUK and Co-Conspirator A controlled and operated public-facing websites for the Subject Booters that cybercriminals used to subscribe to DDoS attack service plans, and input attack instructions against intended victims, including the victim's IP address and/or website Uniform Resource Locator ("URL"), the attack length, the number of servers supporting the attack, the volume of concurrent attacks, the type of attack, and the number of "boots" per day. USATYUK and Co-Conspirator A also developed and maintained source code for processing and routing the Subject Booters' attack orders through a network of servers that they controlled. These servers, in turn, typically launched the Subject Booters' DDoS attacks by spoofing the IP addresses of the intended victims in electronic messages to third-party, Internet-enabled devices (the "amplification servers") that were deceived into reflecting and amplifying junk traffic towards the intended victim without the knowledge and consent of the amplification servers' owners. The co-conspirators developed or obtained lists of amplification servers.

10. In just the first 13 months of the 27-month long conspiracy, the Subject Booters' users ordered approximately 3,829,812 DDoS attacks. As of September 12, 2017, ExoStresser advertised on its website (exostress.in) that its booter service alone had launched 1,367,610 DDoS attacks, and caused targets to suffer 109,186.4 hours of network downtime (~4,549 days).

11. During the conspiracy, the Subject Booters launched DDoS attacks that disrupted the internet connections of targeted victim computers, rendered targeted websites slow or inaccessible, interrupted normal business operations (and associated losses), and caused victims to incur remediation costs.

12. In or around July 2016, ExoStresser was one of a number of booters that cybercriminals used to repeatedly attack servers of a video game manufacturer that hosted a popular multi-player videogame. The attacks contributed to the video game manufacturer suffering an estimated \$164,000 loss from defending and remediating the harm caused by DDoS attacks against the game.

13. The Subject Booters' DDoS attacks also harmed computer systems that were not directly targeted. For example, in November 2016, a Betabooter subscriber launched a series of DDoS attacks against a school district in the Pittsburgh, Pennsylvania area that not only disrupted the school district's computer systems, but affected the computer systems of seventeen organizations that shared the same computer infrastructure, including other school

districts, the county government, the county's career and technology centers, and a Catholic Diocese in the area.

14. The Subject Booters' DDoS attacks additionally exploited third-party "amplification servers" without their owners' consent to reflect and amplify unauthorized web traffic against targets.

15. As a result of the scheme, USATYUK and Co-Conspirator A gained in excess of \$550,000.

Other Relevant Entities and Individuals

16. "Company A" was a domain name registrar headquartered in Los Angeles, California, that registered domain names.

17. "Company B" was a telecommunications service provider located in Buffalo, New York, that provided web, virtual private server (VPS), and dedicating hosting services.

18. "Company C" was a company headquartered in San Francisco, California, that provided DDoS mitigation services that obscured the true IP address of a customer's servers.

19. "Company D" was a cloud infrastructure provider located in New York, New York, that offered VPS and cloud hosting services.

20. "Company E" was a colocation datacenter company headquartered in New York, New York that operated facilities across the country. In its Chicago, Illinois datacenter, customers of Company A could rent space to operate servers and computing hardware.

21. "Company F" was a colocation datacenter company headquartered in San Francisco, California that, among other things, operated a number of datacenter facilities around the world. In its Romania facility, customers of Company F could rent space to operate servers and computing hardware.

22. "Payment Processor A" was a worldwide online payment system headquartered in San Jose, California that supported online money transfers.

23. "OkServers LLC" ("OkServers") was a limited liability corporation incorporated under the laws of Delaware that operated dedicated servers. USATYUK was the sole officer of OkServers.

24. HackForums.Net was an Internet forum that hackers frequently used to discuss security, technology, and general computing issues, including botnets and booters.

COUNT ONE

25. Paragraphs 1 through 24 are re-alleged and incorporated herein as though fully set forth in this count.

26. From on or about August 2, 2015, until approximately November 30, 2017, both dates being approximate and inclusive, in the Eastern District of North Carolina and elsewhere, USATYUK did knowingly and willfully combine, conspire, confederate, and agree with Co-Conspirator A to commit and aid and abet offenses against the United States in connection with the ownership, administration, and support of the Subject Booter Services, that

is: to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage, and attempted to cause damage, without authorization, to a protected computer, thus causing damage affecting 10 and more protected computers during any one-year period, and causing loss aggregating at least \$5,000 in value to one and more persons during any one-year period from a related course of conduct affecting one and more other protected computers, all in violation of 18 U.S.C. §§ 2, 1030(a)(5)(A), and (c)(4)(B).

OBJECT OF THE CONSPIRACY

27. It was an object of the conspiracy for USATYUK and Co-Conspirator A to develop, administer, perpetuate, control, support, and profit from booters, including the Subject Booters, that launched DDoS attacks on behalf of third-parties. A further object of the conspiracy was to administer and support booter-affiliated websites, such as the Subject Booter Websites, that promoted the Subject Booters and generated additional revenue from advertising other illegal booter services.

MANNER AND MEANS

Among the manner and means used to effect and accomplish the purpose of the conspiracy included, but were not limited to, the following:

28. It was a part of the conspiracy that USATYUK and Co-Conspirator A developed websites and software used by the Subject

Booters to receive, process, route, and launch DDoS attacks on behalf of users of the Subject Booters.

29. It was further a part of the conspiracy that USATYUK, Co-Conspirator A and others established, perpetuated, and controlled computer infrastructure used to launch DDoS attacks. The scheme included registering and maintaining domains used by the Subject Booters, creating and maintaining web hosting and colocation service accounts used by booters to process and launch DDoS attacks, purchasing and maintaining computers and servers used for the same, and opening and maintaining bank, payment processing, and cryptocurrency accounts needed to process and collect the payments of subscribers to the Subject Booters.

30. It was further a part of the conspiracy that USATYUK and Co-Conspirator A administered, managed and controlled the Subject Booters, including developing and maintaining the Subject Booters' websites, software, and computer infrastructure, advertising the Subject Booters on public forums, the Subject Booter Websites, and other booter-related websites, providing customer service to the Subject Booters' subscribers, communicating with third-parties who provided services to the Subject Booters, fielding and responding to abuse complaints, identifying third-party amplification servers to unwittingly participate in DDoS attacks, and facilitating the exchange of the Subject Booters' gains into Bitcoin.

31. It was further a part of the conspiracy that that USATYUK and Co-Conspirator A concealed their true identities and criminal activity by, among other things, administering the Subject Booters with online aliases, creating accounts with DDoS mitigation services that obscured the Subject Booters' true IP addresses, registering a domain and creating accounts with false information to obscure the source of money from Payment Processor A, and paying individuals to convert the gains of the conspiracy into Bitcoin at a rate of 15 or more percent of the original transfer amount.

32. It was further a part of the conspiracy that defendant USATYUK and Co-Conspirator A enriched themselves by charging the customers of the Subject Booters subscriber fees for facilitating illegal DDoS attacks.

33. It was further a part of the conspiracy that defendant USATYUK and Co-Conspirator A administered, maintained, and controlled the Subject Booter Websites to promote the Subject Booters, and enriched themselves by selling advertising space to other booter operators.

OVERT ACTS

In furtherance of the conspiracy, and to achieve the unlawful objects thereof, USATYUK and Co-Conspirator A committed and caused to be committed the following overt acts, among others, in the Eastern District of North Carolina and elsewhere:

Control of Computer and Networking Infrastructure Used By the
Subject Booter Services

34. As part of the conspiracy, USATYUK used the aliases "Andrew Quez" and "Brian Martinez" to register the following Subject Booters with Company A:

Subject Booter Service	Domain	Approximate Date of Registration	USATYUK Alias
ExoStresser	exostress.in	August 2, 2015	Andrew Quez
IP Stressers	ipstressers.org	September 2, 2015	Brian Martinez
IP Booters	ipbooters.com	September 15, 2015	Brian Martinez
Databooter	databooter.com	December 13, 2015	Brian Martinez
Instabooter	instabooter.com	April 3, 2016	Brian Martinez

35. In or around August 2015, USATYUK and Co-Conspirator A began hosting Subject Booters, including ExoStresser, on a self-managed dedicated hosting server at Company B that was used to receive, route, and launch DDoS attacks that were ordered by subscribers to the Subject Booters.

36. On or about August 2, 2015, USATYUK, using the alias GIFTEDPVP, registered the domain name "exostress.in" with Company C's free DDoS mitigation service.

37. On or about August 29, 2015, USATYUK, using the alias GIFTEDPV.P, registered a VPS account at Company D that was used to facilitate DDoS attacks ordered through the Subject Booters, and create spoof accounts with Payment Processor A that could receive subscriber payments.

38. On or about January 13, 2017, USATYUK registered a company in Delaware, OkServers LLC, through which he owned, administered, and maintained servers that were used to operate the Subject Booter Services, and facilitate DDoS attacks ordered by the Subject Booters' subscribers.

39. On or about July 16, 2017, USATYUK, as CEO of OkServers, leased a server closet from Company E's datacenter in Chicago, Illinois that housed servers used to facilitate DDoS attacks ordered through the Subject Booters.

40. On or about August 31, 2017, USATYUK, as CEO of OkServers, began hosting servers associated with facilitating the Subject Booters at Company F's datacenter in Bucharest, Romania.

Technical Administration of the Subject Booter Services

41. On or around August 13, 2015, Co-Conspirator A created a forum thread on the HackForums.Net Marketplace section for "Premium Sellers for Server Stress Testing" that advertised the results of ExoStresser's then-recent booter activity.

42. On or around August 24, 2015, USATYUK, using the administrator account alias "Andy," responded to a customer support ticket posted in ExoStresser's customer support system by stating "You can DDOS any IP you want, we don't care."

43. On or around December 9, 2015, USATYUK and Co-Conspirator A sold an ExoStresser DDoS attack plan to a user within the Eastern District of North Carolina who, in turn, launched

different types of DDoS attacks that exploited 699 amplification servers in the Eastern District of North Carolina.

44. On or around July 3, 2016, USATYUK logged into the VPS account at Company D from an IP address that resolved to one of USATYUK's former residences in Orland Park, Illinois.

45. On or around July 21, 2016, USATYUK used the IP address associated with the Orland Park Residence to simultaneously log into the ExoStresser website using the administrator account alias "Andy," and the Company B server that hosted the ExoStresser website.

46. On or around September 16, 2016, USATYUK and Co-Conspirator A used a chat platform to discuss changing the domain name exostress.in to exostresser.com.

47. On or around November 8, 2016, USATYUK and Co-Conspirator A used a chat platform to discuss the arrest of an individual in the United Kingdom who operated a booter service. During that conversation, USATYUK indicated that he planned to remove his personal logs to get rid of evidence, and warned Co-Conspirator A that "[i]f they get the DB [database] and see your name in the log fields they won't care about much else."

48. On or around December 17, 2016, USATYUK and Co-Conspirator A used a chat platform to discuss plans for increasing the strength of DDoS attacks launched by ExoStresser.

49. On or around February 18, 2017, USATYUK used a chat platform to request that Co-Conspirator A check on ExoStresser's operations, and answer customer support tickets.

50. On or around April 10, 2017, USATYUK logged into the VPS account with Company D from an IP address that resolved to USATYUK's former residence in Darien, Illinois.

51. On or around August 7, 2017, USATYUK installed servers at the Company E location in Chicago, Illinois that were used to facilitate DDoS attacks launched by the Subject Booters.

52. On or around September 10, 2017, USATYUK logged into the VPS account with Company D from an IP address resolving to USATYUK's current residence in Hollywood, Florida.

Financial Administration of the Subject Booter Services

53. On or around September 22, 2015, USATYUK used a chat platform to ask Co-Conspirator A to send \$205 from an account with Payment Processor A to tabbdev@gmail.com so that USATYUK could order another server. On or around the same day, USATYUK received a notification from Payment Processor A indicating that Co-Conspirator A had sent him \$205.

54. On or around October 17, 2015, Co-Conspirator A posted in a marketplace section of HackForums.Net entitled "Service Offerings for Currency Exchange" that he/she sought individuals to exchange revenue from Payment Processor A into Bitcoin at a conversion rate of 15%.

55. On or about February 12, 2016, USATYUK used the alias "Brian Martinez" to register a domain, irngur.org, that USATYUK and Co-Conspirator A used to reroute payments from ExoStresser's website (exostress.in) to Payment Processor A. The domain was created after Payment Processor A had stopped processing orders from ExoStresser's website, and designed to circumvent Payment Processing A's terms of use restrictions on processing transactions associated with DDoS attacks.

56. On or around February 21, 2016, USATYUK and Co-Conspirator A agreed over a chat platform to change the Bitcoin address used to receive payments on the ExoStresser website. USATYUK then logged into the server at Company B that hosted the ExoStresser website from an IP address that resolved to the Orland Park Residence, and notified Co-Conspirator A in the chat platform that the ExoStresser Bitcoin address had been updated.

57. On or around July 29, 2016, USATYUK used a chat platform to direct Co-Conspirator A to exchange money received from ExoStresser into Bitcoin, and to pay a bill for one of ExoStresser's web and cloud hosting providers.

58. On or around December 19, 2016, USATYUK and Co-Conspirator A used a chat platform to discuss exchanging money received via Payment Processor A into Bitcoin at a 75% conversion rate. In the same conversation, USATYUK and Co-Conspirator A also

discussed USATYUK taking over the infrastructure for using Payment Processor A to receive revenue for certain Subject Booters.

All in violation of Title 18, United States Code, Section 371.

FORFEITURE NOTICE

Upon conviction of the offense alleged in this Criminal Information, the defendant shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 1030(i) and 982(a)(2)(A), the defendant's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offense, and any property, real or personal, constituting or derived from, any proceeds that the defendant obtained, directly or indirectly, as a result of such offense.

The forfeitable property includes, but it not limited to, the following:

1. \$542,924 in United States currency, including approximately 10.74059929 Bitcoin, representing the gross proceeds of the offense alleged in this Criminal Information obtained by the defendant;

2. The following computers and electronic media, further representing the gross proceeds and instrumentalities of the offense alleged in this Criminal Information:

Electronic Media Seized By FBI Pursuant to Warrants	
Model/Description	Unique Identifier
Phanton 820 Desktop Computer	RM650

ASUS K501U Laptop	GBN0CX26K206479
Samsung Galaxy S9 Cell Phone	354645090161252 (IMEI)
Seagate Barracuda 4 Terabyte Drive	NA86LJ0
Samsung 500 GB Solid State Drive (SSD)	S21HNXAG845946J
Western Digital 1TB Hard Drive (HDD)	WMC150713958
Western Digital 1TB Hard Drive (HDD)	WCC6Y0VSVA9Y
Samsung 250GB Solid State Drive (SSD)	S3PZNF0JA384514
Dell PowerEdge R230	FC8CHH2
Dell PowerEdge R230	FC77HH2
Dell PowerEdge R430	497VMB2

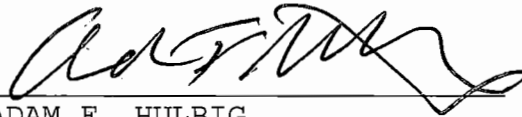
USATYUK's Servers At OkServers' Server Rack at Company E	
Dell PowerEdge R230 - 500GB HDD	FC86HH2
Dell PowerEdge R230 - 500GB HDD	FC75HH2
Dell PowerEdge R230 - 500GB HDD	FC78HH2
Dell PowerEdge R230 - 500GB HDD	FC79HH2
Dell PowerEdge R230 - 500GB HDD	FC76HH2
Dell PowerEdge R230 - 500GB HDD	FC95HH2
Dell PowerEdge R230 - 500GB HDD	FC88HH2
Dell PowerEdge R230 - 500GB HDD	FC8BHH2
Dell PowerEdge R230 - 500GB HDD	FC85HH2
Dell PowerEdge R230 - 500GB HDD	FC7CHH2
Dell PowerEdge R230 - 500GB HDD	FC89HH2
Dell PowerEdge R230 - 500GB HDD	FC7BHH2
Dell PowerEdge R230 - 500GB HDD	FC87HH2
Dell PowerEdge R230 - 480 SSD	CCWZZL2
Dell PowerEdge R230 - 480 SSD	CCWYZL2
Dell PowerEdge R230 - 480 SSD	CCWXZL2
Dell PowerEdge R430 - 480GB SSD	497TBM2
Dell PowerEdge R430 - 2x 240GB SSD	4970CM2

Additional USATYUK Servers Associated with OkServers	
Model/Description	Unique Identifier
HP ProLiant DL160 Gen9 servers - 2TB HDD	CZ263502DZ
HP ProLiant DL160 Gen9 servers - 2TB HDD	CZ263502F2
HP ProLiant DL160 Gen9 servers - 2TB HDD	CZ2704018H
HP ProLiant DL160 Gen9 servers - 1TB HDD	CZ2704018G
HP ProLiant DL160 Gen9 servers - 1TB HDD	CZ2704018D
HP ProLiant DL160 Gen9 servers - 1TB HDD	CZ2704018F
HP ProLiant DL20 Gen9 servers - 2TB HDD	CZ1706030K
HP ProLiant DL20 Gen9 servers - 2TB HDD	CZ1706030L
HP ProLiant DL20 Gen9 servers - 2TB HDD	CZ1706030E
HP ProLiant DL20 Gen9 servers - 2TB HDD	CZ1706030F
HP ProLiant DL20 Gen9 servers - 2TB HDD	CZ1706030G

HP ProLiant DL20 Gen9 servers - 2TB HDD	CZ1706030H
HP ProLiant DL20 Gen9 servers - 2TB HDD	CZ1706030J
Dell PowerEdge R230 - 2x 240GB SSD	7DGW7J2
Dell PowerEdge R230 - 2x 240GB SSD	3MMHZG2

If any of the above-described forfeitable property, as a result of any act or omission of the defendant, cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty, it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described above.

ROBERT J. HIGDON, JR.
United States Attorney



ADAM F. HULBIG
Assistant United States Attorney
Criminal Division

Aarash A. Haghigat
Trial Attorney
Criminal Division
Computer Crime and Intellectual
Property Section