IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, LLC, ML.CLOUD, LLC Defendants.	)	INDICTMENT 1:24 CR 00461 CASE NO._____ Title 18, United States Code, Sections 371, 1343, 1349, 1956 and 2 JUDGE BARKER

GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. MEDIALAND, LLC, (hereinafter "MEDIALAND"), was a business that provided infrastructure for servers and Internet services based in St. Petersburg, Russia. MEDIALAND, LLC was registered and owned by at least ALEXANDER ALEXANDROVICH VOLOSOVIK.

2. ML.CLOUD, LLC, (hereinafter "ML.CLOUD"), was a business that provided infrastructure for servers and Internet services based in St. Petersburg, Russia, and used the ML.CLOUD domain. ML.CLOUD was publicly owned by YULIA VLADIMIROVNA PANKOVA, a citizen of Russia.

3. ALEXANDER ALEXANDROVICH VOLOSOVIK, also known as Aleksandr Aleksandrovich, and the monikers Yalishanda, downlow, nishebrod and Ohyeahhellno, was a citizen of Russia and resided in St. Petersburg, Russia.

4. KIRILL ANDREEVICH ZATOLOKIN, also known under the monikers slim shady, g_host, podzemniy and podzemniy1, was a citizen of Russia and resided in St. Petersburg, Russia.

MEDIALAND'S INFRASTRUCTURE

5. MEDIALAND and ML.CLOUD controlled two Autonomous System Numbering (ASN, as defined below) blocks of IP addresses, ASN blocks 206728 and 215376, to host client services.

6. Since at least in or around June 2024, MEDIALAND and ML.CLOUD controlled these two ASN blocks on hardware physically located in Russia and the Netherlands, respectively.

7. ISP1 was an Internet Service Provider, as described below, that offered a variety of services to clients, administrative server space, and other types of infrastructure used by VOLOSOVIK, ZATOLOKIN, and other Client Conspirators who paid MEDIALAND, VOLOSOVIK, and ZATOLOKIN for access to MEDIALAND infrastructure to carry out criminal computer fraud schemes. ISP1 was located at a location known to the Grand Jury, in the United States and outside the Northern District of Ohio.

8. ISP2 was an Internet Service Provider, as described below, that offered a variety of services to clients, including Virtual Private Network services and other types of infrastructure used by VOLOSOVIK, ZATOLOKIN, and other Client Conspirators. ISP2 was located at a location known to the Grand Jury, in the United States and outside the Northern District of Ohio.

9. From on or about May 21, 2020, to on or about June 23, 2024, VOLOSOVIK, PANKOVA, and others, paid, or caused others to pay, approximately $2,100 to lease the space for the ffv2.ru server hosted by ISP1.

10. From on or about May 21, 2020, until on or about June 23, 2024, VOLOSOVIK, PANKOVA and others paid, or caused others to pay, over $23,000 in total to ISP1 for the lease of multiple servers from ISP1.

11. On June 24, 2024, the domain ffv2.ru was moved from an address leased by MEDIALAND and VOLOSOVIK to Russian-based IP Address 45.141.85.184 associated with MEDIALAND, which is under MEDIALAND's ASN 206728.

12. On or about June 2024, over 3,800 IP addresses were allocated to ASN 206728.

13. On or about July 2024, over 5,800 IP addresses were allocated to ASN 206728.

CLIENT CONSPIRATORS USING DEFENDANTS' CRIMINAL SERVICES

14. Client Conspirator 1, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 1 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and hosting, to carry out their extortionate fraud schemes.

15. Client Conspirator 2, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 2 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to sending ransomware payments from victims to cryptowallets owned and controlled by VOLOSOVIK, to carry out their extortionate fraud schemes.

16. Client Conspirator 3, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 3 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and hosting, to carry out their extortionate fraud schemes.

17. Client Conspirator 4, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 4 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and hosting on ffv2.ru, to carry out their extortionate fraud schemes.

18. Client Conspirator 5, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 5 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to sending ransomware payments from victims to cryptowallets owned and controlled by VOLOSOVIK and using MEDIALAND-owned infrastructure to carry out their extortionate fraud schemes.

19. Client Conspirator 6, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 6 used a specific malware or ransomware

variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and hosting on ffv2.ru, to carry out their extortionate fraud schemes.

20. Client Conspirator 7, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 7 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to hosting, to carry out their extortionate fraud schemes.

21. Client Conspirator 8, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 8 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration, use of IP addresses owned by MEDIALAND, and hosting on ffv2.ru, to carry out their extortionate fraud schemes.

22. Client Conspirator 9, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 9 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and use of IP addresses owned by MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

23. Client Conspirator 10, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 10 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and use of IP addresses owned by MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

24. Client Conspirator 11, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 11 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and use of IP addresses owned by MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

25. Client Conspirator 12, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 12 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and use of IP addresses owned by MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

26. Client Conspirator 13, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims

for money and cryptocurrency. Client Conspirator 13 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to false domain registration and use of IP addresses owned by MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

27. Client Conspirator 14, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 14 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including the use of IP addresses owned by MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

28. Client Conspirator 15, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 15 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to providing hosting from MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

29. Client Conspirator 16, known to the Grand Jury, was a group of individuals who infected victim computers with malware and ransomware variants and then extorted those victims for money and cryptocurrency. Client Conspirator 16 used a specific malware or ransomware variant, known to the Grand Jury, and relied on the services and infrastructure provided by

VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, including, but not limited to providing hosting from MEDIALAND during periods of malware and ransomware attacks, to carry out their extortionate fraud schemes.

30. Client Conspirator 17, unknown to the Grand Jury, infected or attempted to gain access to victim computers through brute force attacks. Client Conspirator 17 used and relied on the services and infrastructure provided by VOLOSOVIK, ZATOLOKIN, PANKOVA, MEDIALAND, and ML.CLOUD, including, but not limited to providing hosting from MEDIALAND and ML.CLOUD during periods of brute force attacks.

VICTIMS OF CLIENT CONSPIRATORS SUPPORTED BY DEFENDANTS

31. Victim 1, known to the Grand Jury, was a municipality located in Newton, Massachusetts.

32. Victim 2, known to the Grand Jury, was a commercial business located in North Grenville, Canada.

33. Victim 3, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Solon, Ohio. At times relevant to this indictment, Victim 3 also had servers located in the Northern District of Ohio.

34. Victim 4, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Medina, Ohio. At times relevant to this indictment, Victim 4 also had servers located in the Northern District of Ohio.

35. Victim 5, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Akron, Ohio. At times relevant to this indictment, Victim 5 also had servers located in the Northern District of Ohio.

36. Victim 6, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Brookfield, Ohio. At times relevant to this indictment, Victim 6 also had servers located in the Northern District of Ohio.

37. Victim 7, known to the Grand Jury, was a commercial business located in Murray, Utah.

38. Victim 8, known to the Grand Jury, was a commercial business located in New York, New York.

39. Victim 9, known to the Grand Jury, was a commercial business located in Menasha, Wisconsin.

40. Victim 10, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Findlay, Ohio.

41. Victim 11, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Cleveland, Ohio.

42. Victim 12, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Cleveland, Ohio.

43. Victim 13, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Elyria, Ohio.

44. Victim 14, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Valley View, Ohio.

45. Victim 15, known to the Grand Jury, was a commercial business located in Minneapolis, Minnesota.

46. Victim 16, known to the Grand Jury, was a commercial business located in Redditch, United Kingdom.

47. Victim 17, known to the Grand Jury, was a commercial business located in Elk River, Minnesota.

48. Victim 18, known to the Grand Jury, was a commercial business located in Waco, Texas.

49. Victim 19, known to the Grand Jury, was a commercial business located in San Mateo, California.

50. Victim 20, known to the Grand Jury, was a commercial business located in Salt Lake City, Utah.

51. Victim 21, known to the Grand Jury, was a commercial business located in Richmond, Virginia.

52. Victim 22, known to the Grand Jury, was a commercial business located in Cranberry Township, Pennsylvania.

53. Victim 23, known to the Grand Jury, was a commercial business located in Broussard, Louisiana.

54. Victim 24, known to the Grand Jury, was a commercial business located in Austin, Texas.

55. Victim 25, known to the Grand Jury, was a commercial business located in Atlanta, Georgia.

56. Victim 26, known to the Grand Jury, was a commercial business located in Blue Bell, Pennsylvania.

57. Victim 27, known to the Grand Jury, was a commercial business located in Doral, Florida.

58. Victim 28, known to the Grand Jury, was a commercial business located in Manchester, New Hampshire.

59. Victim 29, known to the Grand Jury, was a commercial business located in Troy, New York.

60. Victim 30, known to the Grand Jury, was a commercial business located in Peachtree City, Georgia.

61. Victim 31, known to the Grand Jury, was a commercial business located Nashville, Tennessee.

62. Victim 32, known to the Grand Jury, was a commercial business located Lynnfield, Massachusetts.

63. Victim 33, known to the Grand Jury, was a commercial business located in Seattle, Washington.

64. Victim 34, known to the Grand Jury, was a commercial business located in Winston-Salem, North Carolina.

65. Victim 35, known to the Grand Jury, was a commercial business located in Pittsburgh, Pennsylvania.

66. Victim 36, known to the Grand Jury, was a commercial business located in Minneapolis, Minnesota.

67. Victim 37, known to the Grand Jury, was a commercial business located in Troy, Michigan.

68. Victim 38, known to the Grand Jury, was a commercial business located Newark, Delaware.

69. Victim 39, known to the Grand Jury, was a commercial business located in Doraville, Georgia.

70. Victim 40, known to the Grand Jury, was a commercial business located Hunt Valley, Maryland.

71. Victim 41, known to the Grand Jury was a commercial business located in Sarasota, Florida.

72. Victim 42, known to the Grand Jury, was a commercial business located in Chicago, Illinois.

73. Victim 43, known to the Grand Jury, was a commercial business located Berwick, Louisiana.

74. Victim 44, known to the Grand Jury, was a commercial business located in the Northern District of Ohio in Canton, Ohio. At times relevant to this indictment, VICTIM 44 had servers located in the Northern District of Ohio.

RELEVANT COMPUTER AND INTERNET TERMS

75. "Autonomous System." Autonomous Systems (AS) were a large network or group of networks that had a unified routing policy. An AS was typically operated by larger organizations, network ISPs, universities, or government organizations. Each AS controlled its own IP address space, which was listed in the routing policy for that AS. For external communication between routers in different network groups, each AS was assigned a unique number, an Autonomous System Number (ASN), by the Internet Assigned Number Authority (IANA).

76. "Server." A server was a centralized computer that provided services for other computers connected to it via a network or the Internet. When a user accessed email, Internet web

pages, or accessed files stored on the network itself, those files are pulled electronically from the server, where they are stored, and were sent to the user's computer via the network or Internet. Notably, server computers can be physically located in any location; for example, it is not uncommon for a network's server to be located hundreds (or even thousands) of miles away from the user's computers. In larger networks, it was common for servers to be dedicated to a single task. For example, a server that was configured so that its sole task was to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail was known as a "mail server."

77. A "virtual private network" (VPN) was a technology that created a secure network connection over a public network such as the Internet or a private network owned by an Internet Service Provider. By using a VPN, a user could conceal his or her true IP address from those with whom he or she was communicating.

78. "Virtual Private Server." A virtual private server ("VPS") was a virtual server sold as a service by an ISP or Colocation Provider. A VPS ran its own copy of an operating system, such as Windows or Linux. Customers had full control over the entire VPS and had the ability to install almost any software that runs on the operating system. A VPS was functionally equivalent to having a physical server running at a colocation provider but allowed the colocation provider to cost-effectively manage and maximize use of their physical servers by virtualizing multiple systems on one piece of physical hardware.

79. "Internet." The Internet was a collection of computers and computer networks that were connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers existed across state and

international borders, and information sent between computers connected to the Internet may cross state and international borders, even if those computers were located in the same state.

80. "Domain name." A domain name was the familiar, easy-to-remember name used to identify computers on the Internet, for example, justice.gov. Domain names, like justice.gov, corresponded to one or more IP addresses. The Domain Name System (DNS) was a hierarchical naming system for computers connected to the Internet. It associated information with domain names. Most importantly, it translated domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often-used analogy to explain the DNS was that it served as the "phone book" for the Internet by translating human-friendly computer names into IP addresses.

81. "Internet Service Provider ("ISP")." An ISP was a commercial service that provided Internet connections for its subscribers. In addition to providing access to the Internet via telephone or other telecommunications lines, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP. ISPs maintained records pertaining to the individuals or companies that have subscriber accounts with them. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, and other information.

82. "IP address." The Internet Protocol address (IP address) was a unique numeric address used by computers on the Internet. An IP address might include a series of four numbers, each in the range of 0-255, separated by periods. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

83. "Log files." Log files were computer files containing information regarding the activities of computer users, processes/programs running on the system, and the activity of computer resources such as networks, modems, and printers. Log files can be used to identify activities that occurred on a specific computer.

84. "Port." In general terms, a port was a numeric value allowing a computer to uniquely identify different applications or processes running on a single computer over a single shared network connection. The port number worked in conjunction with the IP address. Analogizing to a standard postal mail example, when mailing a letter, the street address (IP address) may lead to an apartment building containing multiple units. But an apartment number (port) will further identify the particular apartment of the person to whom you are mailing the letter. In much the same way, a port number helped computers transmit information to the particular application intended on the IP address. Applications typically used a standard port number to simplify communication, but they could be set to use any allowed number. When sending information, the originating computer assigned a random originating port number so that the destination computer knew how to reach the originating computer. Following the foregoing apartment example, when sending a letter, the return address (IP address) would also contain an apartment number (port) in order for the recipient to send a reply letter back to your apartment. For computers, the return port was randomly picked, allowing the user to have multiple conversations without the computer mixing up the conversations.

85. "Proxy." A proxy was a network service for making indirect connections to other network services. A client computer connected to a proxy and instructed it to connect to another computer. The destination computer perceived an incoming connection from the proxy, not the

client computer. Like many network services, proxies had legitimate uses, but proxies were often used by cyber criminals to conceal their identity and location.

86. "Bot." A bot was a computer compromised by malicious software for use in completing malicious and/or illegal tasks via remote direction. Most users that had a computer acting as a bot were not aware that their computers were compromised. "Compromised computer" was a term synonymous with bot.

87. "Botnet." A large number of bots was called a "bot network" or "botnet." A botnet was typically controlled by one computer called a "command and control server."

88. "Administrative Panel." An administrative panel, or "admin panel," was a website or sub-section of a software platform that enabled administrators and other privileged users to monitor, edit, and control various aspects of the platform, including, but not limited to, creating, changing or deleting user access to the platform and changing internal configurations of the platform.

89. "Brute Force." A brute force attack consisted of a threat actor using large lists of potential passwords to gain access to a victim's account. This type of attack used trial and error, and as such, security software and devices were able to detect when one IP address made multiple attempts at logging on to a server or account. To circumvent this security measure, it was common for threat actors to cycle through IP addresses in order to obfuscate the source of the attempt to gain unauthorized access. Threat actors also spread out their login password attempts across minutes or hours to avoid flagging an account lockout.

90. "Command and Control Server." A "command and control server" was a centralized computer that issued commands to the bots in a botnet and received reports back from the bots. A "Command and Control" (C2) infrastructure consisted of servers and other technical

infrastructure used to control malware in general and, in particular, botnets. C2 servers could either be controlled directly by the malware operators or run on hardware compromised by malware. The owner of a command-and-control server directed a botnet to initiate a denial-of-service attack, send SPAM, operate as proxies (blindly forwarding Internet data), host phishing sites, or participate in other cyber-crime.

91. "Internet Hosting Service." An Internet Hosting Service was a company that ran servers connected to the Internet for the purpose of hosting, serving content, or other hosting services to an end-user or device. These other services could include hosting webpages, email servers, or file transfer services.

92. "Bullet Proof Hoster." Bullet Proof Hosters (BPH) were Internet Hosting Services resilient to complaints of illicit activity, allowing threat actors to engage in online criminal behavior. BPH providers were known in the cyber-criminal underground for selling Internet Hosting Services while taking steps to maintain access and availability for clients, regardless of the type of data being hosted or activity being conducted. BPH providers often ignored abuse reports, obfuscated the users of their services from identification or culpability, and rotated or otherwise disguised server resources to avoid detection and IP or domain "blacklisting." Whereas legitimate hosting service providers held clients responsible for terms-of-service violations (including using the service in support of criminal activity), shutting down services or closing accounts, BPH providers were far more lenient in this regard, and often knowingly permitted and/or supported illegal activity.

93. "Colocation Company." Colocation companies, such as Corporate Colocation, maintained server computers connected to the Internet. Their customers used those computers to operate servers on the Internet that, in turn, provided services to client computers. In some cases,

a subscriber or user communicated directly with a colocation company about issues relating to a website or account, such as technical problems, billing inquiries, or complaints from other users. Colocation companies typically retained records about such communications, including records of contacts between the user and the company's support services, as well as records of any actions taken by the company or user as a result of the communications.

94. "Crypto Currency." Crypto currency was a decentralized (meaning, not controlled by a centralized entity such as a bank), digital asset based on cryptography. The asset was typically tracked on a blockchain, which was a digital public ledger that recorded crypto currency transactions. The ledger built on the previous ledger, which was stored on a "block." This ensured that it could not be retroactively modified, because the blocks built on each other to form a chain that, in turn, was built upon the previously recorded transactions. Crypto currency was traded on the Internet and common examples were Bitcoin and Ethereum.

95. "Cryptowallet." A cryptowallet was a software program, physical device, and/or online service that stored the cryptographic key pairs of a crypto currency asset. The public key was provided to outside parties and was considered the wallet's address. Access to the private key allowed the owner to sign transactions for the wallet. Therefore, access to the private and public key of a crypto currency asset enabled ownership of the asset. The cryptowallet provided a convenient way to store the cryptographic key pair in a manner that could be easily accessed by the owner.

96. "Cyber-Criminal Forums." Cyber-criminal forums were online discussion boards, accessible through either the dark web or clear web, where individuals involved in illicit activities had a platform for collaboration, advertising, providing support, and even selling, trading, or

buying criminal tools such as malware. The forums played an important role in facilitating the growth and development of cyber-crime.

97. "Fast-flux." Fast-fluxing was a technique that involved associating multiple IP addresses with a single domain name, then changing out those IP addresses rapidly. Sometimes, hundreds or even thousands of IP addresses were used. Threat actors used fast-fluxing to keep their web properties up and running, hide the true origin of their malicious activity, and stop security teams of ISPs from blocking their IP address.

98. "Instant messaging." Instant messaging (IM) was a collection of technologies that created the possibility of real-time text-based communication between two or more participants via the Internet. Instant messaging allowed for the immediate transmission of communications, including immediate receipt of acknowledgment or reply. Jabber was a type of instant messaging software that provided a type of encrypted instant messaging.

99. "Malicious code/malware." Malicious code was a term used to describe any software code in any part of a software system or script that was intended to cause undesired effects, security breaches, or damage to a system. Malicious code described a broad category of system security terms that included attack scripts, viruses, worms, Trojan Horses, backdoors, and malicious active content. It was often installed on a victim computer system via the Internet through SPAM that contained attachments or through a web site where code was injected to automatically download onto a victim system when it was viewed through a web browser. When it was installed onto a victim computer system to perform malicious activity, it was often referred to as "malware."

100. A "trojan" was a type of malware that masqueraded as a routine download request or as an opportunity to download files of interest to the user to thereby persuade the victim to

install it unwittingly. Many trojans acted as an unauthorized access point to the victim computer that allowed an unauthorized computer to access and communicate with the infected computer.

101. "Hypertext Transfer Protocol" (HTTP) was the protocol used to transfer data over the Internet. The primary function of HTTP was to establish a connection between computers and servers on the Internet to transfer information, including web pages and downloadable files, from Internet-connected servers to computers using Internet browsers.

102. "Web injects" introduced or injected malicious computer code into a victim's web browser while the victim browsed the Internet and "hijacked" the victim's Internet session. Different injects were used for different purposes. Some web injects were used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which was then captured by the individual employing the web inject.

103. "Phishing" was a criminal scheme in which the perpetrators used mass email messages and/or fake websites to trick a victim into providing information, such as network credentials (e.g., usernames and passwords), that could later be used to gain access to the victim's systems. Phishing schemes often used social engineering techniques, similar to traditional con-artist techniques, to trick a victim into believing he or she was providing his or her information to a trusted vendor, customer, or other acquaintance. Phishing emails were also used to trick a victim into clicking on documents or links that contained malicious software that then infected and compromised the victim's computer system without his or her knowledge or permission.

104. "Anti-Virus Programs and Software" was software that scanned a computer's files and memory for indications of malicious software, such as viruses, malware, spyware, trojans, and similar intrusive computer programs designed to steal information or disable functionality. Anti-Virus Software operated by looking for patterns based on signatures or definition files pre-loaded

into the software. The software then ran scans and actively monitored changes in the computers files and memory that would indicate an infection from malicious software.

105. "Counter Anti-Virus" services checked malware against anti-virus software to determine if the malware would be detected by the anti-virus software. Counter Anti-Virus services did not share and distribute uploaded malware files with anti-virus companies, but instead provided anonymity to malware developers and users.

106. Unsolicited "SPAM" consisted of commercial electronic mail messages sent in bulk to recipients without prior request or approval. Individuals responsible for sending or causing the distribution of SPAM were referred to as "spammers."

107. "Ransomware." Ransomware was a type of malware that prevented or limited users from accessing their own systems. This type of malware forced its victims to pay the ransom through certain online payment methods to grant access to their systems, or to get their data back. Some ransomware encrypted files so that they could not be read without a key to decrypt the files.

THE USE OF MEDIALAND FOR BULLETPROOF HOSTING, DOMAIN REGISTRATION AND FAST-FLUX SERVICE

108. In addition to providing legitimate webhosting and Internet infrastructure services through the ML.CLOUD domain, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, and MEDIALAND also operated a separate service that provided Bullet Proof Hosting (BPH), domain registration, and fast-flux services for clients on servers separate from the public-facing servers of MEDIALAND.

109. As early as on or about June 14, 2016, cryptocurrency wallets controlled and maintained by VOLOSOVIK and ZATOLOKIN, for the support of MEDIALAND infrastructure, received transfers of cryptocurrency from accounts containing funds obtained through ransomware

payments made by victims who were exploited by ransomware attacks launched by Client Conspirators known and unknown by the Grand Jury. These services were also used to launch brute force attacks on victims that caused harm to victims' networks.

110. Since at least on or about August 17, 2016, VOLOSOVIK and ZATOLOKIN used the monikers Yalishanda, downlow, podzemniy1, Ohyeahhellno, Slim Shady and others to advertise MEDIALAND's BPH and fast-flux services while engaged in discussions of criminal schemes with Client Conspirators on various online criminal forums.

111. These forums included Exploit, XSS, Dark Money and Antichat, which were used to discuss, advertise, and promote criminal cyber activities.

112. Beginning as early as August 17, 2016, and continuing through the time of the Indictment, VOLOSOVIK and ZATOLOKIN offered and maintained the BPH, domain registration and fast-flux services to clients conducting ransomware attacks, malware scams and other criminal computer frauds.

113. Initially, Client Conspirators, known and unknown to the Grand Jury, who used the services provided by VOLOSOVIK and ZATOLOKIN, used MEDIALAND infrastructure that was separated from infrastructure used by non-criminal clients using ML.CLOUD domains.

114. After moving MEDIALAND infrastructure to Russia, Client Conspirators used both MEDIALAND and ML.CLOUD infrastructure to conduct criminal computer frauds.

115. Non-criminal clients using ML.CLOUD infrastructure were not able to access the criminal infrastructure on MEDIALAND maintained by VOLOSOVIK and ZATOLOKIN.

116. To provide the BPH infrastructure on which cyber criminals operated, MEDIALAND, VOLOSOVIK, and ZATOLOKIN took advantage of common Internet tools such as emails, domains, IP addresses, financial accounts, cryptocurrency, and communication servers.

117. A domain name server, hosted at an ISP, known as ISP1, located in the United States, was used by VOLOSOVIK and ZATOLOKIN for MEDIALAND'S illicit BPH, domain registration, and fast-flux services. This server was paid for in part by VOLOSOVIK and PANKOVA.

118. The server was hosted on ISP1 and located at Internet Protocol (IP) address 104.194.11.236 and linked to the domain ffv2.ru.

119. Until on or about June 23, 2024, the ffv2.ru server was physically located in New Jersey in the United States, and at all times relevant to the Indictment, was actively engaged in supporting BPH, domain registration, and fast-flux services that were crucial to the deployment and cloaking of ransomware from detection. During this time, the server was not itself deploying or exploiting malware or malicious code or storing stolen credentials or personal victim information.

120. From on or about June 23, 2024, until the date of the Indictment, VOLOSOVIK and ZATOLOKIN migrated the ffv2.ru domain hosted at the ISP1 server associated with IP Address 104.194.11.236 to a new server located in Russia within the MEDIALAND infrastructure.

121. In addition to the ffv2.ru server, MEDIALAND, VOLOSOVIK, and ZATOLOKIN operated infrastructure used in the same or similar manner by Client Conspirators known and unknown by the Grand Jury. This infrastructure included domains and servers identified as ffpanel.ru, ffpanel.top, sshvps.net, and abushost.ru.

122. During all times relevant to the Indictment, Client Conspirators engaged exclusively with MEDIALAND in the support of malware and ransomware to avoid its detection by anti-virus or security software.

123. By selling services like BPH, domain registration, and fast-flux services, VOLOSOVIK and ZATOLOKIN created a heightened degree of anonymity and resiliency against law enforcement actions and takedowns for their clients by providing the following: (1) fraudulent abuse report responses to satisfy suspicious activity reports from victims being attacked by malware; (2) rapid rotation of IP Addresses for domain names in an effort to hide malicious activity from defensive measures; (3) domain registration services via the BPH front company, with added private services to further obfuscate the true domain owner; and (4) other protections that shielded criminal clients from detection during network intrusions, infiltrations, and exfiltrations.

124. One of the services that VOLOSOVIK, ZATOLOKIN and MEDIALAND provided was to allow clients to register multiple domain names that would appear, falsely, to be non-offending domains. These domain names were rotated across a pool of IP Addresses, as needed, in an attempt to avoid detection by security software and further anonymize or obscure the malicious nature of the domains. VOLOSOVIK and ZATOLOKIN used multiple seemingly legitimate email accounts to register these domains, including, but not limited to, medialand.regru@gmail.com, medialand.webnic@gmail.com, alex.kitai@gmail.com, and der_fan@mail.ru.

125. The BPH service that VOLOSOVIK and ZATOLOKIN provided gave Client Conspirators access to panels that were, among other things, configured to funnel abuse reports, intrusion alerts, and other data generated by anti-virus software to the email accounts that VOLOSOVIK and ZATOLOKIN controlled and that were housed on infrastructure paid for, in part, by PANKOVA and MEDIALAND. Those email accounts included medialand[.]regru@gmail[.]com, medialand[.]webnic@gmail[.]com, alex[.]kitai@gmail[.]com, and abuse@sshvps[.]net.

126. Instead of responding to these abuse reports, alerts, and complaints, VOLOSOVIK and ZATOLOKIN took actions to anonymize and obscure the identities of the Client Conspirators or provided fraudulent responses that gave the appearance of addressing the reports in a manner appearing to be consistent with legitimate web hosting services when, in fact, they were not addressing those reports.

127. In addition to registering domains on behalf of their clients, MEDIALAND, VOLOSOVIK, and ZATOLOKIN accepted payments in the form of cryptocurrency in an effort to maintain their clients' anonymity.

128. Unless otherwise noted, communications of Defendants and other Client Conspirators set forth in this Indictment that were not originally in English were translated from Russian to English.

COUNT 1
(Conspiracy to Commit and Aid and Abet Computer Fraud, 18 U.S.C. § 371 and 2)

The Grand Jury charges:

129. Paragraphs 1 through 128 of this Indictment are hereby realleged and incorporated by reference as if fully set forth herein.

The Conspiracy

130. From on or about March 17, 2014, through the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, and ML.CLOUD, and others known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate, and agree to (1) violate the laws of the United States, and (2) aid and abet others known and unknown to the Grand Jury in violating the laws of the United States, namely:

a. to intentionally access a computer without authorization and thereby obtain information from a protected computer, which offense was committed for purposes of commercial advantage and private financial gain, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(i);

b. to intentionally and with intent to defraud access a computer without authorization, and by means of such conduct further the intended fraud and obtain something of value, specifically, money, in excess of $5,000, in a one-year period, in violation of 18 U.S.C. §§ 1030(a)(4) and 1030(c)(3)(A);

c. to knowingly cause the transmission of a program, information, code, and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, which offense caused loss to one or more persons during a one-year period aggregating at least $5,000, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B);

d. to knowingly cause the transmission of a program, information, code, and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, which offense caused damage affecting ten or more protected computers during a one-year period, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B);

e. with intent to extort from a person money and other things of value, to transmit in interstate and foreign commerce a communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer

without authorization, in violation of 18 U.S.C. §§ 1030(a)(7)(B) and 1030(c)(3)(A);

f. with intent to extort from a person money and other things of value, to transmit in interstate and foreign commerce a communication containing a demand and request for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. §§ 1030(a)(7)(C) and 1030(c)(3)(A); and

g. aid and abet others to commit these crimes, in violation of 18 U.S.C. § 2.

Objects of the Conspiracy

131. The objects of the conspiracy were to:

a. enrich the Defendants by advertising, maintaining, and leasing infrastructure services to criminal malware and ransomware actors that supported and aided and abetted the launch and execution of criminal cyber schemes;

b. provide Client Conspirators with BPH infrastructure and fast-flux domain hosting that supported and aided and abetted malware and ransomware schemes that illegally obtained victim funds through extortion and similar means; and

c. avoid detection and conceal the existence of the conspiracy.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

132. MEDIALAND and PANKOVA used ML.CLOUD to provide infrastructure that appeared to be a legitimate ISP to provide cover for the illegal domain and infrastructure support for clients managed by VOLOSOVIK and ZATOLOKIN.

133. MEDIALAND and PANKOVA provided financial support to VOLOSOVIK and ZATOLOKIN by allowing VOLOSOVIK and ZATOLOKIN to use financial accounts and credit cards in the name of MEDIALAND to pay for infrastructure used for illicit purposes.

134. VOLOSOVIK and ZATOLOKIN promoted "Bullet Proof Hosting" and Fast-flux services through MEDIALAND on forums that catered to individuals and groups engaged in ransomware and malware schemes.

135. VOLOSOVIK and ZATOLOKIN then provided those Client Conspirators (1) space on servers owned by or leased to MEDIALAND and (2) access to admin panels controlled and managed by VOLOSOVIK and ZATOLOKIN.

136. VOLOSOVIK and ZATOLOKIN maintained these backend database tables to manage approximately 389 unique usernames belonging to MEDIALAND Client Conspirators 1, 3-8, and 14, who used the fast-flux service hosted on the ffv2.ru server.

137. VOLOSOVIK and ZATOLOKIN used allegedly legitimate and independent email addresses and domains actually controlled by VOLOSOVIK and ZATOLOKIN to accept and reply to abuse reports and other alerts generated by victims and security software of computers victimized by client malware and ransomware.

138. VOLOSOVIK and ZATOLOKIN received abuse reports and other alerts but did not suspend offending domains or client accounts; instead, VOLOSOVIK and ZATOLOKIN provided false or fraudulent replies, ignored reports, and offered clients fast-flux services to further circumvent security procedures.

139. VOLOSOVIK and ZATOLOKIN continued to lease access to servers to malicious Client Conspirators and accepted payment for those hosting services directly from cryptocurrency accounts that contained funds obtained from illicit ransomware and malware schemes.

140. To achieve the objects of this conspiracy, VOLOSOVIK, ZATOLOKIN, PANKOVA, MEDIALAND, and ML.CLOUD, and other Client Conspirators relied on several manners and means to evade detection by both victims and law enforcement. These efforts included, but were not limited to, the following:

a. using credit cards, financial accounts, and credentials associated with accounts of MEDIALAND, VOLOSOVIK, PANKOVA, and others to pay for servers, domains, VPNs, and other infrastructure;

b. using crypto currency transactions to receive payments from Client Conspirators in a manner that made it difficult for law enforcement to track and provide attribution of the account owners;

c. using multiple servers and VPN services to create the illusion of legitimate abuse reporting procedures to anonymize the ultimate identities of clients;

d. communicating over encrypted private messaging servers;

e. using different monikers when communicating over different encrypted communication channels;

f. regularly moving infrastructure and changing communication channels; and

g. using U.S.-based and foreign servers.

141. To achieve the objects of the conspiracy, VOLOSOVIK, ZATOLOKIN, PANKOVA, MEDIALAND, and ML.CLOUD further aided and abetted Client Conspirators 1 through 17 by providing infrastructure that lead to the theft, extortion, and collection of over $62 million dollars from Victims 1 through 44 through schemes to defraud.

Overt Acts

142. In furtherance of the conspiracy and to effect the objects thereof, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, and ML.CLOUD, and others known and unknown to the Grand Jury, did commit and cause to be committed the following overt acts in the Northern District of Ohio, Eastern Division, and elsewhere.

MARKETING AND ADVERTISING OF ILLICIT HOSTING SERVICES

143. On or about August 17, 2016, VOLOSOVIK and ZATOLOKIN, using the moniker *podzemniy,* posted the following on the criminal forum Dark Money:

> Post ID 760355:
>
> > Hello! We are glad to offer you BP hosting services. We keep any projects. All except child porn. Our services: *- Hosting; *- VPS/VDS; *- Dedicated servers *- FastFlux (not on bots) open all ports, no problems with ssl; *- Domain registration; *- Server administration; Only here: *- Own DC, with server / VPS give access to reboot panel. KVM on request. *- Implemented a unique system that is not on the market. FastFlux with very complex logic, FastFlux on the legs, not on the bots, no packet loss and a failure in speed. Your project is always available. You do not lose your traffic accordingly logs; *- Self-signed certificates are generated on the fly. You can download your static SSL certificates, or use auto-generation. *- Only your bots are in the IP stat. *- Free basic server configuration for your purposes; *- Clean IP is always available; *- Servers and VPS with instant activation. Our service is for serious people who need server stability and availability for years!!!! You'll forget about hosting problems! Prices, you will be pleasantly surprised. Rates: 1 domain in FastFlux - 70wmz 5 domains in FastFlux - 200wmz + Free VPS (2000mhz/1gb/50gb) 10 domains in FastFlux - 300wmz + Free VPS (2000mhz/1gb/50gb) Unlimited domains in the FastFlux panel - 500wmz + Free VPS (2000mhz/1gb/50gb) *Panel function: 1. Add/Remove domains. (without Sapport). 2. Add/Remove DNS. (without Sapport). 3. Register your domains through our Domain Registration Panel. (without Sapport). 4. You manage your own SSL certificates. (without Sapport). 5. Any domain settings at the DNS level (without the help of the server). 6. Setting up domains on any port (without the participation of the port). 7. For those who have the system running on haproxy, a projection of your config (without the participation of the sappport). Contacts for ordering services: -*Jabber: [email]nishebrod@abushost.ru[/email]

144. On or about October 11, 2017, VOLOSOVIK and ZATOLOKIN posted the following on the criminal forum Dark Money: "Post ID 1024784: We are looking for new clients!"

145. On or about November 8, 2017, VOLOSOVIK and ZATOLOKIN used WhatsApp to discuss with each other the Dark Money forum interactions with several malware clients, stating "Half of my panel is in red, nobody answers. If they won't wake up, we will have maybe 5 to 7 clients left. We need to get new ones, start advertising on forums like 'Dark Money.'"

146. On or about December 17, 2018, VOLOSOVIK, using the moniker *Yalishanda,* posted on Exploit titled "[СЕРВИС] Революционный FastFlux! Абузоустойчивый хостинг" (translated: "Leading-edge FastFlux! Bulletproof hosting") the following post:

> Ladies and Gentlemen! We are glad to present to your attention a brand new FastFlux panel, from the old hosters who have had time to prove themselves from the best side. In this panel, we took into all the wishes of our customers and our resellers. All wishes have been realized. We rewrote the entire panel from the start, making our own proxy server and abandoning nginx/haproxy and other standard web-proxy servers, and also focused on the privacy and security of our clients.
> Benefits aimed at privacy/security:
> * We have completely written our own personal proxy server, which is installed in the encrypted container on the node. This container works before the first reboot of the node, after rebooting, access to it is lost even from us, which in turn completely excludes the possibility of the data center administrators to look at the config and determine the real ip-address of your server (backend). For this we use only KVM and XEN virtualization. No OpenVZ and etc.
> * In addition, our proxy server creates a lot of fake connections to different ip-addresses with the same packet size as on your server (backend). Thus, it is the most difficult task for administrators to determine your real ip address during sniffing.
> * It makes no sense to write that all traffic is encrypted, because it is done a priori, in default.
> Functional:
> * Add/remove domains/subdomains without the participation of support. Adding domains and updating dns occurs in 1-3 seconds. After the domain is added to the panel, it starts working instantly, no more waiting!
> * Manage dns records such as MX/XT/CNAME, etc. directly from the panel, without the participation of the support.

* Three non-killed public dns + personal FastFlux dns, which you manage yourself, without the participation of a support. In addition, FastFlux dns has the function of automatically replacing NS servers when a domain is locked. This function works without any support, everything is done automatically, which increases uptime and guarantees less gray hair on the client's head. Once a minute, our checker automatically checks your domain (where NS are raised) for blocking, if the domain is blocked, the system replace the NS server (on your working domain) with a working one. This ensures 99% availability of your projects.
* http/http2/https - the Hello SSL function is implemented. From now on, you no longer need to add SSL certificates to our panel; it is enough to add a certificate to your server.
* Implemented a magic button for changing the proxy server. If for some reason you are not satisfied with the ip of the current node (hit the blacklist, slow speed), you can change it in one click, without the participation of the support.
* Each client is allocated its own pool of ip-addresses, which in no way intersect with other clients. This guarantees the maximum time of the purity of the ip-address, before a possible hit in the blacklist. If ip hit the blacklist, then it is only your fault and not the fault of your neighbor.
* Managing incoming and outgoing ports, you specify which ports you need to open, which one to which forward traffic to do by yourself, without participation of support.
* Unlimited backends (IP adding/removing). Without participation of support.
* Support for all known crypto domains, such as .bit and others - for free!
* Three domain registrars (Europe, China and Malaysia). These registrars are positioned on the forum as bulletproof, but we call them loyal. Registration is implemented both in one domain and list (bunch). After registration, you can manage your domains, change NS servers and more. In addition, a random name generator has been implemented for bulk domain registration. Domain registration is done without the participation of the support.
* Added an additional function in the form of a checker for domains on blacklists and blocks, without the participation of a support. In addition, our jabber and telegram bot will tell you if a domain hit the blacklist or block so that you can respond as quickly as possible and replace the domain with a new one.
* Purchase of SSL certificates in one click, directly in the panel, without the participation of the support.
* Purchase of vps and dedicated servers, without the participation of support. (servers only for use with FastFlux), servers are "white".
* Automatic recharge through BTC/ETH, without the participation of support. Please note that our service is made for people who value their time and nerves. We offer quality service focusing on serious people who are ready for long-term cooperation. Using our service - you will forget about the problems with hosting and can concentrate all your strength only on the realization of your ideas and ideas.

We practically created for you the "MONEY" button. If you are looking for a cheap low quality service, we recommend paying attention to neighbored topics. Thanks.
Tariffs
1 domain in FastFlux panel – 150$
5 domains in FastFlux panel – 250$
10 domains in FastFlux panel – 350$
Unlimited domains in FastFlux panel – 500$

Our Contacts:
Jabber: billing – billing@abushost.ru
Jabber: billing2 (RU/ENG/CH) – billing2@abuhost.ru
Jabber: Support (RU/ENG/CH) – nishebrod@abushost.ru
Jabber: Support2 (RU) – support@abushost.ru
Telegram: Support/Billing (RU/ENG/CH) @ohyeahhellno

147. On or about December 18, 2018, VOLOSOVIK, using the moniker downlow, edited a post originally made on November 12, 2012, on the Antichat criminal forum, which was identical to the post in paragraph 149.

148. On June 24, 2019, using the moniker Yalishanda, VOLOSOVIK posted in English and Russian languages on cybercriminal forum Fog.ug:

Bulletproof hosting. Unique FastFlux.
We are glad to offer you services BP hosting. Keeping any project. All except child porn.
Our services:

Hosting;
VPS/VDS;
Dedicated server;
FastFlux (not bots) are open all ports, no problem with ssl, support .bit domains;
Domain registration;
Administration of servers;

Only here:
-Own DC, with a server/VPS give access to reboot panel. KVM on request.
-Implemented a unique system that is not on the market. FastFlux with very complex logic, FasFlux on nodes, not bots, no packet loss and the failure of the speed. Always available to your project. You do not lose your traffic and logs respectively;

-Implemented functionality of generating self-signature certificates on the fly. You can upload your static SSL certificates, or use auto-generation;
-In statistics only your bots IP;
-Free basic setup of servers for your purposes;
-Always available pure IP;
-Servers and VPS with instant activation.
-support.bit domain.
- not die DNS

Our service is for serious people who need the stability and availability of the server for years!!!!
You will forget about the problem with hosting!
Prices will pleasantly surprise you.
Tariffs: 5 domains in FastFlux panel – 200wmz+Free VPS (2000mhz/1gb/50gb), 10 domains in FastFlux panel – 300wmz+Free VPS (2000mhz/1gb/50gb), Unlimited domains in FastFlux panel – 500 wmz+Free VPS (2000mhz/1gb/50gb).
If you need support .bit domains+100$ to the tariff.
Functional Panel:
1. Adding/Deleting Domain (Without support intervention).
2. Add/Deleting DNS. (Without support intervention).
3. Domain registration through our panel. (Without support intervention)
4. You manage your SSL certificates by yourself. (Without support intervention).
5. Any adjustments to the DNS-level domains. (Without support intervention).
6. Configuring domains to any port. (Without support intervention).
7. For botnet users who runs system on haproxy forwarding your config. (Without support intervention)
Contacts: Jabber: nishebrod@abushost.ru

149. On October 12, 2023, Yalishanda posted the following on the criminal forum Exploit.in, with an updated edit made on or about March 23, 2024, under the topic "Socks5/https proxy service for brute force and various checkers, also ipv6 with open port 25":

a."We present a new service from Yalishanda!!! Server proxies! Our proxies do not die, they work at speeds of 100-100mb/s, the number of threads is unlimited, the pool is updated once a day! Proxies are suitable for brute/check.

Currently there is 2 tariff available:

1. 5000ips US/EU number streams unlimited $200

2. several billion IPV6 with open port 25, access to proxy via ipv4 $500"

150. On November 13, 2023, Yalishanda posted this same advertisement on the criminal forum XSS.IS.

PROVIDING INFRASTRUCTURE FOR CLIENT CONSPIRATORS

151. On or about May 21, 2020, VOLOSOVIK and ZATOLOKIN maintained the domain ffv2.ru, which at the time resolved to IP Address 104.194.11.236, hosted on a server leased from ISP1.

152. On or about May 21, 2020, VOLOSOVIK used client number 18394 with ISP1.

153. On or about May 21, 2020, VOLOSOVIK created email account 18394_alex@sshvps.net to manage the account with ISP1.

154. On or about May 21, 2020, VOLOSOVIK provided email addresses and made payments to ISP1 from email accounts of alex@sshvps.net and zakaz@sshvps.net.

155. On or about May 21, 2020, ZATOLOTKIN set up an account on ISP2 using the account der_fan@mail.ru.

156. From on or about May 21, 2020, VOLOSOVIK registered the domain sshvps.net and provided MEDIALAND as the administrator organization.

157. On or about May 21, 2020, VOLOSOVIK and ZATOLOKIN used the email address abuse@sshvps.net to receive abuse reports filed by security and anti-virus software alerting sshvps.net of port scan attacks, phishing, and other malicious activity for domains and IP addresses registered to MEDIALAND or MEDIALAND-associated accounts used by Client Coconspirators.

158. On or about May 21, 2020, VOLOSOVIK also used the email account alex.kitai@gmail.com to receive copies of the abuse report emails sent to abuse@sshvps.net.

159. On or about May 21, 2020, VOLOSOVIK and ZATOLOKIN configured the ffv2.ru server's configuration settings for the ffpanel web application or "admin panel" running on the server including database connections, ffv2.ru site settings, third-party service settings, and various credentials to be used by, and to aid and abet, Client Conspirators.

160. Beginning on or about May 21, 2020, VOLOSOVIK and ZATOLOKIN maintained, on the ffv2.ru server, a backend database named "ffpanel' containing approximately 41 database tables that stored detailed records of Client Conspirator activities on the web panel hosted at the ffv2.ru domain, which included records of registered users, domains, domain name service accounts, records and credentials, and cost for services, cryptocurrency transactions and other records.

161. On or about May 21, 2020, VOLOSOVIK and ZATOLOKIN also maintained accounts for Client Conspirators 1, 3-6, and 8, and those unnamed Client Conspirators in databases on MEDIALAND's ffv2.ru infrastructure that contained user IDs, logins, passwords, domain names, domain IP addresses, user contact information, user access logs, and over 5,000 unique registered domains that were registered through domain-name-registration services.

162. On June 24, 2024, VOLOSOVIK and ZATOLOKIN moved the domain ffv2.ru from IP address 104.194.11.236 to the Russian based IP Address 45.141.85.184 associated with MEDIALAND, under the MEDIALAND's ASN 206728 and with the abuse contact listed as abuse@sshvps.net.

163. On or about October 24, 2024, VOLOSOVIK, ZATOLOKIN, and PANKOVA maintained MEDIALAND IP addresses from ASN 206728 and ML.CLOUD IP addresses from

ASN215376 that were used to aid, abet and support a brute force attack on the systems of Victim 44.

MEDIALAND INFRASTRUCTURE TO SUPPORT AND AID MALWARE ATTACKS AND INFECTIONS BY CLIENT CONSPIRATORS

164. Beginning on or about February 24, 2021, VOLOSOVIK and ZATOLOKIN hosted and provided fast-flux domain hosting for Client Conspirator 1, who used the fast-flux services to protect the locations of their domains and servers hosting their leak sites and communication platforms, with the intent to launch ransomware attacks by Client Conspirator 1 that were intended to extort payments from victims, each of which constituted a separate overt act:

a. On or about April 30, 2022, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 15.

b. On or about May 1, 2022, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 16.

c. On or about May 21, 2022, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 17.

d. On or about June 4, 2022, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support

ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 18.

e. On or about September 10, 2022, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 19.

f. On or about January 9, 2023, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 20.

g. On or about April 10, 2023, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 21.

h. On or about September 18, 2023, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 22.

i. On or about January 17, 2024, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 23.

j. On or about January 8, 2024, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 1 to support ransomware campaigns launched by Client Conspirator 1 that were intended to extort payments from Victim 24.

165. On or about October 21, 2021, VOLOSOVIK and ZATOLOKIN provided services, including domains maintained on ffv2.ru, to Client Conspirator 2 to support ransomware campaigns launched by Client Conspirator 2 that were intended to extort payments from Victim 2.

166. On or about May 21, 2020, VOLOSOVIK and ZATOLOKIN began to offer BPH services to Client Conspirator 3 using MEDIALAND infrastructure.

167. On or about December 31, 2022, MEDIALAND, VOLOSOVIK and ZATOLOKIN hosted over 250 domains as part of their BPH service on behalf of Client Conspirator 3, using the email Bubbagumpshrimpco@exploit.im, including:

a. Gasorr.com
b. Affiliatemarketingletters.com
c. Couponbrothers.com
d. Sikescomposites.com
e. Geotypico.com
f. Bootsinthebigcity.com
g. Bimelectrical.com
h. Hardwarebajaar.com
i. Ksplsoft.com
j. Setechnowork.com
k. Medicare-cost.com
l. Intradayinvestment.com
m. Imsensors.com
n. Mad-colour.com
o. Makemoneyonlinefrom-home.com
p. Optiontradingsignal.com
q. Technicollit.com
r. Discountshadesdirect.com
s. Braprestcom
t. Wasfatsahla.com

u. Clippershipintl.com
v. Propertyexpoandshowcase.com

168. VOLOSOVIK and ZATOLOKIN provided BPH for these domains to support ransomware attacks by Client Conspirator 3 of at least ten separate victims, each of which constituted a separate overt act:

a. On or about November 1, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 30.

b. On or about March 10, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 31.

c. On or about March 12, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 32.

d. On or about March 19, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 33.

e. On or about May 24, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3

to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 34.

f. On or about June 28, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 35.

g. On or about June 18, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 36.

h. On or about November 25, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 37.

i. On or about February 25, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 38.

j. On or about January 22, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, to Client Conspirator 3 to support ransomware campaigns launched by Client Conspirator 3 that were intended to extort payments from Victim 39.

169. On or about September 20, 2020, MEDIALAND, VOLOSOVIK and ZATOLOKIN provided BPH services for Client Conspirator 4 who established the domains Egregorwiki.top and Wikiegregor.top on the ffv2.ru server.

170. On or about October 4, 2020, MEDIALAND, VOLOSOVIK and ZATOLOKIN provided BPH for these domains to support at least two ransomware attacks by Client Conspirator 4, of Victim 3, each of which constituted a separate overt act:

a. On or about October 4, 2020, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 4 to carry out ransomware campaigns against Victim 3.

b. On or about December 29, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 4 to carry out ransomware campaigns against Victim 3 that resulted in damage to the computer systems of Victim 3.

171. From on or about June 28, 2017, through on or about July 6, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, during the time period Client Conspirator 5 launched ransomware campaigns that were intended to extort payments, each of which constituted a separate overt act:

a. On March 31, 2020, VOLOSOVIK and ZATOLOKIN caused an email to be sent from domaine@sshvps.net to medialand.webnic@gmail.com, "Subject: 30 Days Before Expiry Domain Expiration Notice for snatch.team," containing fraudulent

representations that abuse remediation would be undertaken by MEDIALAND administrators.

b. On April 30, 2020, VOLOSOVIK and ZATOLOKIN caused an email to be sent from domaine@sshvps.net to medialand.webnic@gmail.com, "Subject: Reminder to update the WHOIS information snatch.team," based on fraudulent representations that abuse remediation would be undertaken by MEDIALAND administrators.

c. On or about December 29, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 5 to carry out ransomware campaigns against Victim 4.

d. On or about October 16, 2019, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 5 to carry out ransomware campaigns against Victim 5.

e. On or about April 1, 2020, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 5 to carry out ransomware campaigns against Victim 6.

f. On or about December August 6, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 5 to carry out ransomware campaigns against Victim 7.

g. On or about July 6, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 5 to carry out ransomware campaigns against Victim 8.

h. On or about December 14, 2019, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 5 to carry out ransomware campaigns against Victim 9.

172. On March 6, 2023, VOLOSOVIK and ZATOLOKIN maintained, on the ffv2.ru server, a database table "user_domain," for Client Conspirator 5 that contained four domains used by Client Conspirator 5 to carry out ransomware attacks.

173. On June 18, 2024, VOLOSOVIK and ZATOLOKIN maintained, on the ffv2.ru server, a database table, "users_domain," for the Client Conspirator 5 that contained three domains used by Client Conspirator 5 to carry out their ransomware attacks, and a second database table "reg_domain" that contained a domain used by Client Conspirator 5 in its ongoing ransomware scheme.

174. From on or about February 24, 2021, through on or about July 1, 2023, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, during the time period Client Conspirator 6 launched ransomware campaigns that were intended to extort payments from victims, each of which constituted a separate overt act:

a. On or about February 2, 2023, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by

MEDIALAND, used by Client Conspirator 6 to carry out ransomware campaigns against Victim 10.

b. On or about February 24, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 6 to carry out ransomware campaigns against Victim 11.

c. On or about July 1, 2023, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 6 to carry out ransomware campaigns against Victim 12.

175. On or about September 11, 2024, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to domains maintained on ffv2.ru, during the time period Client Conspirator 7 launched ransomware campaigns that were intended to extort payments from Victim 1.

176. From on or about February 27, 2020, through on or about May 26, 2020, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 8 to carry out ransomware campaigns, each of which constituted a separate overt act:

a. On or about February 27, 2020, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 8 to carry out ransomware campaigns against Victim 13 that resulted in damage to the computer systems of Victim 13.

b. On or about May 26, 2020, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 8 to carry out ransomware campaigns against Victim 14 that resulted in damage to the computer systems of Victim 14.

177. From on or about July 15, 2022, through on or about April 15, 2023, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 9 to carry out ransomware campaigns, each of which constituted a separate overt act:

a. On or about April 15, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 9 to carry out ransomware campaigns against Victim 25 that resulted in damage to the computer systems of Victim 25.

b. On or about July 15, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND,/ used by Client Conspirator 9 to carry out ransomware campaigns against Victim 26 that resulted in damage to the computer systems of Victim 26.

178. On or about July 2, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 10 to carry out ransomware campaigns against Victim 29, which resulted in damage to the computer systems of Victim 29.

179. On or about June 18, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND,

used by Client Conspirator 11 to carry out ransomware campaigns against Victim 43 that resulted in damage to the computer systems of Victim 43.

180. On or about February 10, 2022, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 12 to carry out ransomware campaigns against Victim 41 that resulted in damage to the computer systems of Victim 41.

181. On or about January 5, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 13 to carry out ransomware campaigns against Victim 28 that resulted in damage to the computer systems of Victim 28.

182. On or about October 16, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 14 to carry out ransomware campaigns against Victim 40 that resulted in damage to the computer systems of Victim 40.

183. On or about March 24, 2021, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 15 to carry out ransomware campaigns against Victim 42 that resulted in damage to the computer systems of Victim 42.

184. On or about November 30, 2020, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND, used by Client Conspirator 16 to carry out ransomware campaigns against Victim 27 that resulted in damage to the computer systems of Victim 27.

185. On or about October 24, 2024, VOLOSOVIK and ZATOLOKIN provided services, including but not limited to the use of domains and/or IP addresses maintained by MEDIALAND and ML.CLOUD, used by Client Conspirator 17 to carry out brute force attacks against Victim 44 that resulted in damage to the computer systems of Victim 44.

186. From on or about May 21, 2020, MEDIALAND, VOLOSOVIK and ZATOLOKIN provided BPH services to a criminal marketplace named Briansclub.

187. Until on or about April 16, 2024, MEDIALAND, VOLOSOVIK and ZATOLOKIN hosted domain names Briansclub.cm, Brianscrabs.de, located in the ffv2.ru server's domain name service zone files as part of the BPH services provided to the criminal marketplace, Briansclub.

FRAUDULENT BPH SERVICES PROVIDED BY VOLOSOVIK AND ZATOLOKIN TO SUPPORT AND AID AND ABET CLIENT CONSPIRATOR ATTACKS

188. On or about September 21, 2015, VOLOSOVIK and ZATOLOKIN sent an email with subject "test" and body "test" from alex.kitai@gmail.com to admin@ffpanel.ru.

189. On or about and between January 1, 2017, until on or about June 23, 2024, VOLOSOVIK operated iCloud account 1373199991, associated with his email stas_vl@mail.ru and Russian telephone number 79811263828.

190. On or about January 1, 2017, VOLOSOVIK saved screenshots showing an administrator connection to the ffv2.ru server that supported and aided and abetted Client Conspirator malware attacks.

191. On or about January 1, 2017, VOLOSOVIK saved screenshots for IP Address 45.141.84.8, which showed testing the responsiveness and uptime of the MEDIALAND infrastructure.

192. On or about January 1, 2017, ZATOLOKIN operated iCloud account 1004652016, associated with his email der_fan@mail.ru and Russian telephone number 79992202488.

193. On or about January 1, 2017, ZATOLOKIN saved screenshots that show an HTTPS connection to the ffv2.ru server administrator panel listing Client Conspirator's usernames with their associated domain and IP resolution.

194. On or about January 1, 2017, ZATOLOKIN saved screenshots of the website check-host.net[1] identifying IP Address 65.108.65.82 and testing IP addresses through ICMP Pings and TCP connections. IP Address 65.108.65.82 is the resolution for the MEDIALAND server FFPANEL.TOP previously located in Finland.

195. On or about January 1, 2017, ZATOLOKIN saved screenshots of ZATOLOKIN, using the screen name "Slim Shady," discussing setting up domains with a client conspirator.

196. On or about January 1, 2017, VOLOSOVIK's iCloud account contained a WhatsApp account associated to VOLOSOVIK's Russian Telephone number 79811263828, which was in communication with a WhatsApp account associated with ZATOLOKIN's telephone number 79992202488.

197. On or about January 1, 2017, until on or about September 18, 2018, VOLOSOVIK and ZATOLOKIN used WhatsApp to communicate with each other about abuse reports and other issues affecting Client Conspirators, each of which is a separate overt act:

---

1 According to its website, check-host.net is "an online tool for checking availability of websites, servers, hosts and IP addresses. It provides domain and IP address location data from a few geolocation IP databases and whois as well." Services include IP Info, HTTP, TCP port, Subnet calculator, API, Ping, DNS, UDP port, Bookmarklet. The TCP port, "checks the possibility of a TCP connection to host's specified port." The Ping, "allows to test the reachability of a host, to measure network latency and packets loss from difference servers in the world."

a. On or about January 9, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "The client has error codes related to CentOS. I am telling him, we don't have CentOS, and everything is running on Debian. Yes, we gave him the server, but it's his job to properly tune it. Let him hire an admin, I'm not going to do this for him."

b. On or about January 9, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "All tune-up of that VPS is that we have installed a panel on top of it and gave it to him. All further tuning should be done by his admin."

c. On or about January 9, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "This is an error of that VPS. Fast-flux is running on Debian, all messages about CentOS are misleading and mean bad server tune-up. Let him hire his own admin and take care of that."

d. On or about March 2, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "A client needs 10 more domain names. I have told him it will cost an extra 100."

e. On or about August 26, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "I have sent you the money, Nishebrod has paid $300 on the 4th. I have used some of that money to pay the Chinese on Yandex. You can see one of ours is dead. I can buy more, but you need to order socks (sockets)?"

f. On or about September 2, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "We had experienced that before with the Chinese. It's probably an account that was banned, so money cannot be added to it. We need to try that on a clean account."

g. On or about September 2, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "A client has asked to just turn the server on, not the Fast-flux. He needs to add his files first."

h. On or about September 2, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "That American is getting on my nerves again. You have bought that VPS that's not working, so get on your Jabber, connect with him and fix it."

i. On or about November 8, 2017, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "Half of my panel is in red, nobody answers. If they won't wake up, we will have maybe 5 to 7 clients left. We need to get new ones, start advertising on forums like 'Dark Money.'"

j. On or about April 26, 2018, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "Nishebrod and Neverforget are getting new proxies, their domains were tied to old IP addresses."

k. On or about May 1, 2018, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "DNS Pod has correct IP address. There is a glitch somewhere else."

l. On or about August 7, 2018, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "That IP address is banned in Russia. It should work in America and elsewhere in the world."

m. On or about August 20, 2018, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "Kirill, I have forgot to tell you it's time for these two clients, Guest and Neverforget, to pay up. Get the money from them. Once we receive the money, I'll try to procure tickets for you."

n. On or about September 9, 2018, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "IP proxy needs to be added. Try a Chinese one, but you have to make sure he can open his ports. Try pinging 20 minutes after."

o. On or about September 9, 2018, ZATOLOKIN communicated, via WhatsApp, to VOLOSOVIK, "No, ports are closed. These Chinese proxies only have ports 80 and 443 open. I don't know how it used to work in the past."

198. On or about March 17, 2014, VOLOSOVIK linked the email account alex.kitai@gmail.com with admin@abushost.ru to receive system notifications generated by Client Conspirators to the MEDIALAND BPH service controlled and maintained by VOLOSOVIK and ZATOLOKIN.

199. On or about November 12, 2014, Client Conspirators malware activities hosted by VOLOSOVIK caused to be sent to alex.kitai@gmail.com an abuse report with the subject "Domain FFV2.RU blocked," which detailed the blocking of ffv2.ru because of infringement of rules of registration and/or use of a domain name.

200. On or about November 12, 2014, Client Conspirators malware activities hosted by VOLOSOVIK caused to be sent to alex.kitai@gmail.com an abuse report with the subject "Fwd: [regtime #561457] [Spamhaus] Illegal botnet domains – please HOLD" detailing a request for domain suspension from Spamhaus for s777shop.ru and ffv2.ru.

201. On or about November 12, 2014, Client Conspirators malware activities hosted by VOLOSOVIK caused to be sent to alex.kitai@gmail.com an abuse report that read in part, "Hello, Spamhaus has identified the following domain names which are operated by cybercriminals and used to control infected computers (bots) using a so called 'botnet controller' s777shop.ru, ffv2.ru."

202. On or about November 14, 2014, VOLOSOVIK used the email account alex.kitai@gmail.com to send an email to support@webnames.ru with subject "RE: [regtime #561969] Re: Domain FFV2.RU blocked" that contained a conversation where VOLOSOVIK inquired of support personnel about the blocking of an RU zone domain based on information from Spamhaus.

203. On or about to January 10, 2015, VOLOSOVIK and ZATOLOKIN used the email alex.kitai@gmail.com to register the domain "abushost.ru" and set up accounts for encrypted Jabber services.

204. On or about September 24, 2015, VOLOSOVIK created and registered the domain SSHVPS.NET, and provided his name as its Administrator, Administrator telephone: 79811263828, Administrator email: alex.kitai@gmail.com and MEDIALAND as the Administrator Organization.

205. Starting on or about January 10, 2015, to effect the scheme to conspire with and aid and abet malware actors, VOLOSOVIK and ZATOLOKIN provided false or fraudulent representations for abuse mitigation by providing the domain abushost.ru and the email account alex.kitai@gmail.com to accept legitimate abuse reports of victims of Client Conspirator malware attacks, each example serving as an overt act:

a. On or about January 10, 2015, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report with subject "Domain abushost.ru expires at 2015-03-09."

b. On or about February 3, 2015, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report with the same subject, "Domain abushost.ru expires at 2015-03-09."

c. On or about August 30, 2018, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report received from abuse.fraud@cybersoc.deloitte.es reporting an abuse using the IP Address (185.100.222.28) that served as a command and control server for "Malware family: RedAlert, Malware type: Trojan Banker."

d. On or about August 30, 2018, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report from abuse.fraud@cybersoc.deloitte.es further defining the complainant in this email as follows:

> RedAlert is an android banking Trojan that is being distributed via fake apps in order to infect as many smartphones and tables as possible. RedAlert has a configuration file in which it indicates, among other information, the financial institutions defined as targets and has a configuration file to fetch components to perform it malicious activity. Once a user that is using an infected device accesses to the website of one of these entities, the malware steals the credentials injecting malicious code.

e. On or about September 6, 2018, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report from email address support@regtime.net indicating that domain ffpanel.ru has been blocked.

f. On or about September 6, 2018, VOLOSOVIK and ZATOLOKIN, using the email account alex.kitai@gmail.com, sent a response to support@regtime.net requesting that the domain, ffpanel.ru, be unblocked, and VOLOSOVIK included a scanned copy of his passport with the request.

h. On or about October 3, 2018, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an

abuse report from support@webnames.ru, with a reply-to address of abuse-team@hispasec.com, reporting malware was being hosted on domain ffpanel.ru with an IP address of 47.254.171.103. The report included a VirusTotal analysis link, along with the offending URL, that initiated malware downloads for each bank of the malicious file: hxxp://ffpanel.ru/client_ip.php?key=1914558d44bb50. The file is described as: "This files (sic) are associated with a banking Trojan that is trying to infect people to steal their banking credentials, targeting several banks...."

i. On or about November 9, 2018, VOLOSOVIK and ZATOLOKIN sent an email from alex.kitai@gmail.com to cert@bi.zone, complaining about the DNS server on domain ffpanel.ru being blocked because of the report of malware, and requested the domain be unblocked. The associated complaint indicated that ffpanel.ru was involved in malware distribution and provided the following file information:

> Application name: Update Flash Player
> md5(AdobeFlashPlayer.apk) = adefe40f6fa5acd55feecfd8446855f44c2c
> C&C: ffpanel.ru (8.208.10.54)
> Gateway: 188.68.208.159
> Type: Trojan-Banker.AndroidOS.RedAlert 2.0

j. On or about November 29, 2018, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to abuse@sshvps.net a report of abuse from tfischer@bfk.de advising of an abuse, which was identified as Android Malware RedAlert, using an IP address within MEDIALAND's network as a command-and-control.

k. On or about November 29, 2018, VOLOSOVIK and ZATOLOKIN replied from the emails abuse@sshvps.net and alex.kitai@gmail.com to tfischer@bfk.de,

fraudulently advising "this client is blocked," when, in fact, the Client Conspirators continued to distribute malware through MEDIALAND infrastructure.

l. On or about November 29, 2018, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to abuse@sshvps.net a report of abuse from a German IT Security Consulting company informing them that their IP address 185.254.121.69, within MEDIALAND's network (ASN 206728), served as a command-and-control server for the Android banking trojan RedAlert.

m. In response to that notice, VOLOSOVIK and ZATOLOKIN, using the email accounts abuse@sshvps.net, and alex.katai@gmail.com, responded to the complainant, "this client is blocked."

n. On or about March 1, 2020, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com a notification from support @webnames.ru with the same subject, "Domain abushost.ru expires at 2020-03-09."

o. On or about December 9, 2020, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com and medialand.regru@gmail.com a notification from WebNames.ru stating that ffv2.ru expires on December 13, 2020.

p. On or about March 8, 2021, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com a notification from support@webnames.ru with the subject, "Domain abushost.ru expired at 2021-03-09."

q. On or about December 9, 2021, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com a notification from WebNames.ru stating that ffv2.ru expires on December 13, 2021.

r. On or about March 8, 2022, Client Conspirators malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com a notification from support @webnames.ru with the subject, "Domain abushost.ru expired at 2022-03-09."

s. On or about July 11, 2022, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com and abuse@sshvps.net a notification from a cyber security company that Ermac malware was being deployed using MEDIALAND IP address 45.141.85.29.

t. On or about July 11, 2022, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com and abuse@sshvps.net from takedown@innotec.security with the subject: "Malware incident detected on a website hosted by Media Land LLC. This was detected on IP Address 45.141.85.29." The text of the email reported:

> We have detected an ERMAC malware incident against Santander, on a website hosted by Media Land LLC". The email response further explains the ERMAC malware as follows: "The Ermac malware family falls under the category of Android banking malware, which has seen a boom in the latest malware threat trends and has a number of distinctive tactics, techniques and procedures. These mainly consist of camouflaging the malicious code under a harmless application, keeping it hidden on the target system for a while, in order to obtain the necessary permissions and, finally, falsify the login screen of a legitimate application in order to achieve its ultimate goal, that is, to obtain the user's banking credentials."

u. On or about July 27, 2022, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report from takedown@innotec.security with the subject: "Malware detected on a website hosted by MediaLand".

v. On or about March 8, 2023, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report from support @webnames.ru with the subject, "Domain abushost.ru expired at 2023-03-09."

w. On or about May 31, 2023, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com an abuse report from SPFBL Admin with the subject: Abuse report #1hlpjsgik from 45.141.86.82.

x. On or about July 3, 2023, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com and abuse@sshvps.net an email from a security company with the subject: Phishing attack(s) hosted on 91.220.163.63.

y. On or about August 27, 2023, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com and abuse@sshvps.net an email from abuse@skhron.com.ua, with the subject: Abuse report: Portscan/attack detected from 45.141.84.16.

z. On or about September 4, 2023, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent to alex.kitai@gmail.com and

abuse@sshvps.net an email from a security company with the subject: Abuse report: Portscan/attack detected from 194.26.29.16.

206. In or around April 2023, Client Conspirators' malware activities hosted by VOLOSOVIK and ZATOLOKIN caused to be sent another abuse report to alex.kitai@gmail.com, identifying the deployment of malware and an Android banking trojan that had previously been the subject of the abuse report involving MEDIALAND IP address 45.141.85.29 and sent to alex.kitai@gmail.com on or about July 11, 2022.

USE OF MEDIALAND INFRASTRUCTURE BY CRIMINAL MARKETPLACES

207. On or about March 6, 2023, VOLOSOVIK and ZATOLOKIN hosted on the ffv2.ru server on MEDIALAND infrastructure the following domains in support of, and aiding and abetting to, criminal infrastructure and which were associated to criminal marketplaces and forums which advertised and/or sold personal identifiable information, bank account, credit card and other personal information of victims, stolen by unidentified client conspirators, with each domain hosting representing a separate overt act:

Name of Marketplace/Forum	**Domains hosted on MEDIALAND infrastructure**	**Description of the Criminal Marketplace/Forum.**
Briansclub	Brianscrabs.de, Briansclub.cm	Carding marketplace to sell and buy stolen credit card data.
Cardhouse	Cardhouse.cc	Re-Seller on the Bypass Market a darknet Marketplace selling stolen credit card information.
crdclub	Crdclub.su	Forum to advertise stolen credit card
Club2crd	Club2crd.cc	Russian language carding forum
Verified	Verified.mn	Darkweb criminal forum
Fullzinfo	Fullzinfo.com	Selling PII, creditcard and financial account information.
Swipestore	Swipestore.cc	Carding marketplace to sell and buy stolen credit card data.

Name of Marketplace/Forum	Domains hosted on MEDIALAND infrastructure	Description of the Criminal Marketplace/Forum.
Bidencash	Bidencash.link Bidencash.rip	Carding marketplace to sell and buy stolen credit card data.

DATES OF PAYMENTS FROM CRYPTOCURRENCY ACCOUNTS

208. On or about October 21, 2021, VOLOSOVIK caused a deposit in a Bitcoin wallet registered to the email account alex.kitai@gmail.com a share of funds traced back to the ransomware extortion of VICTIM 2 by ransomware attack by an unknown Client Conspirator.

209. Beginning on or about May 24, 2022, MEDIALAND, VOLOSOVIK, and ZATOLOKIN hosted servers used by Client Conspirator 5 to launch a ransomware attack on VICTIM 8.

210. On or about August 6, 2022, VICTIM 7 was attacked with ransomware during a malware attack launched by Client Conspirator 5.

211. On or about August 13, 2022, VICTIM 7 made payments to Client Conspirator 5 in response to the ransomware attack launched on August 6, 2022.

212. On or about September 5, 2022, VOLOSOVIK, using a Bitcoin cluster identified as "Yalishanda – bulletproof hoster," received approximately $4,665, or .23 BTC, from Client Conspirator 5 for the use of MEDIALAND infrastructure in support of the August 6, 2022, ransomware attack on VICTIM 7.

All in violation of 18 U.S.C. § 371.

COUNT 2
(Conspiracy to Commit Wire Fraud, 18 U.S.C. § 1349)

The Grand Jury further charges:

213. Paragraphs 1 through 128 and 143 through 212 of this Indictment are realleged and incorporated by reference as if fully set forth herein.

214. From on or about February 19, 2016, to the date of the Indictment, in the Northern District of Ohio, Eastern Division and elsewhere, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, and ML.CLOUD, and others known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate and agree with others to commit wire fraud, that is:

> to knowingly devise and execute, and attempt to execute, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises; and in executing and attempting to execute this scheme and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by means of wire communication, certain signs, signals and sounds as further described herein, in violation of Title 18, United States Code, Section 1343.

Objects of the Conspiracy

215. The objects of the conspiracy included:

a. to enrich the Defendants by advertising, maintaining and leasing infrastructure services to malware and ransomware actors that supported and aided and abetted the launch and execution of criminal cyber schemes;

b. to provide Client Conspirators with BPH infrastructure and fast-flux domain hosting that supported and aided and abetted malware and ransomware schemes that obtained illicit funds; and

c. to avoid detection and conceal the existence of the conspiracy through materially false and fraudulent pretenses and representations.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

216. MEDIALAND and PANKOVA used ML.CLOUD to provide infrastructure that appeared to be a legitimate ISP in order to provide cover for the illegal domain and infrastructure support for clients managed by VOLOSOVIK and ZATOLOKIN.

217. MEDIALAND and PANKOVA provided financial support to VOLOSOVIK and ZATOLOKIN by allowing VOLOSOVIK and ZATOLOKIN to use financial accounts and credit cards in the name of MEDIALAND to pay for infrastructure used for illicit purposes.

218. Defendants VOLOSOVIK and ZATOLOKIN promoted "Bullet Proof Hosting" and Fast-flux services through MEDIALAND on forums that catered to individuals and groups engaged in ransomware and malware schemes.

219. Defendants VOLOSOVIK and ZATOLOKIN then provided those Client Conspirators space on servers owned by or leased to MEDIALAND and access to admin panels controlled and managed by VOLOSOVIK and ZATOLOKIN.

220. VOLOSOVIK and ZATOLOKIN maintained these backend database tables to manage approximately 389 unique usernames belonging to MEDIALAND Client Conspirators 1, 3-, and 14 who used the fast-flux service hosted on the ffv2.ru server.

221. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 1 to install malware on computers used by VICTIMS 15-24 to extort and steal money and other things of value.

222. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 3 to install malware on computers used by VICTIMS 30-39 to extort and steal money and other things of value.

223. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting hosted on ffv2.ru to Client Conspirator 4 to install malware on computers used by Victim 3 to extort and steal money and other things of value.

224. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 5 to install malware on computers used by Victims 4-9 to accept extortionate ransomware payments made by Victims 4-9 to release data exfiltrated by Client Conspirator 5.

225. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting hosted on ffv2.ru to Client Conspirator 6 to install malware on computers used by Victims 10, 11 and 12 to extort and steal money and other things of value.

226. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting hosted on ffv2.ru to Client Conspirator 7 to install malware on computers used by Victim 1 to extort and steal money and other things of value.

227. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting hosted on ffv2.ru to Client Conspirator 8 to install malware on computers used by Victims 13 and 14 to extort and steal money and other things of value.

228. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 9 to install malware on computers used by Victims 25 and 26 to extort and steal money and other things of value.

229. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 10 to install malware on computers used by Victim 29 to extort and steal money and other things of value.

230. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 11 to install malware on computers used by Victim 43 to extort and steal money and other things of value.

231. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 12 to install malware on computers used by Victim 41 to extort and steal money and other things of value.

232. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 13 to install malware on computers used by Victim 28 to extort and steal money and other things of value.

233. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 14 to install malware on computers used by Victim 40 to extort and steal money and other things of value.

234. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 15 to access data exfiltrated from computers used by Victim 42 to extort and steal money and other things of value.

235. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to Client Conspirator 16 to install malware on computers used by Victim to extort and steal money and other things of value.

236. Defendants VOLOSOVIK, ZATOLOKIN, and MEDIALAND provided infrastructure and domain hosting to a Client Conspirator unknown to the Grand Jury to attempt to commit a brute force denial of service attack on Victim 44.

237. Defendants VOLOSOVIK and ZATOLOKIN, used allegedly legitimate and independent email addresses and domains actually controlled by VOLOSOVIK and ZATOLOKIN to accept and reply to abuse reports and other alerts generated by victims and security software of computers victimized by client malware and ransomware.

238. Defendants VOLOSOVIK and ZATOLOKIN received abuse reports and other alerts but did not suspend offending domains or client accounts; instead, Defendants VOLOSOVIK and ZATOLOKIN provided false or fraudulent replies, ignored reports, and offered clients fast-flux services to further circumvent security procedures.

239. Defendants VOLOSOVIK and ZATOLOKIN continued to lease access to servers to malicious Client Conspirators and accepted payment for those hosting services directly from cryptocurrency accounts that contained funds obtained from illicit ransomware and malware schemes.

Acts in Furtherance of the Conspiracy

240. In furtherance of the conspiracy and to effect the objects thereof, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, and ML.CLOUD, and others known and unknown to the Grand Jury, did commit and cause to be committed the overt acts alleged in

Paragraphs 143-212, realleged and incorporated herein, in the Northern District of Ohio, Eastern Division and elsewhere.

241. On or about the date listed below, VOLOSOVIK and ZATOLOKIN maintained and hosted the Internet infrastructure that sent and supported the distribution of malware and ransomware to be sent by means of wire communications in interstate and foreign commerce the writings, signs, signals, pictures and sounds described below, with each wire communication being a separate act in furtherance of the conspiracy as set forth below:

Malware/ Ransomware Variant	Victim(s)	Approximate Date Client Conspirator Sent Wire Communication	Medialand/ML.Cloud Infrastructure Used to Fraudulently Support and Aid and Abet Client Conspirator Wire Communication
CC1	15	4/30/2022	Domain hosted by MediaLand
CC1	16	5/1/2022	Domain hosted by MediaLand
CC1	17	5/21/2022	Domain hosted by MediaLand
CC1	18	6/4/2022	Domain hosted by MediaLand
CC1	19	9/10/2022	Domain hosted by MediaLand
CC1	20	1/9/2023	Domain hosted by MediaLand
CC1	21	4/10/2023	Domain hosted by MediaLand
CC1	22	9/18/2023	Domain hosted by MediaLand
CC1	23	1/17/2024	Domain hosted by MediaLand
CC1	24	1/8/2024	Domain hosted by MediaLand
CC2	2	10/21/2021	VOLOSOVIK received funds from ransomware payment
CC3	30	11/1/2021	Domains hosted by MediaLand
CC3	31	3/10/2022	Domain hosted by MediaLand
CC3	32	3/12/2022	Domain hosted by MediaLand
CC3	33	2/19/2022	Domain hosted by MediaLand
CC3	34	5/24/2022	Domain hosted by MediaLand
CC3	35	6/28/2022	Domain hosted by MediaLand
CC3	36	6/18/2022	Domain hosted by MediaLand
CC3	37	11/25/2022	Domain hosted by MediaLand
CC3	38	2/25/2022	Domain hosted by MediaLand
CC3	39	1/21/2022	Domain hosted by MediaLand
CC4	1	10/4/2020	Domain on ffv2.ru
CC5	4	12/19/2019	Domain hosted by MediaLand
CC5	5	10/16/2019	Domain hosted by MediaLand

Malware/ Ransomware Variant	Victim(s)	Approximate Date Client Conspirator Sent Wire Communication	Medialand/ML.Cloud Infrastructure Used to Fraudulently Support and Aid and Abet Client Conspirator Wire Communication
CC5	6	4/1/2020	Domain hosted by MediaLand
CC5	7	8/6/2022	A portion of one victim's ransom was paid to Yalishanda ; Domains hosted by MediaLand
CC5	8	7/6/2022	Domain hosted by MediaLand
CC5	9	12/14/2019	Domain hosted by MediaLand
CC6	10	2/2/2021	Domains on ffv2.ru & Users on ffv2.ru coincide with CC6 ransomware variant
CC6	11	2/24/2021	Domains on ffv2.ru & Users on ffv2.ru coincide with CC6 ransomware variant
CC6	12	7/1/2023	Domains on ffv2.ru & Users on ffv2.ru coincide with CC6 ransomware variant
CC7	1	9/11/2024	MediaLand IP address associated with attack
CC8	13	2/27/2020	Domain on ffv2.ru
CC8	14	5/26/2020	Domain on ffv2.ru
CC9	25	4/15/2023	IP address associated with attack was assigned to MediaLand at the time
CC9	26	7/15/2022	IP address associated with attack was assigned to MediaLand at the time
CC10	1	7/2022	MediaLand IP address associated with the attack
CC11	1	6/18/2021	MediaLand IP address associated with attack
CC12	1	2/10/2022	MediaLand IP address associated with attack
CC13	1	1/5/2021	MediaLand IP address associated with attack
CC14	1	10/16/2021	MediaLand IP address associated with attack
CC15	1	3/24/2021	MediaLand IP address logged into Mega.nz account used for data exfiltration
CC16	1	11/30/2020	MediaLand IP address associated with attack
CC17	44	10/24/2024	Attempted brute force denial of service attack

All in violation of Title 18, United States Code, Section 1349.

COUNTS 3-12
(Wire Fraud, Title 18, United States Code, Section 1343 and 2)

The Grand Jury further charges:

242. The factual allegations of Paragraphs 1 through 128, 143 through 212, and 241 of this Indictment are hereby repeated, realleged and incorporated by reference as if fully set forth herein.

243. From on or about December 17, 2018 to the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, and ML.CLOUD, and others devised a scheme and artifice to defraud the victims listed in the table below, whose identities are known to the Grand Jury, to obtain money and property, by means of false and fraudulent pretenses, representations and promises, as described in Paragraphs 132 through 141 and 216 through 239.

244. On or about the date listed below, VOLOSOVIK and ZATOLOKIN controlled and maintained servers in New Jersey and Russia that provided MEDIALAND and ML.CLOUD infrastructure which transmitted false and fraudulent responses to ransomware attacks, including agreements to pay ransoms, receive locker passwords, and other communications related to malware attacks that were sent to domains associated with Client Conspirators 4, 5, 6, 7, 8, and a Client Conspirator unknown to the Grand Jury, from computers in the Northern District of Ohio and elsewhere through the use of interstate and foreign wires.

245. On or about the date listed below, for purposes of executing and attempting to execute the above-described scheme and artifice to defraud and to obtain money and property, which scheme affected a financial institution, Defendants VOLOSOVIK and ZATOLOKIN maintained and hosted the Internet infrastructure that sent and supported the distribution of

malware and ransomware to be sent by means of wire communications in interstate and foreign commerce the writings, signs, signals, pictures and sounds described below, with each wire communication being a separate count as set forth below:

Count	Defendants	Victim	Client Conspirator	Date Medialand/ ML.Cloud Infrastructure Used	Medialand/ML. Cloud Infrastructure Used to Fraudulently Support and Aid and Abet	Victim	Medialand / ML.Cloud Infrastructure Location
3	VOLOSOVIK ZATOLOKIN	3	Client Conspirator 4	10/4/2020	Domains on ffv2.ru	Solon, OH	New Jersey
4	VOLOSOVIK ZATOLOKIN	4	Client Conspirator 5	12/29/2021	Domain on ffv2.ru	Medina, OH	New Jersey
5	VOLOSOVIK ZATOLOKIN	5	Client Conspirator 5	10/16/2019	Domain on ffv2.ru	Akron, OH	New Jersey
6	VOLOSOVIK ZATOLOKIN	6	Client Conspirator 5	4/1/2020	Domain on ffv2.ru	Brookfield, OH	New Jersey
7	VOLOSOVIK ZATOLOKIN	10	Client Conspirator 6	2/2/2023	Domains on ffv2.ru & Users on ffv2.ru	Findlay, OH	New Jersey
8	VOLOSOVIK ZATOLOKIN	11	Client Conspirator 6	2/24/2021	Domains on ffv2.ru & Users on ffv2.ru	Cleveland, OH	New Jersey
9	VOLOSOVIK ZATOLOKIN	12	Client Conspirator 6	7/1/2023	Domains on ffv2.ru & Users on ffv2.ru	Cleveland, OH	New Jersey
10	VOLOSOVIK ZATOLOKIN	13	Client Conspirator 8	2/27/2020	Domain on ffv2.ru	Elyria, OH	New Jersey
11	VOLOSOVIK ZATOLOKIN	14	Client Conspirator 8	5/26/2020	Domain on ffv2.ru	Valley View, OH	New Jersey
12	VOLOSOVIK ZATOLOKIN	44	Client Conspirator unknown to the Grand Jury	10/24/2024	MEDIALAND and ML.CLOUD IP addresses from ASNs 206728 and 215376	Canton, OH	Russia

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT 13
(Conspiracy to Commit Money Laundering, 18 U.S.C. § 1956(h))

The Grand Jury further charges:

246. The factual allegations of Paragraphs 1 through 128, 143 through 212, 241, and 243-245 of this Indictment are hereby repeated, realleged and incorporated by reference as if fully set forth herein.

The Conspiracy

247. From in or around June 14, 2016, through the date of this Indictment, in the Northern District of Ohio, Eastern Division and elsewhere, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, and ML.CLOUD, and others known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate and agree with each other:

a. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, Wire Fraud, in violation of 18 U.S.C. § 1343 and Fraudulent Access to Computers, in violation of 18 U.S.C. § 1030, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i);

b. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument and funds involving the proceeds of specified unlawful activity, that is, Wire Fraud, in violation of 18 U.S.C. § 1343, and Fraudulent Access to Computers, in violation of 18 U.S.C. § 1030, from a place in the United States to and through a place outside the United States, knowing that the funds involved in the transportation, transmission, and transfer, and attempt to transport, transmit, or transfer, represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(2)(B)(i); and

c. to knowingly engage and attempt to engage in a monetary transaction in criminally derived property with a value greater than $10,000, which property was derived from a specified unlawful activity, that is, Wire Fraud, in violation of 18 U.S.C. § 1343 and Fraudulent Access to Computers, in violation of 18 U.S.C. § 1030, by, through, and to a financial institution and affecting interstate and foreign commerce, in violation of 18 U.S.C. § 1957.

Manner and Means of the Conspiracy

248. The manner and means used to accomplish the conspiracy are set forth in Paragraphs 1 through 128, 143 through 212, 241, and 243-245 of this Indictment and are hereby re-alleged and incorporated by reference as if fully set forth herein.

249. Defendants VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND, and other Client Conspirators known and unknown to the Grand Jury, directed victims of ransomware

attacks to pay ransom payments using anonymous cryptocurrency accounts provided and controlled by Client Conspirators and Defendants VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND to conceal and disguise the nature, location, source, ownership, and control of the proceeds of ransomware and malware attacks launched by Client Conspirators.

250. Defendants VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND and other Client Conspirators known and unknown to the Grand Jury, did maintain infrastructure in the United States and in foreign locations that concealed and disguised the nature, location, source, ownership and control of electronic funds transferred and transmitted from victims in the Northern District of Ohio and elsewhere of ransomware and malware attacks by Client Conspirators to cryptocurrency accounts provided and controlled by Client Conspirators and Defendants VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND located outside the Northern District of Ohio.

251. Client Conspirators of Defendants VOLOSOVIK, ZATOLOKIN, PANKOVA, and MEDIALAND sent funds consisting of criminal proceeds of wire fraud and computer fraud schemes, in amounts of cryptocurrency whose value exceeded $10,000, to cryptocurrency accounts controlled by VOLOSOVIK and ZATOLOKIN, either through ACH, wire transfer, or other electronic fund transfers derived from criminal proceeds of Wire Fraud, in violation of 18 U.S.C. § 1343 and Fraudulent Access to Computers, in violation of 18 U.S.C. § 1030.

All in violation of Title 18, United States Code, Section 1956(h).

ENHANCEMENT PURSUANT TO TITLE 18, UNITED STATES CODE, SECTION 3559(g)(1)
(False Registration of a Domain Name)

The Grand Jury further charges that:

252. The factual allegations of Paragraphs 1 through 128, 143 through 212, 241, and 243-245 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

253. In furtherance of the offenses alleged in Counts 1 through 13, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, and ML.CLOUD, together and with others known and unknown to the Grand Jury, knowingly falsely registered and caused to be falsely registered, domain names and knowingly used and caused to be used said domain names in the course of committing the offenses alleged in Counts 1 through 13, namely, VOLOSOVIK and ZATOLOKIN, together and with others unknown to the Grand Jury, registered domains, including volosovichkov-taxi.info, volosovichkov.info, ffv2panelbot.info, carshome.info, vesperdns.info, nicedomainname.info, dndpark.info, dnsmhere.ru, newserversdns222.info, dnsmhere11.info, pspark.info, jackladamada.info, jackladamadab.info, dmsmanagereu.info, mydnshelpers.info, targetpost.info, greatdor.info, greatdor.ru, mydnsserver.info, fatraf.info, unitednstools.info, chernobyldns.info, s3dns.com, lambdadns.com, besdns.ru, cptdns.info, lincomap.ru, publicdns.ru, publicdns.info, domain4dns.info, protonomail.info, protonommail.info, fifdns.info, proxy-dns1.ru, proxy-dns2.ru, min0taur.ru, boxodns.info, rocodns.info, cntdnsnet.info, setdnsnet.info, vipedron.ru, dsfgghgsfadfgh.info, cardhouse.info, amazkonto.info, amazondeutschland.info, fablirsgd.ru, microsoft-windows-defender-update.ru, googleu.ru, googleup.ru, dnspods.ru, xmrdealshere.ru, wedoaccounting.ru, vhost-vps.ru,

mobirevolutconfirmation.com, sdfsdfsdfsdfdsfsdf.ru, 54bb47h.ru, googleclouddns.com, with false names and addresses in a manner that prevented the effective identification of and contact with Defendants and other conspirators, and used those domains in the course of committing the felony offenses charged in Counts 1 through 13.

All in violation of Title 18, United States Code, Section 3559(g)(1).

FORFEITURE

The Grand Jury further charges:

253. The allegations contained in Counts 1-13 of this Indictment are hereby realleged and incorporated by reference as if fully set forth herein for the purpose of alleging forfeiture pursuant to the provisions of Title 18, United States Code, Section 982(a)(2)(B); Title 18, United States Code, Section 1030(i); Title 18, United States Code, Section 981(a)(1)(C); Title 18, United States Code, Section 982(a)(1); and Title 28, United States Code, Section 2461(c). As a result of these offenses, Defendants ALEXANDER ALEXANDROVICH VOLOSOVIK, KIRILL ANDREEVICH ZATOLOKIN, YULIA VLADIMIROVNA PANKOVA, MEDIALAND, LLC, and ML.CLOUD, LLC, shall forfeit to the United States: (i) all property, real and personal, constituting or derived from proceeds they obtained, directly or indirectly, as the result of the offense charged in Count 1; (ii) all personal property that was used or intended or be used to commit or to facilitate the commission of the offense charged in Count 1; (iii) all property, real and personal, which constitutes or is derived from proceeds traceable to the offenses charged in Counts 2-12, inclusive; and, (iv) all property, real and personal, involved in the offense charged in Count 13, and any property traceable to such property.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.

United States v. Alexander Alexandrovich Volosovik, et al.

A TRUE BILL.

_____

FOREPERSON

By: _____

REBECCA C. LUTZKO
United States Attorney