UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Seizure of *(Briefly describe the property to be seized)* Virtualine.net, A Domain Name Registered at Verisign	)	Case No. 1:26-sw-829

APPLICATION BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of Virginia is subject to forfeiture to the United States of America under 18 U.S.C. §§ 982(a)(1), 981(a)(1)(A), 2253(a)(1), (3), 2254 and 47 U.S.C. § 223(h)(7)(A)(i), (iii). (*describe the property*):

SEE ATTACHMENT A, incorporated herein by this reference.

The application is based on these facts:

SEE AFFIDAVIT, incorporated herein by this reference.

☐ Continued on the attached sheet.

Applicant's signature

Reviewed by AUSA/SAUSA:

AUSA Laura Withers

Special Agent Caroline Moolenaar, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. 4.1 by reliable electronic means, specifically telephone (*describe the means*).

Date: 10/22/2026

Judge's signature

City and state: Alexandria, VA

The Hon. William E. Fitzpatrick, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

With respect to "**virtualine.net**" ("SUBJECT DOMAIN NAME"), **Verisign**, which is the domain registry of the SUBJECT DOMAIN NAME, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAME:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation by associating the SUBJECT DOMAIN NAME to the following authoritative name-server(s):
    (a) ns1.fbi.seized.gov;
    (b) ns2.fbi.seized.gov; and/or
    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Verisign;
2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAME pending transfer of all right, title, and interest in SUBJECT DOMAIN NAME to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAME cannot be made absent court order or, if forfeited to the United States, without prior consultation with the **FBI**.
3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN NAME will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"Virtualine.net has been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Virginia as part of a joint law enforcement action involving the partners listed below."

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEIZURE OF:	)	Case No.: 1:26-sw-829
	)	
Virtualine.net,	)	
A Domain Name Registered at Verisign	)	
	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Caroline Moolenaar, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation, and I have been so employed since October 2024. I have been assigned to the Cyber Squad of the Washington Field Office since July 2025. In this role, I investigate computer-related crimes. Prior to becoming a Special Agent, I was an FBI Computer Scientist; I participated in numerous investigations involving computer and high-technology-related crimes such as computer intrusions, cyber espionage, online extortion, and online threats. I have participated in investigations involving fraudulent activity in connection with computers and email. In the course of conducting or participating in criminal investigations, I have been involved in the following: interviewing and debriefing witnesses and subjects; conducting physical surveillance; tracing and analyzing Internet Protocol (IP) addresses; conducting network traffic analysis; performing mobile malware analysis; conducting digital forensics; writing code for data exploitation; collecting and analyzing evidence; and preparing search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. As set forth below, there is probable cause to believe that the domain name **virtualine.net** is property used, or intended to be used, to commit or facilitate violations of Title 18, U.S. Code, Section 2251(d)/(e) (advertising, conspiracy to advertise, and conspiracy to aid and abet advertising of sexually explicit images of minors); Title 47, U.S. Code, Section 223(h) (intentional disclosure of nonconsensual intimate visual depictions of adults and minors); Title 18, United States Code, Section 1956(a)(2)(a) and (a)(1)(B)(i) (concealment and international promotion money laundering) (SUBJECT OFFENSES), and is subject to forfeiture pursuant to 18 U.S.C. §§ 982(a)(1), 981(a)(1)(A), 2253(a)(1), (3), 2254 and 47 U.S.C. § 223(h)(7)(A)(i), (iii). I make this affidavit in support of a warrant to seize the property described in Attachment A, specifically, **virtualine.net**.

4. The procedure by which the government will seize the **Virtualine.net** is described in Attachment A hereto and below. The procedure by which the United States will seize the **Virtualine.net** is described in Attachment A hereto and below.

BACKGROUND ON DOMAIN NAMES

5. Based on my training and experience and information learned from others, I am aware of the following:

6. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). 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. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

7. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

8. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and is the web server.

9. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol ("IP") addresses.

10. Registry: For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".com" and ".net" top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

11. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

12. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

PROBABLE CAUSE

13. The FBI is investigating the bulletproof hosting provider Virtualine. Bulletproof hosting providers do not require Know Your Customer (KYC) data and are generally unresponsive to law enforcement requests for subscriber information or site takedowns.

14. According to its website (**virtualine.net**), Virtualine is a company that offers hosting and server solutions along with domain name purchasing options. The prices for these services vary from $4.74 a month for web hosting to $1,554.80 a month for "high performance bare metal servers."

Virtualine Advertises Its Services to Criminals

15. In September 2025 and in 2026, **virtualine.net** featured advertisements such as the following, in which Virtualine pledged "No KYC," "No Personal Data," and "Offshore locations":

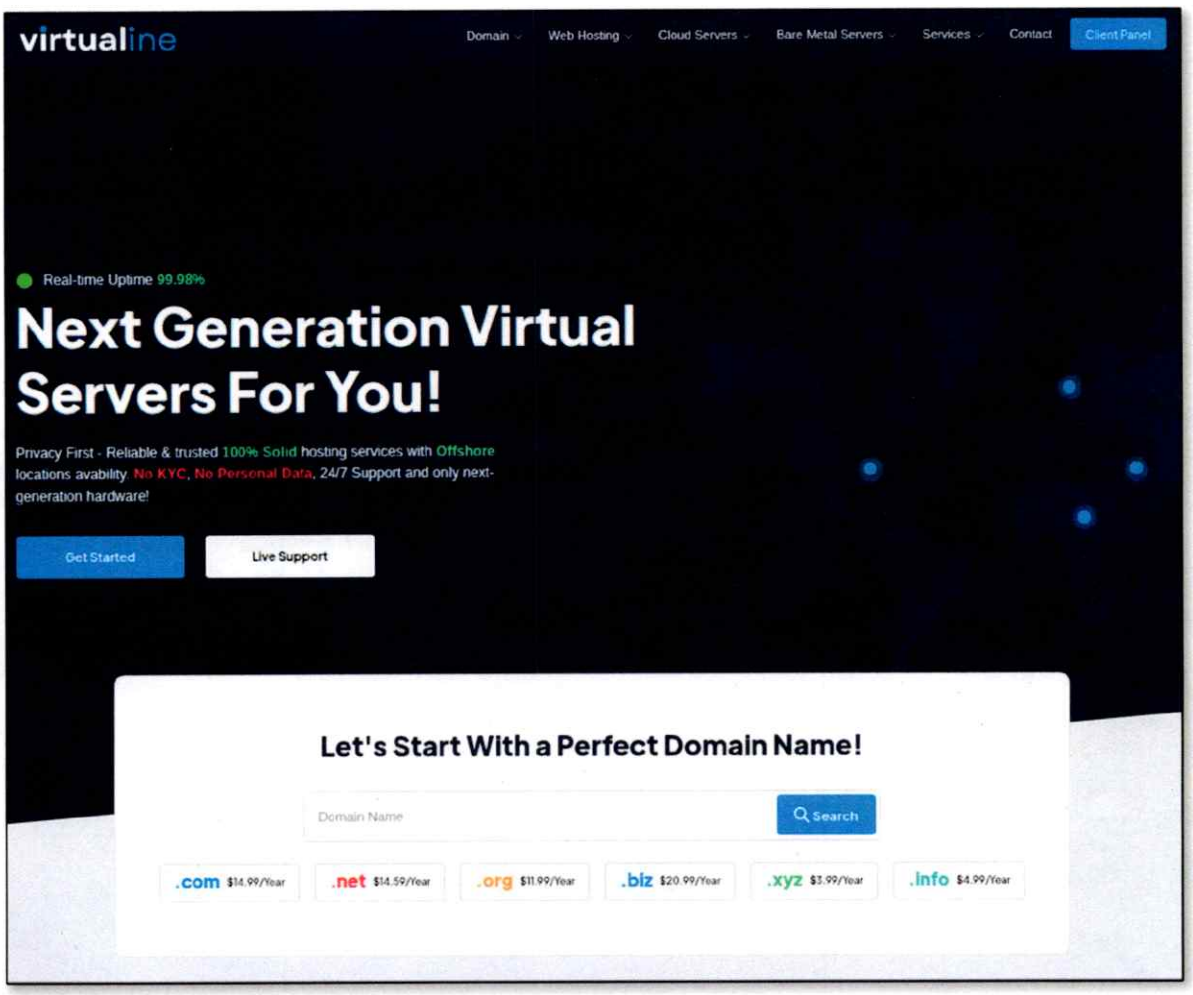


Figure 1. Screenshot of **virtualine.net** from September 2025

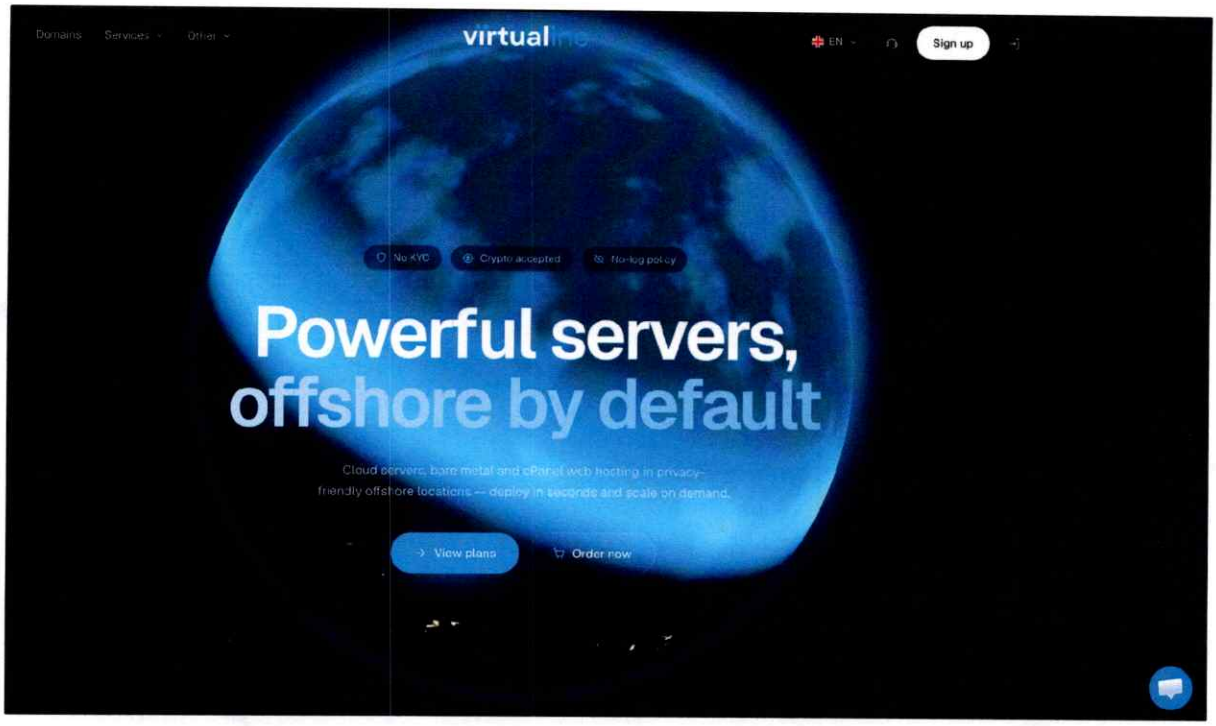


Figure 2. Screenshot of **virtualine.net** from September 2026

16. Virtualine advertised its services on various websites and criminal forums, such as Exploit.in,[1] XSS.is,[2] BlackHatWorld, and HackForums.[3] For example, on or about September 28, 2024, a user wrote in a post on Exploit.in:

> *I do not understand why people advertise services that do not allow any illegal activity on a website that is known for it*

The user "Virtualine" responded:

> *Hi there,*
> *First of all thanks for your comment. You can use Virtualine for all illegal/black hat activities (including phising* [sic]*, carding, email spam, port scanning and all others) except for child contents and terrorism activities.*
> *We actively serve hosting many well-known stores on the TOR network,*
> *we can offer solutions according to the needs.*

[1] "Exploit" is a long-running Russian cybercriminal forum.

[2] "XSS" is an online forum that serves as a marketplace for stolen data, hacking tools, and illicit services.

[3] HackForums is an online discussion forum focusing on hacking and cybersecurity.

I know you mentioned the TOS on the website, but we cannot write everything clearly on the website, you should understand that. I hope this message was explanatory.
You can contact us for detailed information.
Thanks.

17. I know the following terms to have the following meanings:

a. "Black hat activities" often refer to criminal hackers who violate computer security for person gain or other malicious purposes.

b. "Phising" is likely a misspelling of "phishing," which is an attempt to steal sensitive information, typically by masquerading as a legitimate source.

c. "Carding" is the illegal practice of obtaining, trafficking, or using credit card information without authorization.

d. "Email spam" is unsolicited or unwanted emails sent out in bulk to an indiscriminate recipient list.

e. "Port scanning" is a technique used to identify open ports on a network device, often for the purposes of determining exploitable vulnerabilities on that device.

f. "TOS" is most likely an acronym for "Terms of Service."

18. On or about March 25, 2026, the user Virtualine made the following Exploit post, which stated, in part:[4]

When we receive an official request from law enforcement agencies regarding a server, we temporarily suspend its operation to prevent possible data transfer to third parties and immediately contact the client.

If an additional protection package is activated, the IP address (/32) assigned to your server is transferred to the infrastructure of another shell company not affiliated with

[4] The post was originally in Cyrillic. The excerpt has been machine translated.

Virtualine, after which the server is reactivated.

In this case, we cover the costs of the intermediary provider's services.

This is the true level of bulletproof hosting.

Everyone knows examples of "providers" who supposedly ignore police and court requests, but ultimately lose their infrastructure and hand over all data to government agencies.

19. On or about April 14, 2026, the user Virtualine replied to a post on Exploit, stating:

This applies only to high-risk industries.

Remember that we manage the world's biggest malware/botnet[5] ASN.[6] Ensuring everyone's security is essential.

20. Virtualine also advertised on HackForums, where it created a thread titled "[BULLETPROOF] Windows/Linux/MacOS VPS from $4.99 DMCA[7] & Abuse Ignored Virtualine" posted on or about August 20, 2024.

---

[5] Botnet" refers to a network of compromised computers (known as "bots"). Botnet operators are able to covertly access the bots for a variety of malicious purposes, including stealing financial information, such as online banking passwords and login credentials, from the bots. Botnet operators frequently use the stolen information to commit fraud or sell it to others who intend to use the information to commit fraud.

[6] Autonomous System Number (ASN) is a unique identification number assigned to a large network or a group of connected IP networks that share a single routing policy.

[7] "DMCA" likely stands for the Digital Millenium Copyright Act.

Figure 3. HackForums Screenshot

21. On or about November 24, 2025, in response to a user's question, Virtualine stated, "Hi, you can host RAT."[8]

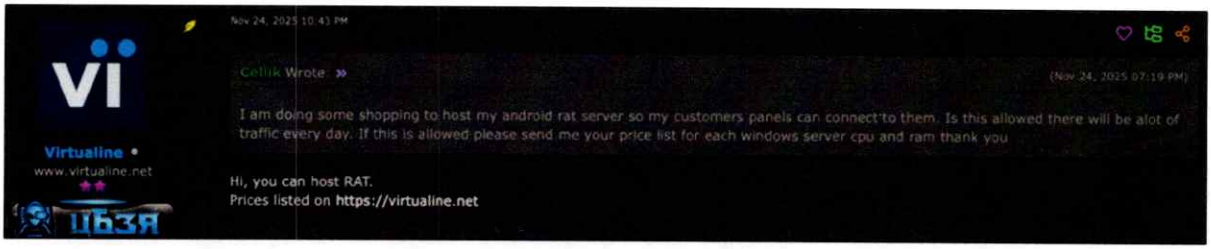


Figure 4. Exploit Screenshot

22. On or about December 8, 2025, in response to a question "May I ask if this ignores virustotal[9] reports?" Virtualine stated, "Hi, malware allowed. No problem."

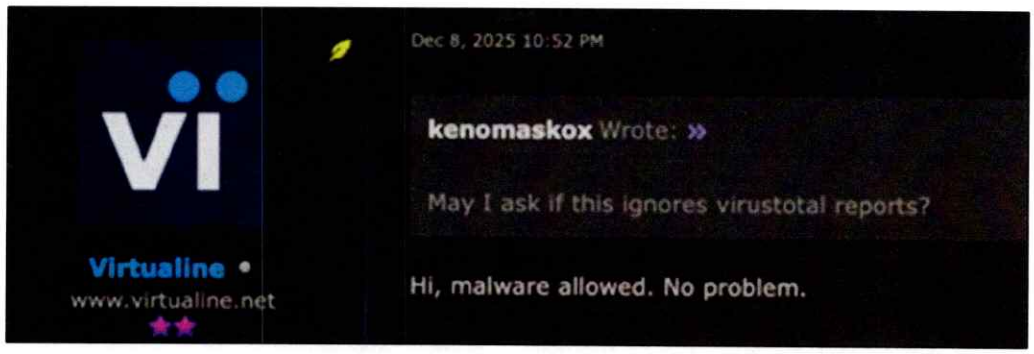


Figure 5. Exploit Screenshot

---

[8] RAT is an acronym for a remote access trojan, which is malicious software disguised as a harmless file or program that gives a hacker hidden, full administrative control over your computer.

[9] VirusTotal is a free online service that analyzes suspicious files, URLs, IP addresses, and domains for malware and other security threats.

23. Virtualine advertised on BlackHatWorld with a post titled "[BULLETPROOF] Windows/Linux/MacOS VPS from $4.99 DMCA & Abuse Ignored cPanel Hosting from $0.79 Offshore Locations | Virtualine.net | Fully NVMe." The account previously used the name "Secury."

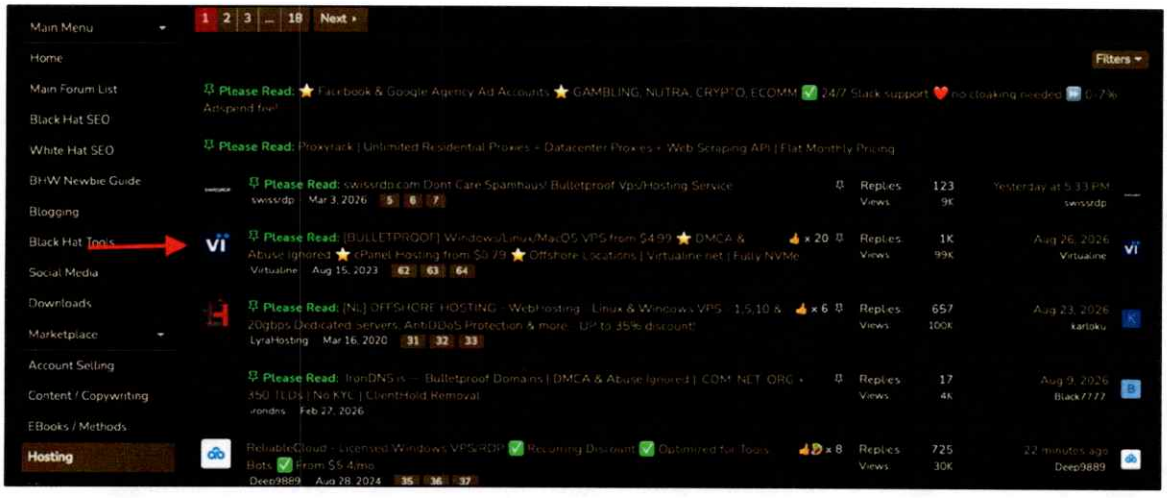


Figure 6. BlackHatWorld Screenshot

24. On or about July 26, 2025, Virtualine stated on Exploit, "All abuse reports and DMCA takedown requests are fully ignored (except than child abuse and terrorism)."

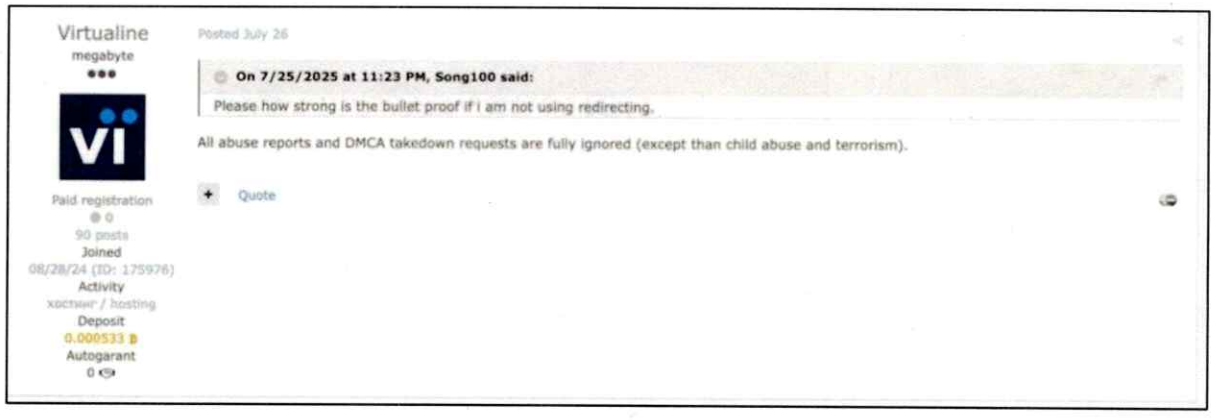


Figure 7. Exploit Screenshot

25. On or about August 7, 2025, Virtualine stated on Exploit, "The terms of use on our website are standard. We do not enforce them. We ignore everything except for child abuse

and terrorism."

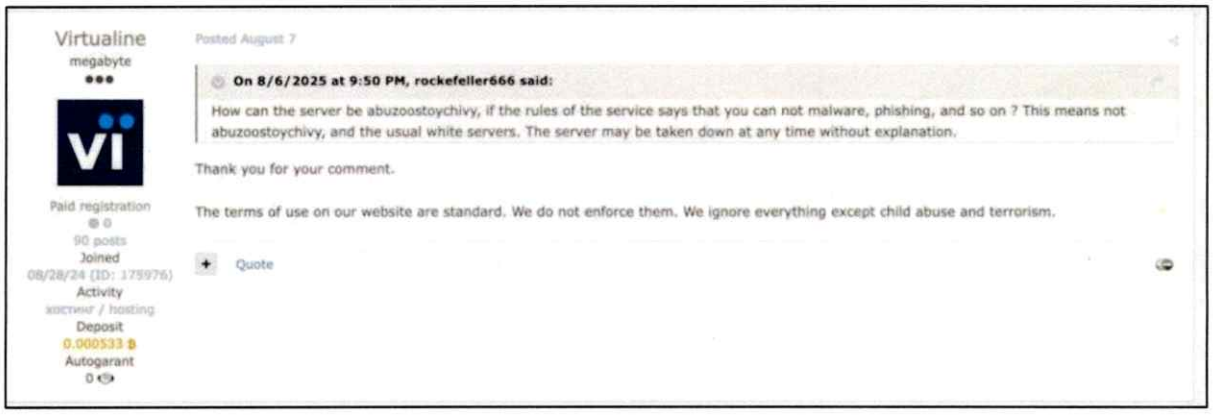


Figure 8. Exploit Screenshot

26. On or about December 19, 2025, an FBI online covert employee (OCE) communicated with a Virtualine operator via **virtualine.net**'s live chat feature. When the operator asked what the use purpose would be for a potential server, the OCE responded that it would be used for "data exfil," which typically indicates the exfiltration of stolen data. The operator then stated, "Yes, it is offshore," "don't worry," "We are doing this business for 3+ years," "You can check our forum threads," "So, if you are not a child porner, we will not sharing any information," and "Of course, we will not kill your server with no warning."

27. On or about June 2025, Virtualine purchased a HackForums thread titled "Virtualine ignored more abuse than your last three therapists."

28. Virtualine also operates, or has in the past operated as, virtualine.org, secury.co, lanedo.net, massgod.com, and spamhouse.net. The moniker "Secury" first advertised the bulletproof hosting service virtualine.net on BlackHatWorld on or about August 15, 2025. The profile icon for "Secury" is the same icon used by the Virtualine Facebook, Exploit.in, and XSS.is accounts. It also matches the first two letters of the logo on virtualine.net.

Figure 14. Logo from virtualine.net

Figure 15. Icon from Online Accounts

29. On or about May 9, 2024, the Virtualine user on BlackHatWorld changed their username from "massgod" to "secury."

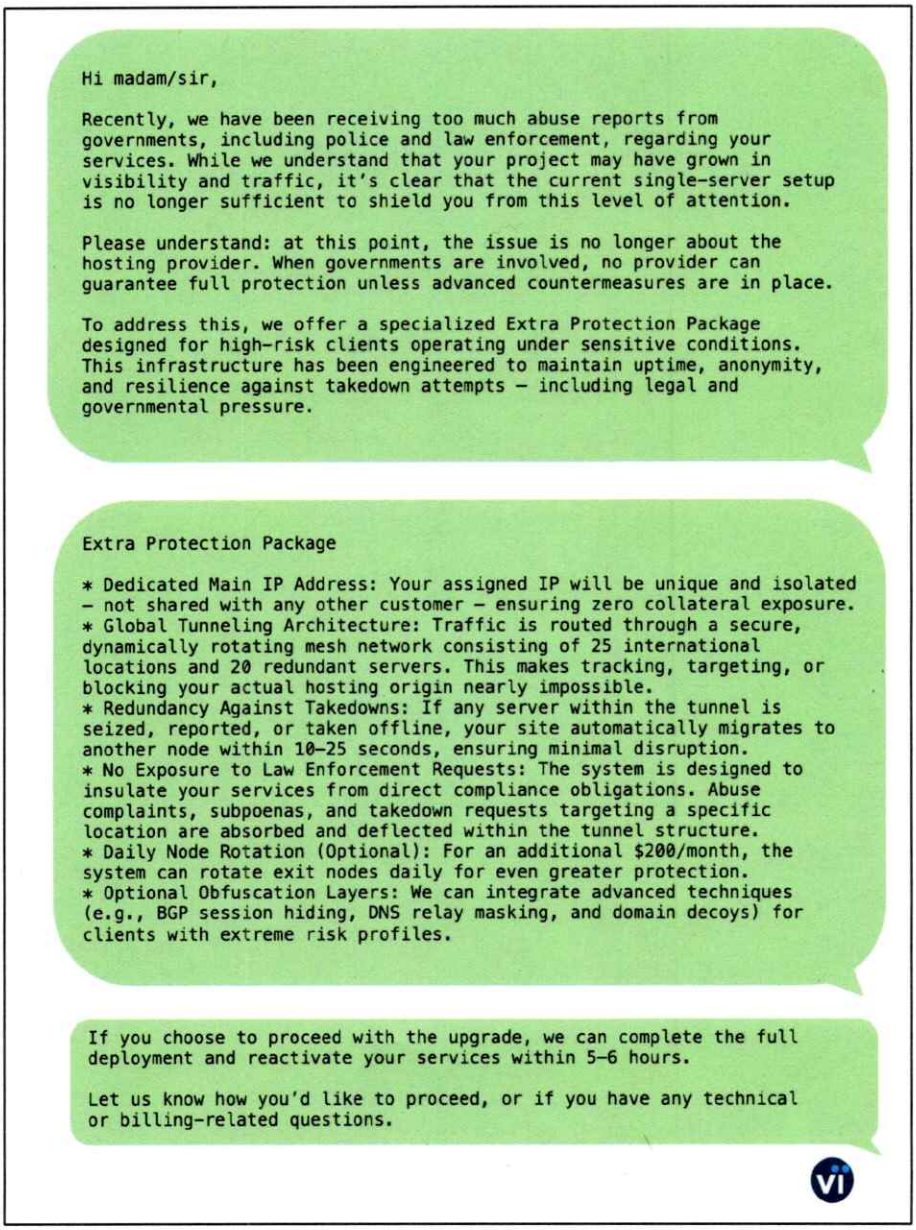
Virtualine Protects Its Criminal Clients From Law Enforcement

30. As of in or about February 2026, Virtualine.net was hosted at 95.216.68.50, a server hosted by Hetzner Online GmbH (Hetzner) located in Germany. The same account that purchased that Hetzner server also owned approximately ten other servers/storage boxes under the same account. The FBI obtained an image of one of the storage boxes at Hetzner, which contained a backup copy of the Virtualine customer database. This database stored information about customers, including emails, invoices, and tickets, as well as information about administrators, including administrator accounts and logs.

31. Through customer tickets, the FBI identified a pattern of protection that Virtualine offered its customers whose abusive or illegal activity drew law enforcement attention:

a. Virtualine receives multiple abuse complaints/law enforcement requests for a domain/IP address of a customer.

b. Virtualine suspends domain/IP address and sends the following message (or a variation of the message) to the customer:

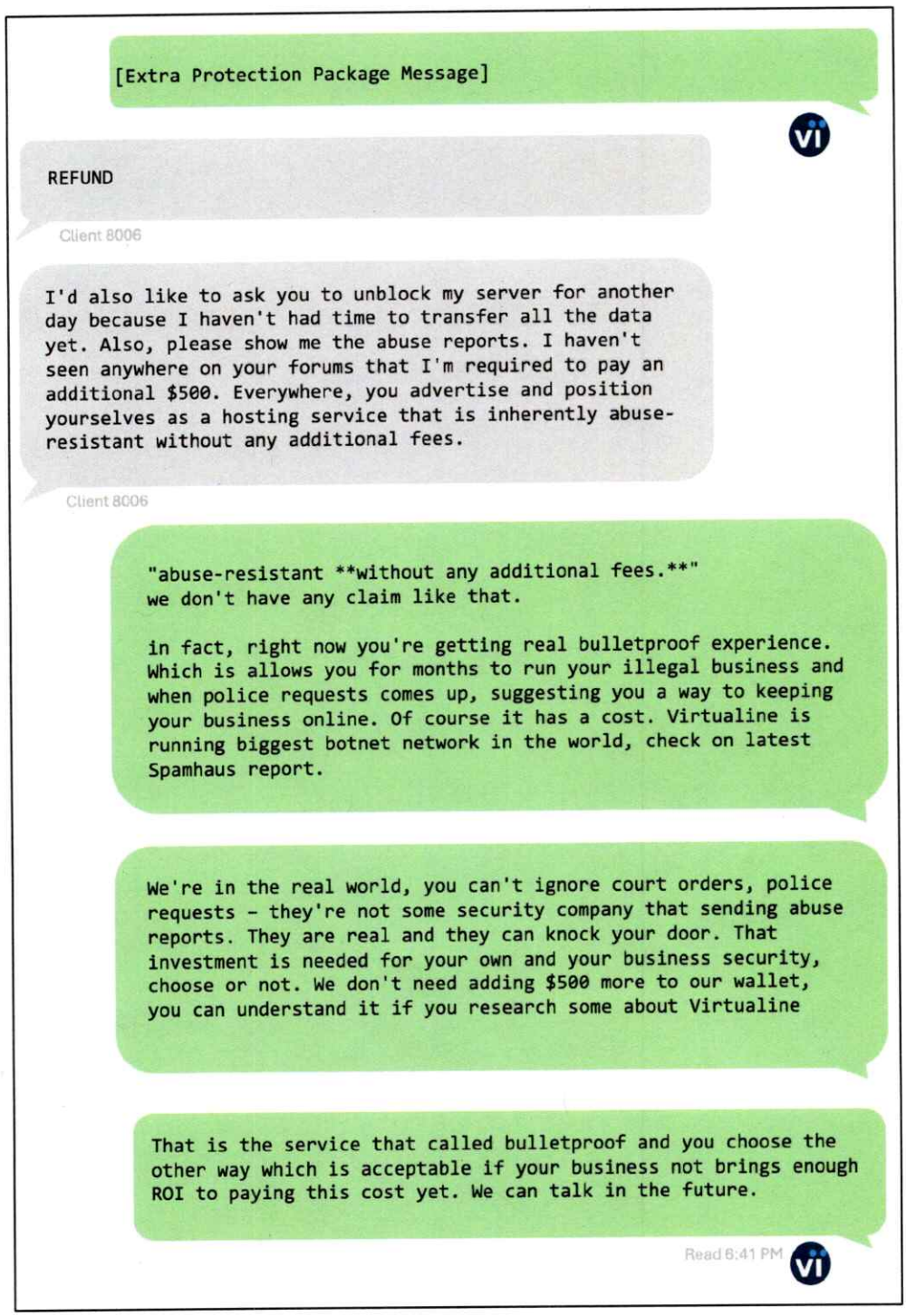


c. The customer either chooses 1) to log back into their server, retrieve any data they might need, and receive a refund for days not used; or 2) to pay $500 to continue operations under the same domain/IP address.

32. Numerous customer tickets depicted this process in action, as seen below.[10] In many of these messages, Virtualine customer support directly addresses law enforcement takedown notices and their approach to allowing their customers to continue to operate, for an extra fee. The messages also indicate that despite abuse reports, once the customer pays the extra fee, their account becomes unsuspended and they once again can use Virtualine services.

[10] Some conversations have been shortened to show the substantive communications between Virtualine and its customers.

[Extra Protection Package Message]
Hello Admin,
Received your message with so much surprise.
A third party accessed my VPS and used it for an abusive activity.
Please i kindly request if I could access the VPS for few mins so i could copy my private files then you can go ahead and suspend it.
Will greatly appreciate your positive feedback!
Client 8782
we allow botnet, Samuel. its just needed extra protection. No need to excuses, of course you can take backups - unsuspended.
Read 9:12 PM



33. Through review of the Virtualine customer database and accounts belonging to Virtualine administrators and associated with Virtualine's operation, FBI identified several

specific criminal schemes that Virtualine directly facilitated through their advanced protection plan.

34. Virtualine sold infrastructure to a client identified as "3571," including IP address 178.16.54.109 on or about May 12, 2025. On or about February 13, 2026, Netcraft[11] sent a takedown request to abuse@omegatech.sc[12] for this IP address for its involvement in malware.

35. On or about March 3, 2026, Virtualine sent a message to client 3571 notifying them of the report and offering its Extra Protection Plan for an extra $500 per month. They also detailed the features of the Extra Protection Plan that the client could expect, should they elect to upgrade their service. One of those features was, "*No Exposure to Law Enforcement Requests: The system is designed to insulate your services from direct compliance obligations. Abuse complaints, subpoenas, and takedown requests targeting a specific location are absorbed and deflected within the tunnel structure." The client elected to pay for the extra protection, and once they notified Virtualine they had made the payment, Virtualine notified them that their account was unsuspended.

Userid	Title	Message Date	Message
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/3/2026 6:56:17 PM	Dear aefef aefef, Recently, we have been receiving too much abuse reports from governments, including police and law enforcement, regarding your services. While we understand that your project may have grown in visibility and traffic, it's clear that the current single-server setup is no longer sufficient to shield you from this level of attention. Following an internal security and risk review, we regret to inform you that we can no longer host this server under its current usage profile within our standard network environment.

[11] Netcraft is a London-based cybersecurity company specializing in cybercrime disruption, automated website takedowns, and digital risk protection.

[12] This email is listed as the public abuse email for Omegatech, a Virtualine company.

			This decision is made to protect the stability and safety of our infrastructure and is final under the current conditions. You may choose one of the following options: — **Option 1 — Refund** We can refund the remaining days of paid amount either: * To your account balance, or * Back to the original payment method. Please confirm your preferred refund method. — **Option 2 — Upgrade to Extra Protection Package** If you wish to continue hosting this project within a segregated and reinforced environment, you may purchase the following protection package in addition to the server price: ``` Extra Protection Package * Dedicated Main IP Address: Your assigned IP will be unique and isolated — not shared with any other customer — ensuring zero collateral exposure. * Global Tunneling Architecture: Traffic is routed through a secure, dynamically rotating mesh network consisting of 25 international locations and 20 redundant servers. This makes tracking, targeting, or blocking your actual hosting origin nearly impossible. * Redundancy Against Takedowns: If any server within the tunnel is seized, reported, or taken offline, your site automatically migrates to another node within 10–25 seconds, ensuring minimal disruption. * No Exposure to Law Enforcement Requests: The system is designed to insulate your services from direct compliance obligations. Abuse complaints, subpoenas, and takedown requests targeting a specific location are absorbed and deflected within the tunnel structure. * Daily Node Rotation (Optional): For an additional $200/month, the system can rotate exit nodes daily for even greater protection. * Optional Obfuscation Layers: We can integrate advanced techniques (e.g., BGP session hiding, DNS relay masking, and domain decoys) for clients with extreme risk profiles. Price: $500/mo (+ server price) ``` If you do not wish to proceed with the protection package, we will not grant further permission for this specific usage purpose within our network. Kindly inform us how you would like to proceed.

			> PLEASE READ: We cannot continue hosting this server without the Extra Protection Plan. This requirement is non-negotiable. Please reply to this ticket with only one of the following words: "REFUND" or "EXTRA PROTECTION". No other responses will be processed. Best regards.
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/4/2026 11:45	EXTRA PROTECTION
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/4/2026 11:49	Hi madam/sir, Forwarded to networking team. We will let you know after confirmation. Kind regards. ---------- Virtualine Support Team
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/4/2026 11:51	will my old ip work after payment again?
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/4/2026 11:57	Hi madam/sir, https://client.virtualine.net/viewinvoice.php?id=44286 same ip will work, upstream will change. We will need 1-3 hours after payment to announce to another upstream. Kind regards. ---------- Virtualine Support Team
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/4/2026 12:10	payment has been made.
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/4/2026 12:13	the reports was from my spam operation, i wont spam anymore. just need my old ip again.
3571	Action Required: Service Continuation Decision (178.16.54.109)	3/4/2026 14:30	Hi madam/sir, Server unsuspended Kind regards. ----------

			Virtualine Support Team
3571	Server was updated, invoice	3/26/2026 9:11	hello, my server got suspended and i had to pay 500$ for it. will i get automaticly invoice to pay again the 500$ or i have todo it manualy asking each time.
3571	Server was updated, invoice	3/26/2026 9:12	Hi madam/sir, No sir, its will be generated with your server invoice automaticly. Kind regards. ---------- Virtualine Support Team

36. Virtualine also sold server space to a client identified as "5270," including IP address 158.94.208.206 on or about September 18, 2025, and IP address 178.16.55.108 on or about December 31, 2025.

37. On or about January 2, 2026, the IP address 158.94.208.206 was used to access without authorization a brokerage services account and conduct buy and sell orders.

38. On or about January 5, 2026, the true owner of the account contacted the brokerage service and reported potential fraud on their account. After investigating the unauthorized access, the brokerage service remitted the funds back to their customer and incurred a loss of $25,800.

39. On or about February 25, 2026, AbuseIPDB.com[13] received reports for IP address 178.16.55.108, indicating the IP address was being used to conduct computer fraud, including web app attacks, brute force SSH, and SQL injections.[14] There were a total of 45 abuse reports

[13] AbuseIPDB is an IP address blacklist for webmasters and system administrators to report IP addresses engaging in abusive behavior on their networks.

[14] An SQL injection is code injection technique where an attacker inserts malicious Structured Query Language (SQL) commands into input fields (such as login forms or search boxes) to manipulate backend database queries

submitted between February 25 and June 8, 2026.

40. On or about March 25, 2026, Virtualine sent a message to client 5270 indicating they had received abuse reports and offering the client their Extra Protection Package. The client opted for the extra protection and their account was unsuspended and upgraded. The next day, Virtualine reached out about the customer's other IP address and offered the same package. The customer asked if they stopped using the server for "harmful reasons," if they still had to pay. Virtualine responded, "if you delete all malware/botnet in it, and guarantee that you won[]t run malware/botnet in this server anymore, we can keep it active. We can re-report current server deleted from customer and now using by different customer." Virtualine continued to host the customer.

userid	title	date	message
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/25/2026 17:28	Dear KingB99 , Recently, we have been receiving too much abuse reports from governments, including police and law enforcement, regarding your services. While we understand that your project may have grown in visibility and traffic, it‚Äôs clear that the current single-server setup is no longer sufficient to shield you from this level of attention. Following an internal security and risk review, we regret to inform you that we can no longer host this server under its current usage profile within our standard network environment. This decision is made to protect the stability and safety of our infrastructure and is final under the current conditions. You may choose one of the following options: ‚àè^a **Option 1 ‚Äî Refund**

			We can refund the remaining days of paid amount either: * To your account balance, or * Back to the original payment method. Please confirm your preferred refund method. ,∏ª **Option 2 ,Äî Upgrade to Extra Protection Package** If you wish to continue hosting this project within a segregated and reinforced environment, you may purchase the following protection package in addition to the server price: ``` Extra Protection Package SAME IP ADDRESS, NOTHING CHANGES ON YOUR SIDE. NO FASTFLUX, NO PROXY-SERVER. EVERYTHING THE SAME, ONLY BGP-SIDE UPSTREAM CHANGES. * Dedicated Main IP Address: Your assigned IP will be unique and isolated ,Äî not shared with any other customer ,Äî ensuring zero collateral exposure. * Global Tunneling Architecture: Traffic is routed through a secure, dynamically rotating mesh network consisting of 25 international locations and 20 redundant servers. This makes tracking, targeting, or blocking your actual hosting origin nearly impossible. * Redundancy Against Takedowns: If any server within the tunnel is seized, reported, or taken offline, your site automatically migrates to another node within 10,Äì25 seconds, ensuring minimal disruption. * No Exposure to Law Enforcement Requests: The system is designed to insulate your services from direct compliance obligations. Abuse complaints, subpoenas, and takedown requests targeting a specific location are absorbed and deflected within the tunnel structure. * Daily Node Rotation (Optional): For an additional $200/month, the system can rotate exit nodes daily for even greater protection. * Optional Obfuscation Layers: We can integrate advanced techniques (e.g., BGP session hiding, DNS relay masking, and domain decoys) for clients with

			extreme risk profiles. Price: $500/mo (+ server price) ``` If you do not wish to proceed with the protection package, we will not grant further permission for this specific usage purpose within our network. Kindly inform us how you would like to proceed. >PLEASE READ: We cannot continue hosting this server without the Extra Protection Plan. This requirement is non-negotiable. Please reply to this ticket with only one of the following words: "REFUND" or "EXTRA PROTECTION". No other responses will be processed. Best regards.
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/25/2026 18:34	i can upgrade but keep everything as it was Option 2 ,Äî Upgrade to Extra Protection Package
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/25/2026 18:47	Hi madam/sir, it will take 25-45minutes to activate server after its paid. https://client.virtualine.net/viewinvoice.php?id=47112&view_as_client=1 please let us know. Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision	3/26/2026 21:07	rdp will back with same ip ?

	(158.94.208.206)		
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/26/2026 21:11	Hi madam/sir, yes same ip Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/26/2026 21:34	invoice has been paid payment id : 4673374524 Invoice #PAID - 38493
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/26/2026 21:41	Hi madam/sir, okay thanks. please allow us 20-25min to announce ip address. Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/26/2026 21:49	ok
5270	Action Required: Service Continuation Decision (158.94.208.206)	3/26/2026 22:16	Hi madam/sir, please check server if all good if not connecting please share server password, we need to configure network in server Kind regards. ---------- Virtualine Support Team

5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 16:40	Dear, Recently, we have been receiving too much abuse reports from governments, including police and law enforcement, regarding your services. While we understand that your project may have grown in visibility and traffic, it‚Äôs clear that the current single-server setup is no longer sufficient to shield you from this level of attention. Following an internal security and risk review, we regret to inform you that we can no longer host this server under its current usage profile within our standard network environment. This decision is made to protect the stability and safety of our infrastructure and is final under the current conditions. You may choose one of the following options: ‚Äì **Option 1 ‚Äì Refund** We can refund the remaining days of paid amount either: * To your account balance, or * Back to the original payment method. Please confirm your preferred refund method. ‚Äì **Option 2 ‚Äì Upgrade to Extra Protection Package** If you wish to continue hosting this project within a segregated and reinforced environment, you may purchase the following protection package in addition to the server price: ``` Extra Protection Package SAME IP ADDRESS, NOTHING CHANGES ON YOUR SIDE. NO FASTFLUX, NO PROXY-SERVER.

			EVERYTHING THE SAME, ONLY BGP-SIDE UPSTREAM CHANGES. * Dedicated Main IP Address: Your assigned IP will be unique and isolated ,Äî not shared with any other customer ,Äî ensuring zero collateral exposure. * Global Tunneling Architecture: Traffic is routed through a secure, dynamically rotating mesh network consisting of 25 international locations and 20 redundant servers. This makes tracking, targeting, or blocking your actual hosting origin nearly impossible. * Redundancy Against Takedowns: If any server within the tunnel is seized, reported, or taken offline, your site automatically migrates to another node within 10,Äì25 seconds, ensuring minimal disruption. * No Exposure to Law Enforcement Requests: The system is designed to insulate your services from direct compliance obligations. Abuse complaints, subpoenas, and takedown requests targeting a specific location are absorbed and deflected within the tunnel structure. * Daily Node Rotation (Optional): For an additional $200/month, the system can rotate exit nodes daily for even greater protection. * Optional Obfuscation Layers: We can integrate advanced techniques (e.g., BGP session hiding, DNS relay masking, and domain decoys) for clients with extreme risk profiles. Price: $500/mo (+ server price) ``` If you do not wish to proceed with the protection package, we will not grant further permission for this specific usage purpose within our network. Kindly inform us how you would like to proceed. >PLEASE READ: We cannot continue hosting this server without the Extra Protection Plan. This requirement is non-negotiable. Please reply to this ticket with only one of the following words: "REFUND" or "EXTRA

			PROTECTION". No other responses will be processed. Best regards.
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 19:48	I want option 2 but would I loose all my files ??
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 20:05	Hi madam/sir, no, all data and everything will stay same. we will just change isp connection, will take about 20min. https://client.virtualine.net/viewinvoice.php?id=47276&view_as_client=1 let us know after its paid Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 21:40	How much does it cost
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 21:42	Hi madam/sir, its same $500, you just paid for 158-94-208-206.virtualine.org if you need it for 178-16-55-108.virtualine.org as well, let me know so i will create support ticket to datacenter for 2 ip address Kind regards. ---------- Virtualine Support Team

5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 21:48	no just get this rdp back fast plz
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 21:48	158-94-208-206 this
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/26/2026 21:49	Hi madam/sir, ok, got it Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/27/2026 0:34	This 178-16-55-108 if I pay 500$ does that mean I only have to renew normal again or I keep paying 500$ +
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/27/2026 1:20	Hi madam/sir, Its monthly fee, not one time. Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/27/2026 16:10	This 500$ is too much damn so in a month I would be paying 545$??

5270	Action Required: Service Continuation Decision (178.16.55.108)	3/27/2026 17:30	Hi madam/sir, that is correct. Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 4:48	Can I get all my data from the rdp ?
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 6:38	Hi madam/sir, yes, let us know when you're here we can unsuspend it for an hour. you can transfer data to your 158-94-208-206.virtualine.org adn use it. Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 6:40	Thanks
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 6:42	Hi madam/sir, unsuspended Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 6:45	What if I promise not to use it for the harmful reasons again ?

5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 6:58	Hi madam/sir, if you delete all malware/botnet in it, and gurantee that you won't run malware/botnet in this server anymore, we can keep it active. We can re-report current server deleted from customer and now using by different customer. But if you run same things in it, it will put our network in risk and we might need to terminate your account without any warning. Kind regards. ---------- Virtualine Support Team
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 6:59	Yes I won't run them again
5270	Action Required: Service Continuation Decision (178.16.55.108)	3/28/2026 7:05	Hi madam/sir, okay, we can keep it active. Kind regards. ---------- Virtualine Support Team

SUBJECT OFFENSES

41. Based on a review of Virtualine's customer database, on or about November 19, 2025, VENDOR 1[15] created an account with Virtualine. VENDOR 1 is a criminal online forum that allows users to post and sell access to nude, sexual suggestive, and/or sexually explicit images and videos of minors and adults. VENDOR 1 also promotes a hack-for-hire service in which users can pay hackers to access victims' online accounts without their consent and illicitly obtain explicit images and videos.

[15] The true name of VENDOR 1 is known to law enforcement.

42. On or about November 19, 2025, VENDOR 1 created an account with Virtualine. On or about December 15, 2025, Virtualine assigned the IP address 91.92.240.239 to VENDOR 1. On or about January 22, 2026, Virtualine started receiving notifications that VENDOR 1 was using 91.92.240.239 to store sexually explicit images and videos of minors.

43. On or about January 22, 2026, the German police notified Virtualine at abuse@omegatech.sc with the subject "Abuse content on your service." The report included the following information:

Hotline unique report number: P830
Reason code: Child sexual abuse material (minor under 18 in a sexual context)
Violation: Art 184b/c German Criminal Code
IP Address: 91.92.240.239
Date/time Assessed: 22.1.2026
URL(s): https://[VENDOR 1].pk[REDACTED]/
https://[VENDOR 1].pk/[REDACTED]

44. On or about February 1, 2026, a victim's attorney emailed contact@omegatech.sc with the subject line: "Notice of Illegal and Harmful Content." The email included the following:

To Whom it May Concern:

This firm is counsel to [REDACTED] (the "Client"). We are writing on behalf of our Client concerning the presence of illegal and harmful content appearing on your website "[VENDOR 1].pk". "[VENDOR 1].pk" currently has pornographic content depicting a minor in violation of United States Federal Law Title 18 U.S.C. Â§ 2252, a federal law that prohibits the production, distribution, reception, and possession of an image of child pornography using or affecting any means or facility of interstate or foreign commerce. Location of this content can be found at the URLs listed below:

45. As a result, on or about February 2, 2026, a Virtualine administrator visited the URLs listed in the email. On or about March 19, 2026, VENDOR 1 still offered this collection on their website.

46. On or about February 4, 2026, the eSafetyCommissioner in Australia wrote to advise abuse@omegatech.sc as follows:

Dear Omegatech Ltd,

The eSafety Commissioner is responsible for improving and promoting online safety for Australians and administering a complaints system for certain types of harmful online material.

For more information about eSafety's role and functions, please refer to our website *and the Online Safety Act 2021 (Cth) (the* ***Act****).*

Why we are writing to you

eSafety has received a complaint about material that appears to be on a service for which you are the hosting service provider. The complaint is about material located at the following URL's (the ***Material****):*

https://[VENDOR 1].pk/[*REDACTED]*

In summary, the complaint is in relation to non-consensual intimate images available on the above website. The material includes sexually explicit images and videos of the victim, who was aged under 18 years when much of the material was created (and would therefore be considered child sexual abuse material under Australian laws - ***CSAM****). eSafety report IBA-2025-0718309 relates.*

This letter is notifying you that the Material may be in breach of your terms of service/rules/policies/standards etc.

47. On or about February 5, 2026, the U.S. National Center for Missing and Exploited Children emailed abuse@omegatech.sc to advise of its "2nd attempt" to contact Virtualine about particular child sexual abuse material:

This is the 2nd attempt to come in contact with you pertaining to alleged child sexual abuse material or text on your service.

The National Center for Missing & Exploited Children's CyberTipline was made aware that alleged child sexual abuse material may be depicted on your service. NCMEC is providing you with the reported URL of the alleged child sexual abuse material. Please review the reported URL to determine if it contains content that may violate federal and/or state law or your Terms of Service, or Member Services Agreement, or Community Guidelines or Standards.

The URL:

https://[VENDOR 1].pk/shop/[REDACTED] /

Please review the reported URL to determine if it contains content that may violate your Terms of Service, or Member Services Agreement, or Community Guidelines or Standards.

The CyberTipline was created by NCMEC to provide an online mechanism for members of the public and electronic service providers to report incidents of suspected child sexual exploitation

including online enticement of children for sexual acts, child sexual molestation, child sexual abuse material (child pornography), child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the Internet.

As an electronic service provider you have the ability to register with the CyberTipline in order to access a separate, secure reporting form reserved for companies. Reporting through the ESP form allows you to receive a confirmation receipt indicating a report was successfully submitted for your records, and also allows for any uploaded files to be submitted with the incident information. The registration process is fairly simple and entails providing us with basic information regarding your platform. Please contact ESPteam@NCMEC.org to request more details if you are interested in registering.

You may also visit https://www.missingkids.org/theissues/csam and https://www.missingkids.org/gethelpnow/cybertipline for more information.

48. On or about February 11, 2026, and then again on or about February 15, 2026, Cybertip.ca[16] sent notices to abuse@omegatech.sc with the subject "Notice and takedown request (CSAM)" advising of sexually explicit images of the same individual flagged by NCMEC in its February 5, 2025, email to Virtualine. On or about February 16, 2026, abuse@omegatech.sc responded that the "content was already removed."

49. On or about February 11, 2026, NCMEC emailed abuse@omegatech.sc with the subject line "4th Notice of Possible Child Sexual Abuse Material on Your Service."

50. On or about February 12, 2026, Cybertip.ca sent another notice to Virtualine with the subject "Notice Pertaining to Sexual, Harmful and/or Abusive Material of a Child."

51. On or about February 15, 2026, Cybertip.ca sent another "Notice Pertaining to Sexual, Harmful and/or Abusive Material of a Child." On or about February 16, 2026, Virtualine responded, "Hello, Content is not related about childs or under 18 years age, its false report. Kind regards."

52. Cybertip.ca sent continual warnings to Virtualine, stating that it had "become

[16] Cybertip.ca is Canada's version of NCMEC.

aware of content depicted on your service that is sexual, harmful and/or abuse of someone we believe to be a child." In all, these emails were sent to abuse@omegatech.sc on or about February 11, 12, 15, 20, and 23.

53. From on or about February 2 to 11, 2026, NCMEC sent six emails to abuse@omegatech.sc regarding various URLs containing sexually explicit images of minors on the VENDOR 1.pk domain.

54. The FBI identified communications between VENDOR 1 and Virtualine that took place on an encrypted application. In those communications, Virtualine assisted VENDOR 1 with infrastructure development, including creating a sandbox[17] for the VENDOR 1.cc website on Virtualine infrastructure to allow the VENDOR 1 administrator to test changes to website. Virtualine also discussed the creation of a new project for VENDOR 1 called "[UPLOAD SERVICE 1].net."[18] These conversations included price negotiations for development fees for both projects.

55. Additionally, VENDOR 1 told Virtualine about legal action from the lawyers of the same victim mentioned in the abuse complaint Virtualine received on February 1, 2026.

56. Virtualine directed VENDOR 1 to upload files to UPLOAD SERVICE 1 in order to test the new website's capabilities. In April 2026, VENDOR 1 announced that the service would no longer be using Mega to upload and download files and was instead switching to a site called UPLOAD SERVICE 1, which is a site that resolves to Virtualine Technologies.

57. On or about July 17, 2026, NCMEC sent an abuse report to abuse@virtualine.org

---

[17] A sandbox environment for a website is a common way to test new changes to a site without affecting the contents or the availability of the original site.

[18] The true name of UPLOAD SERVICE 1 is known to law enforcement.

for UPLOAD SERVICE 1.net. As of on or about August 19, 2026, NCMEC had not received any responses from Virtualine.

58. According to WHOIS records, the site hosting VENDOR 1.pk was first seen hosted by Virtualine January 8, 2026, and last seen on May 26, 2026. According to Virtualine customer records, the same customer (6571) actively owned the IP address 91.92.240.239 as of July 15, 2026, even though the VENDOR 1 site is no longer hosted by Virtualine. As of September 2026, Virtualine continues to host UPLOAD SERVICE 1.net. Additionally, the VENDOR 1 Virtualine account is still active, owning/operating at least six Virtualine servers as of July 2026.

59. Messages from an encrypted messaging platform dated on or about June 3, 2026, showed Virtualine confronting VENDOR 1 about the presence of CSAM on their site, specifically of pre-pubescent children, in which VENDOR 1 denied knowledge of the content. Despite the confrontation with VENDOR 1 and the abuse complaints received by various entities, VENDOR 1 maintained an account with Virtualine and continued to use Virtualine's infrastructure. On or about June 5, 2026, VENDOR 1 paid Virtualine approximately $10,000 to Virtualine's no-AML payment option to continue using Virtualine's services.

60. Beginning in or around September 2025, UPLOAD SERVICE 1 was sporadically accessible and inaccessible to users. Regardless of its availability status, as of October 2026, UPLOAD SERVICE 1 still resolved to a Virtualine IP address owned by the VENDOR 1 Virtualine account. Additional encrypted messages between VENDOR 1 and Virtualine were identified in which Virtualine told VENDOR 1 that no "cp" was allowed and requested it be taken down.[19] The last identified payment VENDOR 1 sent to Virtualine was in or about August

[19] The timestamps of these messages are unknown.

2026.

61. In all, while the current relationship between VENDOR 1 and Virtualine is unknown, numerous abuse reports and explicit conversations about the presence of CSAM on VENDOR 1.pk occurred over the span of at least six months, during which Virtualine continued to allow VENDOR 1 to maintain their account and infrastructure with Virtualine.

VIRTUALINE ENGAGES IN A CONCEALMENT MONEY LAUNDERING CONSPIRACY

62. Through analysis of the funds received by Virtualine from their customers, there is probable cause to believe that at least a portion of the funds held by Virtualine are traceable, via direct or circumstantial evidence, to Virtualine customers engaging in criminal activity including violations of 18 U.S.C. §§ 1030 (computer fraud and abuse), 2251(d)/(e) (advertisement of sexually explicit images of minors), 371 (conspiracy), and 1343 (wire fraud).

63. Based on the facts and circumstances set forth below, I further submit that there exists probable cause to believe that all the funds held by Virtualine were involved in, or are traceable to funds involved in, concealment money laundering offenses committed in violation of 18 U.S.C. § 1956(a)(1)(B)(i), international promotional money laundering offenses committed in violation of 18 U.S.C. § 1956(a)(2)(A), and conspiracy to engage in concealment money laundering offenses committed in violation of 18 U.S.C. § 1956(h).

64. There is also probable cause to believe that the **Virtualine.net** facilitates the laundering of those funds and is therefore subject to civil and criminal forfeiture pursuant to 18 U.S.C. §§ 982(a)(1) and 981(a)(1)(A).

65. Virtualine has routinely offered at least three payment options for its services on **Virtualine.net**: Credit/Bank cards (processed by Stripe), "crypto payment" (processed by Virtual

Asset Payment Processors[20] (VAPPs)), and "BTC [NO-AML]." NO-AML refers to no Anti-Money Laundering – rules and procedures used by financial institutions to prevent and limit the laundering of criminal proceeds. Based on my training and experience and knowledge of Virtualine operations, they likely offer this option so that criminal organizations paying for their services can utilize proceeds of their illicit activity to pay for their Virtualine account, without fear that a VAPP or a traditional bank or financial institution will block payment or freeze their account. FBI analysis determined that the addresses used by Virtualine for the "BTC [NO-AML]" payment option were unhosted and controlled by the operators of Virtualine. From in or around August 2023 to present, Virtualine has used at least five different addresses for its NO-AML payment option (hereafter "NO-AML addresses"). Prior to August 2025, the NO-AML address remained consistent; however, starting in or around August 2025, the address used for the NO-AML payment option changed every few months, likely as an operational security measure. The addresses for payment were consistently listed on Virtualine's homepage, **Virtualine.net**.

66. By reviewing records provided by the VAPPs used by Virtualine, information obtained from the above-referenced Virtualine customer database, publicly-available blockchain information, and information from other criminal investigations, investigators were able to correlate multiple payments to the same Virtualine customer account and then attribute those accounts to particular criminal activity. Investigators were also able to identify addresses

---

[20] VAPPs enable online merchants and service providers to accept payments from customers using virtual assets without needing to operate their own payment infrastructure. VAPPs generate payment addresses, receive customer payments, and give merchants options on how to receive proceeds. VAPPs can support hundreds of different virtual assets, with the merchant often able to convert and withdraw proceeds in their preferred format. VAPPs typically collect a commission for each processed payment.

controlled by the Virtualine actors to receive payments, from both the "BTC [NO-AML]" payment option or from Virtualine merchant accounts at the VAPPs.

67. As of in or around July 2026, the Virtualine customer database contained records for at least 7,950 customer accounts and nearly 34,000 invoices marked as paid between at least July 2023 and July 2026. Due to the volume of accounts and payments, at least 28,500 of which were made using cryptocurrency, analysis is ongoing, but to date several accounts and their corresponding invoice payments have been attributed to criminal actors.

68. For example, investigators identified Bitcoin clusters controlled by VENDOR 1 that were used to receive payments from VENDOR 1 customers. When analyzing these clusters, payments from VENDOR 1 to the Virtualine NO-AML addresses were identified between at least December 2025 and August 2026. Comparison of these payments against the Virtualine customer database revealed they were associated with a Virtualine account attributed to VENDOR 1 which had been active since at least November 2025.

69. Between payments directly to the Virtualine NO-AML addresses and to the VAPPs used by Virtualine, VENDOR 1 paid at least $105,000 to Virtualine between at least November 2025 and August 2026.

70. Investigators also traced ransom payments from victims of ransomware and found that portions of several ransom payments that were paid to ransomware groups in cryptocurrency ultimately were used to pay for Virtualine services.

71. Once Virtualine received payment, either through the "BTC [NO-AML]" payment option or through their VAPP accounts, Virtualine administrators took additional steps to further conceal the source of their customers' payments.

72. Prior to February 2026, Virtualine payments to the BTC [NO-AML] addresses or

to Virtualine's VAPP accounts were sent to accounts at cryptocurrency exchanges. From those accounts, the funds would then be swapped into other types of cryptocurrency and further sent along through other unhosted addresses. Each transfer of funds incurs network or transaction fees for each transaction. Movement through various unhosted addresses in rapid succession and conversion from one stablecoin to another is indicative of efforts to conceal illicit proceeds.

73. Beginning in or around February 2026, rather than transferring Virtualine proceeds directly to cryptocurrency exchanges, the Virtualine operators concealed the true source of their cryptocurrency and used decentralized cross-chain bridges to anonymously exchange Bitcoin from the NO-AML addresses for other virtual currencies and used unhosted wallet addresses to receive proceeds from their account at a particular VAPP. While some of the transactions conducted using these cross-chain bridges can be traced and identified by law enforcement personnel with the appropriate training and experience, use of cross-chain bridges has been identified as a favored technique for the speedy exchange of virtual currencies by a variety of criminal actors in order to conceal and obfuscate their origin from virtual currency exchanges and to slow or disrupt law enforcement tracing.

74. In March, April, May, and June 2026, Virtualine used at least three different cross-chain bridges to exchange their NO-AML Bitcoin for other virtual currencies.

75. In addition to using cross-chain bridges, Virtualine administrators used other methods to conceal the origins of their illicit proceeds. They swapped some of the proceeds from USDT, a type of stablecoin cryptocurrency that has a value pegged to the U.S. dollar that can be frozen and seized by U.S. law enforcement, to DAI, another stablecoin that cannot be seized in the same manner. They also routinely sent proceeds in rapid succession through multiple unhosted wallet addresses, a strategy which incurs additional transactions fees for each

transfer and has no financial benefit.

76. Based on my training and experience, I know that criminals often conduct an otherwise unnecessary and costly number of transactions to transfer criminal proceeds via layered transactions designed to conceal or disguise the nature, location, source, ownership, or control of those proceeds. The large number of rapid transfers described above – which have no apparent legitimate purpose– indicate that these funds were transacted in a way designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity.

THE SUBJECT DOMAIN NAME

77. Virtualine uses the website **virtualine.net** to advertise and sell its "bulletproof" servers to customers to be used for illegal activity without adherence to law enforcement requests. On the website, Virtualine states that its servers are "protected by design" and that "your servers stay private – by policy and by jurisdiction."

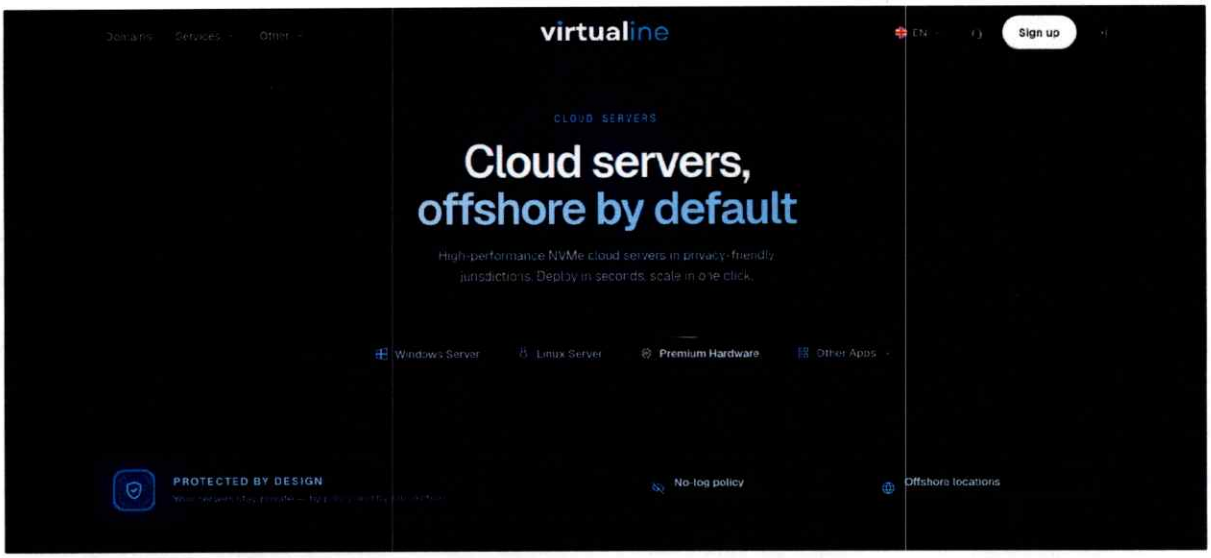


Figure 8. Virtualine.net Page

78. **Virtualine.net** also displays the different services available for purchase, allows

the website visitor to view more information about a product, and also allows a visitor to ask questions via a "live chat" feature.

Figure 9. Virtualine.net Offered Services

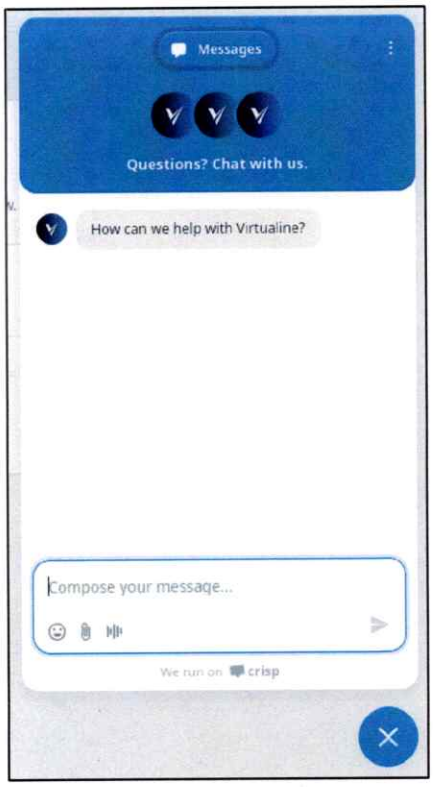


Figure 10. Virtualine.net Live Chat Feature

79. Additionally, the website allows a customer to add items to a cart and complete a purchase through a variety of payment options on the site.

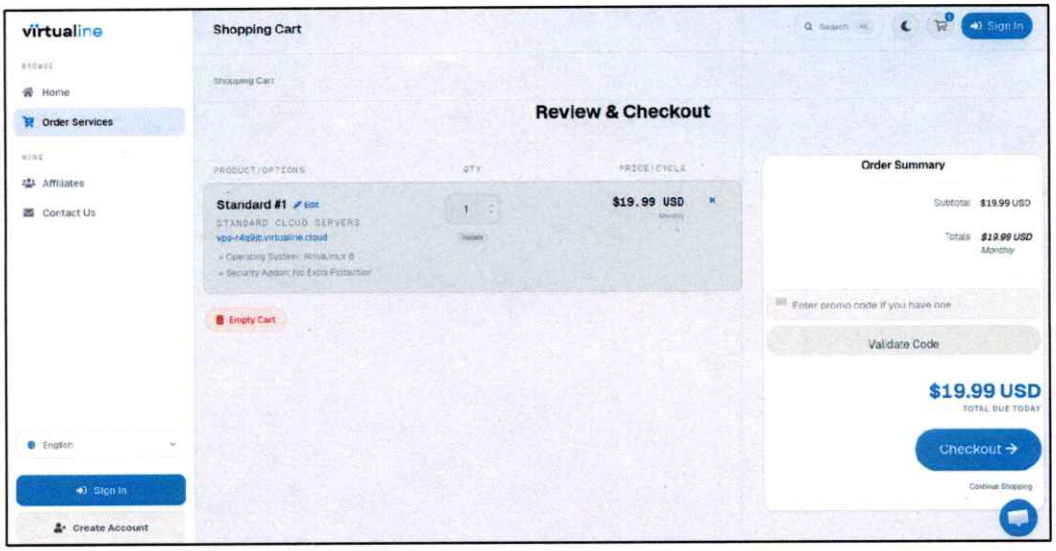


Figure 11. Virtualine.net Checkout

80. Once logged in, the customer has the options to manage purchases services, view invoices, create new support tickets, and order additional services.

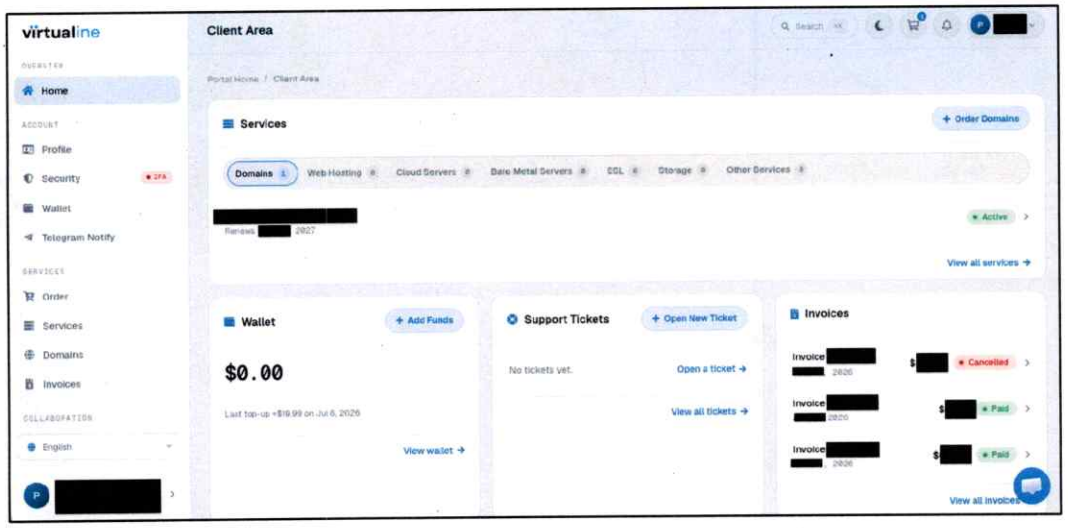


Figure 12. **Virtualine.net** Client Portal

81. A search of publicly available WHOIS domain name registration records revealed that the **virtualine.net** was registered through the registrar CNOBIN INFORMATION TECHNOLOGY LIMITED ("Cnobin"), which has its headquarters at Hong Kong, China. The publicly available WHOIS database lists the registrant of the **virtualine.net** as "REDACTED FOR PRIVACY." Cnobin is an entity that allows website owners to keep their contact details private during the domain name registration process.

82. The top-level domain for **virtualine.net** is Verisign. Verisign currently manages all ".net" domains.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

83. Title 18, United States Code, Section 2253(a) authorizes seizure of property subject to criminal forfeiture of a person convicted of an offense under Chapter 110 involving a visual depiction described in, among others, section 2251. Such property includes any property used or intended to be used to commit or to promote the commission of such an offense.

84. Title 18, United States Code, Section 2254 authorizes the civil forfeiture of any property subject to forfeiture pursuant to Title 18, United States Code, Section 2253.

85. Title 47, United States Code, Section 223(h)(7) similarly authorizes seizure of property subject to criminal forfeiture of a person convicted of an offense under section 223(2) or (3). Such property includes any property used or intended to be used, in any manner or part, to commit or to facilitate the commission of the violation.

86. Pursuant to 18 U.S.C. §§ 982(a)(1) and 981(a)(1)(A), any property, real or personal, which was involved in a violation of 18 U.S.C. § 1956, is subject to criminal and civil forfeiture. Assets "involved in" a violation include the corpus of the offense, any funds laundered, any proceeds, and any property facilitating the offense. *United States v. Miller*, 295 F.Supp.3d 690, 697 (E.D.Va. 2018) (collecting cases), *aff'd*, 911 F.3d 229 (4th Cir. 2018).

87. Title 18, United States Code, Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

88. Title 18, United States Code, Section 982(b)(1) authorizes the issuance of a criminal seizure warrant under Title 21, United States Code, Section 853(f) which provides in relevant part that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture.

89. Neither a restraining order nor an injunction is sufficient to guarantee the availability of **Virtualine.net** for forfeiture. By seizing **Virtualine.net** and redirecting it to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the **Virtualine.net** will prevent third parties from continuing to access the **Virtualine.net** website in its present form.

90. Title 18, United States Code, Section 981(h) provides that venue for civil forfeitures brought under this section lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought.

91. Title 21, United States Code, Section 853(l), which is made applicable to criminal forfeiture under 47 U.S.C. § 223(h)(7)(B) and 18 U.S.C. §§ 2253(b), 982(b)(1), provides that U.S. district courts shall have jurisdiction to enter orders without regard to the location of any property which may be subject to forfeiture. Venue for criminal forfeitures lies in the district where the criminal prosecution may be brought.

92. As set forth above, there is probable cause to believe that **Virtualine.net** is subject to civil and criminal forfeiture because it was used in the commission of violations of **Virtualine.net**. Specifically, **Virtualine.net** was involved in, enabled, and facilitate, among others, the criminal activity committed by VENDOR 1, which were conducted in violation of Title 18, U.S. Code, Section 2251(d)/(e) (advertising, conspiracy to advertise, and conspiracy to aid and abet advertising of sexually explicit images of minors) and Title 47, U.S. Code, Section 223(h) (intentional disclosure of nonconsensual intimate visual depictions of adults and minors).

SEIZURE PROCEDURE

93. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the top-level domain, Verisign, headquartered at 12061 Bluemont Way, Reston, VA 20190

shall be directed to restrain and lock **Virtualine.net** pending transfer of all right, title, and interest in **Virtualine.net** to the United States upon completion of forfeiture proceedings, to ensure that changes to **Virtualine.net** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ.

94. In addition, upon seizure of **Virtualine.net** by the FBI, Verisign will be directed to associate **Virtualine.net** to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which **Virtualine.net** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

95. For the foregoing reasons, I submit that there is probable cause to believe that **Virtaline.net** is used in and/or intended to be used in facilitating Title 18, U.S. Code, Section 2251(d)/(e) (advertising, conspiracy to advertise, and conspiracy to aid and abet advertising of sexually explicit images of minors); Title 47, U.S. Code, Section 223(h) (intentional disclosure of nonconsensual intimate visual depictions of adults and minors); and Title 18, United States Code, Sectio 1956 (concealment and international promotion money laundering). Accordingly, **Virtualin.net** is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 982(a)(1), 981(a)(1)(A), 2253(a)(1), (3), 2254 and 47 U.S.C. § 223(h)(7)(A)(i), (iii), and I respectfully request that the Court issue a seizure warrant for **Virtualine.net**.

96. Because the warrant will be served on **Verisign**, which controls **Virtualine.net**, and **Verisign** thereafter, at a time convenient to it, will transfer control of **Virtualine.net** to the government, there exists reasonable cause to permit the execution of the requested warrant at any

time in the day or night.

Respectfully submitted,

Caroline Moolenaar
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me on this 22nd day of October, 2026.

William E. Fitzpatrick
United States Magistrate Judge

ATTACHMENT A

With respect to "**virtualine.net**" ("SUBJECT DOMAIN NAME"), **Verisign**, which is the domain registry of the SUBJECT DOMAIN NAME, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAME:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation by associating the SUBJECT DOMAIN NAME to the following authoritative name-server(s):
    (a) ns1.fbi.seized.gov;
    (b) ns2.fbi.seized.gov; and/or
    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Verisign;
2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAME pending transfer of all right, title, and interest in SUBJECT DOMAIN NAME to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAME cannot be made absent court order or, if forfeited to the United States, without prior consultation with the **FBI**.
3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN NAME will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"Virtualine.net has been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Virginia as part of a joint law enforcement action involving the partners listed below."