FBI FLASH
ACTIONABLE CYBER INTELLIGENCE
21 May 2026
FLASH Number
FLASH-20260521-001

“First VPN Service” Used by Ransomware Actors to Compromise Systems

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate indicators of compromise (IOCs) and identified tactics, techniques, and procedures (TTPs) associated with the First VPN Service. The service has been active since approximately 2014 and currently provides 32 exit node servers in 27 countries. At least 25 ransomware groups, such as Avaddon Ransomware, have used First VPN Service infrastructure to perform network reconnaissance and intrusions. First VPN Service IP addresses have been used for scanning activity, botnets, denial of service attacks, scams, and hacking. First VPN Service was almost exclusively advertised in known criminal dark web forums such as Exploit[.]in and XSS[.]is, two of the most prominent Russian-language online forums which provide marketplaces for cyber criminals to buy and sell unauthorized access to computer systems, stolen personal identifying information, hacking tools, and contraband.

This reporting applies solely to the First VPN Service and does not extend to other VPN providers with similar naming.

The release of this FLASH follows the coordinated takedown of the First VPN Service through a joint law enforcement operation supported by the FBI. This operation was conducted by France’s Direction Régionale de la Police Judiciaire Brigade de Lutte Contre la Cybercriminalité (BL2C), and the Dutch National Police, National High Tech Crime Unit (NHTC), with assistance from Ukraine, the United Kingdom, Switzerland, and Luxembourg.

Technical Details

First VPN Service's website was accessible at `1vpns[.]com`, `1vpns[.]org`, and `1vpns[.]net`, as well as an onion service accessible via the Tor Network. First VPN Service also hosted a Jabber server at `1jabber[.]com`. As of April 2026, First VPN Service offered a range of pricing options and included approximately 32 servers, known as "nodes," in approximately 27 countries for users to choose from. Some of the subscription options allowed users to select up to four different nodes to increase anonymity online. There were three US-based exit nodes, `92.223.66[.]103`, `5.181.234[.]59`, and `92.38.148[.]58`. First VPN Service offered subscription durations ranging from one day to one year, with users paying for the service in cryptocurrency.

First VPN Service offered several connection protocols including OpenConnect, WireGuard, Outline, and VLess TCP Reality, and multiple encryption options including OpenVPN ECC, L2TP/IPSec, and PPtP. Technical support was also offered to users via a self-hosted Jabber server and Telegram encrypted messaging service. Among the VPN protocol options, First VPN Service offered "VLESS" and "Reality" which provides the ability to disguise VPN Internet traffic as HTTPS traffic over ports which are commonly used to connect to websites.

Indicators

The FBI recognizes that malicious infrastructure may be hosted on cloud or virtualized platforms where IP addresses are dynamically or ephemerally assigned. As a result, addresses associated with malicious activity may later be reassigned to non-malicious services. These indicators should therefore be interpreted as historically observed infrastructure within the identified activity window and corroborated with current network telemetry or additional intelligence sources. The IP addresses listed below were assessed to be statically assigned to the First VPN Service at the time they were originally observed.

Domains	
1vpns[.]com	1vpns[.]org
1vpns[.]net	1jabber[.]com

Communication Account	**Description**
support@1vpns[.]com	Jabber
1vpns@1jabber[.]com	Jabber
@FVPNS	Telegram
https://t[.]me/FirstVPNService	Telegram
support@1vpns[.]com	Email
82822222	ICQ

Current IPs (As of May 2026)		
92.38.180[.]39	195.206.107[.]203	178.175.139[.]203
37.120.143[.]203	91.232.29[.]114	86.105.25[.]219
134.255.210[.]160	190.97.163[.]88	193.106.31[.]98
82.146.50[.]52	185.247.71[.]107	51.79.208[.]134
92.38.162[.]4	77.246.157[.]26	54.37.200[.]68
185.253.98[.]243	51.79.111[.]220	188.92.78[.]242
51.75.34[.]158	92.223.66[.]103	46.105.79[.]45

92.38.186[.]86	82.202.160[.]36	92.38.148[.]58
193.239.86[.]19	139.99.255[.]144	91.193.5[.]91
5.181.234[.]59	91.132.139[.]67	95.213.164[.]12
89.38.224[.]3	77.83.247[.]81	152.89.162[.]139

Historical IPs (Prior to May 2026)		
31.135.14[.]182	94.23.27[.]208	134.255.210[.]26
31.210.70[.]184	94.242.253[.]11	178.209.51[.]234
31.210.70[.]186	94.242.253[.]13	179.43.184[.]22
31.210.70[.]190	94.242.254[.]43	185.128.43[.]54
139.99.68[.]157	94.242.254[.]54	185.178.209[.]193
37.235.55[.]113	94.242.254[.]8	185.184.192[.]108
37.235.60[.]141	94.26.226[.]75	145.239.5[.]30
152.89.162[.]138	95.141.32[.]237	185.253.98[.]242
46.148.16[.]138	95.213.164[.]11	185.65.205[.]82
49.12.133[.]165	95.215.61[.]192	188.126.79[.]82
49.50.66[.]72	95.216.15[.]11	188.127.244[.]3
5.135.164[.]8	95.216.15[.]25	188.165.236[.]151
5.181.234[.]56	103.16.26[.]135	188.227.173[.]198
5.181.234[.]58	103.16.26[.]229	188.40.81[.]84
5.188.163[.]34	103.16.27[.]96	188.42.253[.]16
51.38.66[.]162	108.59.1[.]133	190.123.46[.]11
178.175.139[.]202	111.90.141[.]47	190.2.142[.]25
185.247.71[.]106	111.90.158[.]72	190.2.142[.]28
190.97.163[.]213	139.99.122[.]162	190.97.163[.]117
62.112.8[.]202	139.99.149[.]85	190.97.163[.]142
77.83.247[.]80	193.239.86[.]18	192.71.211[.]77
80.90.39[.]95	147.135.11[.]223	192.71.249[.]70
80.90.55[.]44	147.135.11[.]234	192.99.0[.]114
195.206.107[.]202	147.135.36[.]162	193.105.134[.]152
88.150.220[.]248	147.135.40[.]102	193.106.31[.]99
217.182.199[.]126	147.135.87[.]184	37.120.143[.]202
45.12.222[.]150	46.105.107[.]231	51.161.128[.]135
66.70.179[.]236	158.255.208[.]155	198.50.157[.]109
92.38.162[.]11	158.255.211[.]165	199.71.233[.]178
93.113.36[.]137	176.123.1[.]250	209.58.131[.]32

93.113.36[.]142	176.123.175[.]242	212.7.217[.]5
93.190.142[.]7	176.123.6[.]58	213.128.89[.]184
94.185.85[.]210	176.31.252[.]121	217.12.219[.]11
94.23.218[.]129	176.53.40[.]221	217.23.1[.]110
79.137.69[.]34	86.105.25[.]218	89.38.224[.]2
91.132.139[.]66	91.193.5[.]90	

MITRE ATT&CK Mapping

- **T1090 (Proxy):** Adversaries use VPN services such as First VPN Service to route traffic through intermediary systems, masking the true origin of malicious activity and evading detection.
- **T1133 (External Remote Services):** Threat actors leverage VPN infrastructure to access victim environments remotely, often using valid accounts to establish persistence or conduct follow-on activity.
- **T1078 (Valid Accounts):** VPN services are frequently used to authenticate enterprise systems using compromised credentials, blending malicious activity with legitimate access patterns.
- **T1046 (Network Service Discovery):** Observed scanning activity from First VPN Service-associated IP addresses is consistent with adversary efforts to identify open ports, services, and network configurations.
- **T1018 (Remote System Discovery):** VPN infrastructure may be used to enumerate systems within a target network following initial access.
- **T1110 (Brute Force):** VPN exit nodes can facilitate password spraying or brute force attempts against exposed services such as SSH, RDP, or web applications.
- **T1498 (Network Denial of Service):** First VPN Service infrastructure has been associated with denial-of-service activity, enabling adversaries to disrupt services or distract defenders.

Recommendations

Organizations should implement layered defensive controls that combine network restrictions, identity-based protections, and behavioral monitoring to mitigate the risks associated with anonymization services such as First VPN Service.

- **Block and Monitor Known First VPN Service Infrastructure:** Deny-list known First VPN Service domains and scrutinize IP addresses where operationally feasible. Continuously monitor connections to unapproved VPN infrastructure and newly observed IPs associated with anonymization services.

- **Implement VPN-Aware Access Controls:** Restrict authentication to corporate resources from approved networks or managed devices. Where possible, enforce conditional access policies that limit or flag logins originating from known VPN or proxy networks.
- **Enhance Authentication Security:** Require multi-factor authentication (MFA) for all remote access services, including VPN, SSH, RDP, and cloud-based applications. Monitor for authentication attempts from unfamiliar IP addresses, geolocations, or autonomous systems (ASNs).
- **Monitor for Anomalous Identity and Session Activity:** Detect and investigate indicators such as impossible travel, concurrent sessions from disparate regions, or changes in user-agent strings and device fingerprints associated with a single account.
- **Harden Remote Access Services:** Limit SSH and other remote management interfaces to trusted IP ranges or through secure access solutions (e.g., bastion hosts or zero trust architectures). Disable direct exposure of management services to the public internet where possible.
- **Inspect and Analyze Network Traffic:** Utilize network monitoring and logging solutions to identify abnormal traffic patterns, including potential lateral movement, scanning activity, or command-and-control (C2) communications originating from VPN-associated infrastructure.
- **Apply Least Privilege and Network Segmentation:** Reduce the potential impact of unauthorized access by enforcing least privilege principles and segmenting networks to limit lateral movement.
- **Review and Restrict Firewall Rules:** Regularly audit firewall configurations and close unnecessary ports and services to reduce exposure to external scanning and exploitation attempts.
- **Correlate Indicators with Behavioral Context:** Given the use of dynamically and ephemerally assigned IP addresses by VPN services, do not rely solely on IP-based blocking. Correlate indicators with behavioral analytics, endpoint telemetry, and identity context.
- **Leverage Threat Intelligence and ASN-Based Detection:** Incorporate threat intelligence feeds and monitor for activity originating from known VPN, hosting, or proxy provider ASNs commonly associated with anonymization services.

Reporting Notice

If you identify suspicious activity within your enterprise or have information related to the contents of this document, please contact your local FBI Cyber Squad immediately at **www.fbi.gov/contact-us/field-offices**. The FBI also encourages you to report suspicious or criminal activity to the FBI Internet Crime Complaint Center at **www.ic3.gov**. When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated considering your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistent with applicable state and federal laws.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by the FBI.

This FLASH was coordinated with the Cybersecurity and Infrastructure Security Agency (CISA) and is marked **TLP: CLEAR**. The information in this product may be shared without restriction. Information is subject to standard copyright rules.