

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.166.51 EDN: BWTYFQ

SECURITY THREATS IN VIRTUAL PRIVATE NETWORK INFRASTRUCTURE THROUGH BOTNET INTEGRATION AND DISTRIBUTED DENIAL OF SERVICE ATTACK MECHANISMS

Research article

Gibadullin R.F.[1, *]

[1] ORCID : 0000-0001-9359-911X;

[1] Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

* Corresponding author (landwatersun[at]mail.ru)

Abstract

This paper presents a comprehensive analysis of security threats arising from the exploitation of Virtual Private Network (VPN) infrastructure by botnet operators and Distributed Denial of Service (DDoS) attack organizers. The study examines three primary attack vectors: the distribution of malicious VPN clients embedding botnet functionality, the abuse of VPN provider infrastructure for traffic anonymization during cyberattacks, and the exploitation of vulnerabilities in tunneling protocols (GRE, IPIP, L2TP, 6in4) that allow unauthenticated packet injection. Using the Russian Federation as a case study, where VPN adoption reached 41% of internet users by 2025 due to escalating state censorship, the paper demonstrates how restrictive digital policies inadvertently expand the attack surface by driving users toward unverified VPN solutions. The analysis covers technical mechanisms of device recruitment into botnets, legal and reputational risks for VPN operators, and the regulatory landscape across jurisdictions. Practical security recommendations are formulated for end users, VPN service operators, and infrastructure hosts to mitigate the risks of involuntary participation in cybercriminal activities.

Keywords: Virtual Private Network, Distributed Denial of Service, Botnet, Cybersecurity, Tunneling Protocols, Malicious Clients, Traffic Anonymization, Network Vulnerabilities, Proxy Nodes, Infrastructure Abuse.

УГРОЗЫ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ, СВЯЗАННЫЕ С ИНТЕГРАЦИЕЙ БОТ-СЕТЕЙ И МЕХАНИЗМАМИ РАСПРЕДЕЛЕННЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

Научная статья

Гибадуллин Р.Ф.[1, *]

[1] ORCID : 0000-0001-9359-911X;

[1] Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

* Корреспондирующий автор (landwatersun[at]mail.ru)

Аннотация

В данной статье представлен всесторонний анализ угроз безопасности, возникающих в результате использования инфраструктуры виртуальных частных сетей (VPN) операторами бот-сетей и организаторами атак типа «распределенный отказ в обслуживании» (DDoS). В исследовании рассматриваются три основных вектора атак: распространение вредоносных VPN-клиентов, содержащих функциональность бот-сети; злоупотребление инфраструктурой VPN-провайдеров для анонимизации трафика во время кибератак; а также использование уязвимостей в протоколах туннелирования (GRE, IPIP, L2TP, 6in4), допускающих ввод неподтвержденных пакетов. На примере Российской Федерации, где к 2025 году использование VPN достигло 41% интернет-пользователей из-за усиления государственной цензуры, в работе показано, как ограничительная цифровая политика непреднамеренно расширяет поверхность атаки, подталкивая пользователей к непроверенным VPN-решениям. Анализ охватывает технические механизмы вербовки устройств в бот-сети, правовые и репутационные риски для операторов VPN, а также регуляторную среду в различных юрисдикциях. Сформулированы практические рекомендации по безопасности для конечных потребителей, операторов VPN-сервисов и хостинг-провайдеров, направленные на снижение рисков невольного участия в киберпреступной деятельности.

Ключевые слова: виртуальная частная сеть, распределённая атака типа «отказ в обслуживании», бот-сеть, кибербезопасность, протоколы туннелирования, вредоносные клиенты, анонимизация трафика, уязвимости сети, прокси-узлы, злоупотребление инфраструктурой.

Introduction

Virtual Private Networks (VPNs) have become one of the most widely adopted tools for ensuring online privacy and circumventing internet censorship worldwide. Their fundamental role in encapsulating and encrypting user traffic has been extensively documented in the networking literature [1], [2], [3]. However, the same infrastructure that provides legitimate users with privacy and access has increasingly attracted the attention of cybercriminals, who exploit VPN services for traffic anonymization, botnet command-and-control concealment, and large-scale Distributed Denial of Service (DDoS) attacks [4], [5], [6].

The scale and sophistication of DDoS attacks have grown dramatically in recent years. According to Cloudflare's threat reports, the total number of DDoS attacks exceeded 47 million in 2025, a 121% increase over the previous year, with peak attack bandwidth reaching 11.5 Tbps [7]. The AISURU/Kimwolf botnet, which compromised over two million Android devices and set a record-breaking 31.4 Tbps DDoS attack in late 2025, exemplifies the convergence of VPN abuse and botnet infrastructure: its operators used residential proxy networks and VPN applications to both recruit devices and anonymize attack traffic [8]. The largest botnet dismantled to date, 911 S5, which infected 19 million devices across 190 countries, was propagated specifically through malicious VPN applications such as MaskVPN, DewVPN, and ShieldVPN [9]. These developments underscore the urgency of studying VPN-related security threats.

Recent research has also revealed fundamental vulnerabilities in tunneling protocols widely used in VPN infrastructure. Beitis and Vanhoef identified critical flaws in GRE, IPIP, 6in4, and 4in6 protocols (CVE-2024-7595, CVE-2024-7596, CVE-2025-23018, CVE-2025-23019), demonstrating that 4.2 million internet hosts accept unauthenticated tunneling packets, allowing attackers to use them as one-way proxies for anonymous attacks [10]. Simultaneously, the TunnelVision vulnerability (CVE-2024-3661) showed that attackers on a local network can force VPN traffic to bypass the encrypted tunnel entirely using DHCP manipulation [11]. These findings highlight that VPN security threats extend beyond malware distribution to fundamental protocol-level weaknesses.

The Russian Federation presents a particularly instructive case study for examining these threats. The rapid expansion of internet censorship since 2022, including the blocking of major social media platforms, throttling of YouTube, and systematic targeting of VPN services by Roskomnadzor, has driven VPN adoption to approximately 41% of Russian internet users by 2025 [12]. The departure of reputable Western VPN providers from the Russian market, combined with the criminalization of VPN advertising and the blocking of 258 VPN services in 2024–2025, has created conditions in which users are increasingly driven toward unverified, potentially malicious VPN applications [13]. This environment amplifies the risks analyzed in the present study.

While existing literature addresses individual aspects of VPN security—botnet architectures [4], [5], [6], tunneling protocol vulnerabilities [10], [14], [15], and DDoS attack mechanisms [16], [17] — there is a notable gap in comprehensive analyses that integrate these threat vectors with the socio-political context that drives mass VPN adoption. The novelty of this work lies in providing a unified framework that combines technical analysis of VPN exploitation mechanisms (malicious clients, protocol vulnerabilities, infrastructure abuse) with an examination of the regulatory and geopolitical factors that create favorable conditions for these threats, using Russia's digital censorship landscape as a case study.

The objective of this work is to conduct a comprehensive analysis of the technical and organizational-legal risks associated with the use and hosting of VPN services, with a focus on the potential involvement of their users and operators in botnet infrastructure and DDoS attacks. To achieve this objective, the following tasks have been set:

· To systematize and analyze current threats related to the exploitation of VPN infrastructure by malicious actors, drawing on recent incident data and threat intelligence reports.

· To examine specific technical mechanisms through which users are recruited into botnets via malicious VPN clients and vulnerabilities in network tunneling protocols.

· To investigate the socio-political factors, particularly internet censorship policies, that amplify VPN-related security risks by driving users toward unverified solutions.

· To assess the legal and reputational risks faced by VPN service operators and hosts across different regulatory jurisdictions.

· To develop practical, evidence-based recommendations for reducing the risks of involuntary participation in cybercriminal activities for end users, VPN operators, and infrastructure hosts.

Digital Landscape and Internet Censorship in Russia

The current digital landscape of the Russian Federation is characterized by a systematic and multi-level increase in state control over the Internet. This process, which began long before 2022, has significantly accelerated and radicalized due to geopolitical events, leading to a persistent trend towards the creation of a "sovereign Internet" (Runet). The evolution of restrictions has taken place in two main areas: Firstly, under the influence of international sanctions and political decisions, a significant number of foreign companies have begun to withdraw their operations or restrict access to their services for Russian users. Secondly, Russian government agencies, primarily Roskomnadzor, have implemented extensive measures to block and restrict access to a wide range of foreign and even some Russian online resources. These parallel processes have created a complex and contradictory environment in which users are forced to rely on VPN technology at scale.

Since February 2022, in response to political events and the imposition of international sanctions, numerous foreign companies representing a wide range of industries, from finance and retail to high-tech and entertainment, have taken steps to curtail their operations in the Russian Federation. This process has been comprehensive, encompassing both complete market exit and the implementation of targeted restrictions on access to their products and services for Russian users. According to the Yale School of Management [18], by February 2025, more than 1,000 major international companies had announced plans to reduce their operations in Russia. This mass exodus has affected key sectors of the economy and had profound implications for the Russian consumer and corporate markets.

Some of the most notable examples include the following companies and their actions:

· Technology sector: Industry giants such as Apple, Google, Intel, AMD, Cisco, and Dell have suspended sales of their products and restricted access to certain services. For example, Apple stopped online sales of its products in Russia in March 2022 and limited the functionality of Apple Pay. Grammarly, a company that provides AI-powered services, has completely blocked users from Russia and Belarus.

· Financial sector: Major payment systems such as Visa and Mastercard, as well as American Express and PayPal, have suspended their operations, severely limiting the ability of Russian bank cards to conduct international transactions.

· Entertainment and retail sector: Disney, Warner Bros., Sony, and other film studios have suspended the release of their films in Russian theaters. Retail brands, including Nike, Adidas, H&M, Zara (Inditex), and IKEA, have closed their stores and suspended online sales.

Along with corporate decisions to withdraw from the market, foreign countries, primarily members of the European Union, have imposed sanctions that have directly affected digital services. In April 2022, regulations came into effect that require Internet service providers, social media platforms, and app stores to take reasonable steps to prevent users from accessing content created or distributed by sanctioned individuals and organizations. As a result, platforms such as Facebook, Instagram, and Twitter (now X) were forced to restrict access to accounts of Russian state-owned media outlets like RT and Sputnik for users in Europe. In response, the Russian authorities took countermeasures, leading to subsequent blockages of these platforms in Russia.

In parallel with the restrictions imposed by foreign companies, Russian regulatory authorities, particularly Roskomnadzor, have launched and significantly intensified a campaign to block and restrict access to foreign online services, social media, and censorship-evading tools, including VPNs, since 2022. This campaign is part of a broader government policy aimed at creating a "sovereign Internet" and increasing control over information space. Although the first blockages of major platforms such as LinkedIn occurred in 2016, it was in 2022 that the pace and scale of restrictions increased dramatically.

Key stages of strengthening censorship measures include:

· Blocking social media: In March 2022, Roskomnadzor began blocking access to Facebook and Instagram (owned by Meta, which is recognized as an extremist organization in Russia). Access to Twitter (now X) was initially "slowed down" and then completely blocked.

· Restricted access to YouTube: Starting in August 2024, YouTube's video hosting service was almost completely shut down on the networks of Russian providers due to targeted traffic throttling by the authorities.

· Blocking of messengers and other services: In 2024-2025, popular services such as Signal, Viber, Snapchat, Roblox, and Apple's FaceTime video calling feature were blocked. The official reasons for the blockages were "terrorist activities," "extremism," and "fraud."

· Campaign against VPNs: Since 2024, Roskomnadzor has been systematically targeting VPN services. On March 1, 2024, a law was enacted granting the agency the authority to demand the removal of all VPN apps that allow for circumvention of blockings from app stores. By October 2024, at least 197 VPN services had been blocked. In 2025, additional restrictions were introduced, including a ban on VPN advertising and criminal liability for using VPNs to spread "fake news" about the armed forces.

These measures have created a difficult situation in which access to a significant portion of the global Internet has become impossible for users in Russia without the use of censorship-bypassing tools. However, as experts point out, it is the pressure on foreign technology companies and the tightening of legislation that has forced many reputable Western VPN providers to leave the Russian market, leaving users with less reliable and potentially dangerous solutions.

Malicious VPN Clients and Botnet Functionality

The infrastructure of commercial VPN providers is actively used by cybercriminals to carry out cyberattacks, including DDoS attacks on media resources, government systems, and commercial systems. The main advantage that VPN services provide cybercriminals is the masking of the attacker's true IP address. Victims and law enforcement agencies record the IP addresses of VPN nodes rather than the end users of the attacks, making attribution and response processes more challenging. This allows DDoS campaign organizers to operate with a high degree of anonymity, using both legitimate VPN subscriptions and compromised or anonymously purchased accounts. As a result, VPN provider infrastructure effectively becomes a transportation platform for cybercriminal activities, endangering both the providers themselves and their law-abiding users, whose devices may be involved in attacks without their knowledge.

Botnet functionality in VPN clients. One of the most dangerous and widespread mechanisms for involving user devices in cybercriminal infrastructure is the distribution of malicious VPN clients that masquerade as legal and free solutions for ensuring privacy and bypassing blocks. Once installed on a user device, such applications establish a hidden connection with a control server (C&C, Command and Control) controlled by attackers, effectively turning the device into a "zombie" — a full-fledged botnet node. These malicious clients not only fail to perform their primary task of protecting traffic, but also actively exploit the device's resources to perform malicious actions on behalf of the botnet operators. The functionality of such Trojan programs can be extremely diverse and dangerous.

Key malicious capabilities embedded in fake VPN clients include:

· Traffic generation for DDoS attacks: The user's device may be involved in a distributed attack such as an HTTP-flood [16], [17]. In this case, the client, upon receiving a command from the C&C server, begins generating many HTTP(S) requests to the victim's target web server, overloading it and causing it to malfunction. The user is typically unaware of what is happening until they notice abnormal behavior on their device or receive complaints from their Internet service provider.

· Using the device as a proxy: Malware can configure the device as an open proxy server, through which attackers can redirect their traffic. This allows attackers to conceal their real geolocation and IP address, using the victim resources for further attacks, spam campaigns, or other illegal activities. As a result, the user's IP address may be blacklisted, and the user may be suspected of cybercriminal activities.

· Downloading and executing additional malicious code: A Trojan VPN client can serve as a downloader for other malicious programs. Upon receiving a command, it can download and install additional modules on the device, such as keyloggers, ransomware, or other malicious software, significantly increasing the level of system compromise and potential damage to the user.

Thus, the use of questionable or free VPN applications with an opaque data processing policy poses an extremely high risk. A user seeking anonymity may unknowingly become part of a criminal infrastructure, which they may eventually become a victim of.

Some VPN and proxy services [19], [20], especially those offering their services for free or on a shareware basis, build their architecture on a model in which users' client devices turn into exit nodes for other people's traffic. Under this model, the user gets free access to anonymize their own traffic in exchange for providing their network resources — bandwidth and IP address — to other network users. However, as a rule, there is no clear and understandable information about exactly how and to what extent these resources will be used. The user is often unaware that their device and their IP address have become an infrastructure for the relaying of extraneous traffic, the nature and content of which are unknown and beyond their control.

This architecture creates serious potential for the involvement of good-faith users in various types of abuse. Since all outgoing traffic is displayed as coming from the user's IP address, the device owner may be involved in:

· DDoS attacks: If other network users decide to attack a resource, all the attacking traffic will originate from the user's network, making their IP address the source of the attack.

· Spam mailings: The device can be used for mass spam mailings, which will result in the IP address being blacklisted by email servers.

· Other illegal activities: Traffic can be used to spread malware, child pornography, extremist materials, and other prohibited data. This creates a legal and reputational conflict, as the user may not have directly initiated or committed the illegal actions, but their infrastructure and IP address served as a platform for these activities.

In the event of an investigation, the IP address owner will be the first to come under scrutiny by law enforcement agencies.

DDoS Attack Traffic Anonymization via VPN Infrastructure

Analysis of incidents shows that the organizers of DDoS campaigns actively exploit the infrastructure of major VPN providers to generate attack traffic. They use both legally purchased subscriptions and compromised or anonymously purchased accounts. The attackers run specialized software on their devices that route all attack traffic through a VPN server. This effectively masks the geography and origin of the attack, as the victim and law enforcement agencies will see the VPN server's IP address as the source of the traffic, rather than the actual attacker. This approach significantly complicates the attribution and response process, allowing attackers to operate with a high degree of anonymity and avoid responsibility.

In addition to generating traffic directly from VPN servers, attackers also actively use VPN nodes as intermediate proxies in multi-step chains. In this scenario, the attack traffic passes through multiple different VPN servers, as well as possibly through other anonymizing technologies such as Tor or public proxies. This "onion" routing scheme makes it nearly impossible to determine the true source of the attack. Each node in the chain only knows its previous and subsequent neighbor, making tracing significantly more challenging. This method is particularly effective in complex, targeted attacks, where attackers need to conceal their identity and location as much as possible to avoid detection and ensure the ability to launch repeated attacks.

To achieve maximum anonymity and resilience of their infrastructure, attackers often combine VPNs with other anonymization technologies, such as Tor (The Onion Router) and public proxy servers. This allows them to build extremely complex and convoluted schemes to hide the source of their attack. For example, traffic may first be routed through a local VPN client, then through multiple Tor nodes, before being routed back to the Internet through one or more VPN servers in different countries. This multi-layered architecture makes attribution nearly impossible, as it requires the cooperation of multiple different providers and organizations across different jurisdictions to uncover the chain. This allows attackers to operate with a high degree of impunity.

Vulnerabilities in Tunneling Protocols

Modern research in the field of information security has revealed that a significant number of hosts on the Internet are vulnerable to attacks due to incorrect processing of packets that use various tunneling protocols. These include protocols such as GRE (Generic Routing Encapsulation), IP-in-IP, L2TP (Layer 2 Tunneling Protocol) [14], [15], and other traffic encapsulation mechanisms that are widely used in VPN and corporate network infrastructure. Vulnerabilities arise due to errors in the implementation of these protocols in network equipment and software, as well as due to incorrect configuration of tunnel interfaces. Attackers can exploit these vulnerabilities to carry out various types of attacks that do not require the installation of malware on the target system. This makes vulnerable VPN gateways and routers potential infrastructure elements for cyberattacks.

Vulnerability abuse scenarios. One of the vulnerability abuse scenarios in tunneling protocols is the forced use of a vulnerable host as a one-way proxy. In this case, an attacker can send specially crafted encapsulated packets to a vulnerable VPN gateway or router, forcing it to forward these packets to third parties without requiring authentication from the sender. This allows the attacker to use someone else's network infrastructure for attacks while masking their true IP address. For the victim of the attack, all malicious traffic will appear to be coming from the network where the vulnerable host is located, which can lead to the host being blocked and causing additional problems for its owner.

Vulnerabilities in tunneling protocols can be exploited to amplify DoS/DDoS attacks. An attacker can send encapsulated packets to a vulnerable host, specifying the target IP address as the source. The vulnerable host, while processing these packets, will send responses directly to the target IP address, unintentionally participating in the attack. Additionally, improper handling of tunnel packets can lead to network equipment overload, causing denial-of-service for legitimate users. In more complex scenarios, an attacker can exploit vulnerabilities to uncontrollably route encapsulated packets within corporate and operator networks, potentially leading to overloaded internal communication channels and disruption of critical services.

Vulnerabilities in tunneling protocols can also be exploited to carry out attacks on network infrastructure, such as DNS spoofing [21], [22] and poisoning attacks. An attacker can exploit vulnerable tunnel interfaces to inject false data into the DNS server in cache or to redirect traffic to malicious resources. For example, by sending specially crafted packets through a vulnerable VPN gateway, an attacker can cause it to process these packets incorrectly, leading to the compromise of network

traffic. This can allow an attacker to intercept sensitive data, conduct phishing attacks, or distribute malware. As a result, vulnerable VPN gateways and routers become not only tools for conducting DDoS attacks, but also a vector for more subtle and dangerous attacks on network infrastructure.

Legal and Regulatory Risks for VPN Operators

VPN service operators and individuals hosting VPN nodes on VPS or home servers face increased technical risks related to the possibility of using their infrastructure for illegal purposes. These risks include overloading communication channels, which can lead to reduced service quality for legitimate users or even complete denial of service. Additionally, exploiting vulnerabilities in VPN software or network protocols can compromise the VPN system itself. Attackers can gain unauthorized access to the server, steal user data, modify the service configuration, or use it as a springboard for further attacks on other systems. This not only damages the operator's reputation but can also lead to serious financial and legal consequences.

In addition to the technical consequences, VPN service providers face significant legal and reputational risks. If the VPN service infrastructure is used for DDoS attacks or other cybercrimes, the provider may be held accountable for facilitating criminal activities. This is particularly relevant in an increasingly regulated cybersecurity landscape, where not only the perpetrators but also those providing infrastructure support may face legal consequences. Reputational costs can also be significant: news that a VPN service has been involved in cyberattacks can erode user trust and lead to a mass exodus of customers. This can cause irreparable damage to a business, especially if it operates on a commercial basis.

Law enforcement practices and legislative initiatives in several countries demonstrate a steady trend towards increasing liability for participation in DDoS attacks and creating conditions for their implementation. In such circumstances, the owner of a VPN infrastructure may be considered an entity that has failed to provide an adequate level of control and prevention of abuse, especially in the case of commercialization of the service. This means that VPN service providers are required to implement effective measures for monitoring traffic, identifying, and blocking suspicious activity. Failure to comply with these requirements may be considered negligence or indirect facilitation of cybercriminal activities, which can result in both administrative and criminal liability. This trend has prompted VPN service providers to review their security policies and implement stricter protection measures.

The legal assessment of the actions of VPN infrastructure owners depends on national legislation, but the general trend is to expand the range of individuals potentially liable for participation in DDoS attacks. Various jurisdictions are discussing or have already implemented regulations that impose penalties not only on the direct perpetrators of attacks, but also on individuals who provide infrastructure support. This means that even if there is no direct intent, a VPN service provider may be held accountable for negligent or indirect involvement in cybercriminal activities. Several countries have introduced special requirements for VPN operators, requiring them, for example, to connect to government-run blacklist registries to filter traffic. Failure to comply with these requirements may result in severe fines and other penalties.

Duration and scale of abuse. When assessing the responsibility of the owner of a VPN infrastructure, the key factor is the duration and scale of abuse of this infrastructure for conducting attacks. If suspicious activity is recorded on the VPN provider server for an extended period and is systematic in nature, it may indicate that insufficient measures have been taken to combat abuse. In such cases, the operator may face greater responsibility compared to situations where the attack was a single and short-lived incident that was promptly detected and addressed. Therefore, regular monitoring and analysis of network traffic are crucial for demonstrating the operator's integrity and minimizing legal risks.

Another important factor that affects the legal assessment of a VPN operator's actions is the presence or absence of reasonable measures to monitor and suppress malicious activity. An operator that has implemented effective intrusion detection systems (IDS/IPS [23], [24]), maintains user activity logs, regularly analyzes traffic for anomalies, and promptly blocks suspicious sessions will be viewed more favorably than an operator that does not take any efforts to prevent abuse. The presence of a clear security policy, incident response procedures, and documented actions to prevent malicious activity can serve as a strong indicator of the operator's integrity.

Finally, the commercial nature of the service provision and the operator's awareness of potential abuse also play a significant role in the legal assessment. A commercial VPN provider that generates revenue from its services has a higher responsibility to ensure the security of its infrastructure compared to an individual who provides access to a VPN server for free. If the operator has been informed about instances of abuse in their infrastructure but has not taken any steps to address them, it may be considered as intentional facilitation of cybercriminal activities. In this case, the operator's responsibility will be significantly higher, and they may face more severe sanctions.

Security Recommendations for Users and Operators

To minimize the risks of involvement in a botnet infrastructure, it is recommended that end users use VPN clients only from trusted and reputable providers. When choosing a VPN service, it is important to consider its history, user reviews, and clear privacy policies. The client application should be downloaded only from official software distribution sources, such as the provider's official website or official app stores (App Store, Google Play). Using clients from unofficial sources significantly increases the risk of installing malware that disguises itself as a VPN app.

Users are strongly advised to avoid questionable free VPN solutions with an opaque traffic handling policy and a lack of information about the service owner. Typically, such services monetize at the expense of the user, for example, by selling their data to third parties, embedding ads, or, even worse, using their device as a proxy node for relaying external traffic. "There's no such thing as a free lunch," and in the context of VPNs, this expression holds particular significance. A reliable and secure VPN service requires significant costs for server rental, software development, and security measures, so it cannot be completely free.

After installing the VPN client, it is recommended that the user regularly monitor the behavior of their system. They should pay attention to indicators such as network activity, CPU usage, and RAM usage. If there are any abnormalities, such as unusually high network activity in the background, slow system performance, or device overheating, it may be a sign of

malicious activity. In such cases, it is important to immediately disable the VPN client, perform a full antivirus scan of the system, and, if necessary, remove the suspicious application.

It is advisable for VPN service operators and private hosts to implement strict restrictions on the list of open protocols and ports. It is necessary to configure firewalls (firewall) in such a way as to block all unused traffic. In addition, it is recommended to implement intrusion detection and prevention systems (IDS/IPS) that will analyze incoming and outgoing traffic for signs of attacks. This will allow for timely detection and blocking of attempts to abuse the VPN service infrastructure.

To prevent unauthorized access to the VPN service, operators should use strict authentication mechanisms. Instead of using simple logins and passwords, it is recommended to use more secure methods such as certificate or key-based authentication. Additionally, multi-factor authentication (MFA) [25], [26] should be implemented for administrative access to servers. Regular auditing of user and administrator accounts is also an important security measure, allowing for the timely identification and deactivation of compromised or suspicious accounts.

VPN service providers should implement monitoring and logging tools to analyze abnormal outgoing traffic. They should keep detailed logs of user activity, including information about connections, transmitted traffic volume, and target IP addresses. Automated log analysis systems should detect suspicious patterns, such as sudden spikes in outgoing traffic, multiple connections from a single account, or attempts to access known malicious resources. When anomalies are detected, suspicious sessions should be promptly blocked, and the incident should be investigated.

Finally, it is crucial for VPN service providers to keep their VPN software, operating systems, and network equipment up to date to address known vulnerabilities. Many attacks on VPN infrastructure exploit outdated software versions that have already been patched. Regularly updating the system can help close these security gaps and significantly reduce the risk of compromise. It is also important to implement a regular security audit process and monitor new vulnerabilities in the software and hardware used.

Conclusion

The present study has produced the following principal results. First, a systematic classification of VPN-related security threats has been developed, identifying three primary attack vectors:

1) distribution of malicious VPN clients with embedded botnet functionality, as exemplified by the 911 S5 botnet that infected 19 million devices through six VPN applications;

2) exploitation of legitimate VPN infrastructure for DDoS traffic anonymization, with attack volumes reaching 11.5 Tbps in 2025;

3) abuse of vulnerabilities in tunneling protocols (GRE, IPIP, L2TP, 6in4/4in6), with 4.2 million hosts identified as vulnerable to unauthenticated packet injection.

Second, the study demonstrates, using the Russian Federation as a case study, that restrictive internet censorship policies create a paradoxical security effect: by blocking reputable VPN providers and driving 41% of internet users toward unverified alternatives, state censorship inadvertently expands the attack surface available to botnet operators and cybercriminals. Third, a comparative analysis of the regulatory landscape across jurisdictions has revealed a clear trend toward expanding liability for VPN infrastructure abuse, where operators face increasing legal responsibility for failing to implement adequate monitoring and abuse prevention measures.

The novelty and originality of this work consist in the integration of technical threat analysis with the socio-political context of mass VPN adoption. Unlike prior studies that address botnet architectures, tunneling vulnerabilities, or DDoS attack mechanisms in isolation, this paper provides a unified analytical framework that traces the causal chain from internet censorship policies through user migration to unverified VPN solutions to the expansion of botnet infrastructure. This interdisciplinary approach enables a more complete understanding of the threat landscape and supports the development of more effective countermeasures.

Based on these findings, the study formulates a set of practical recommendations targeting three stakeholder groups: end users (prioritizing trusted VPN providers, monitoring system behavior for signs of botnet activity), VPN operators (implementing IDS/IPS systems, enforcing strict authentication, maintaining activity logs for anomaly detection), and infrastructure hosts (restricting open protocols and ports, regular security audits, timely patching of tunneling protocol vulnerabilities). The implementation of these measures can significantly reduce the likelihood of involuntary involvement in cybercriminal activities. Future research should focus on developing automated detection mechanisms for malicious VPN clients and on quantitative assessment of the relationship between censorship intensity and the prevalence of VPN-based botnet infections [27], [28].

Финансирование

Данная работа/публикация была финансирована грантом Академии наук Республики Татарстан, выделенным высшим учебным заведениям, научным и другим организациям в целях содействия реализации планов по развитию кадрового потенциала, направленных на стимулирование научно-преподавательского состава к защите докторских диссертаций и ведению научно-исследовательской деятельности (Договор № 15/2025-PD-KAI от 22 декабря 2025 г.).

Конфликт интересов

Не указан.

Рецензия

Рудой Е.М., ООО «ГК «Иннотех», Москва Российская Федерация

DOI: https://doi.org/10.60797/IRJ.2026.166.51.1

Funding

This work/publication was funded by a grant from the Academy of Sciences of the Republic of Tatarstan provided to higher education institutions, scientific and other organizations to support human resource development plans in terms of encouraging their research and academic staff to defend doctoral dissertations and conduct research activities. (Agreement No. 15/2025-PD-KAI dated December 22, 2025).

Conflict of Interest

None declared.

Review

Rudoi E.M., Innotech Group LLC, Moscow Russian Federation

DOI: https://doi.org/10.60797/IRJ.2026.166.51.1

Список литературы на английском языке / References in English

1. Barguil S. Experimental validation of L3 VPN Network Model for improving VPN service design and provisioning / S. Barguil, O. Gonzalez de Dios, V. Lopez Alvarez [et al.] // 2020 16th International Conference on Network and Service Management (CNSM). — Izmir, 2020. — P. 1–5. — DOI: 10.23919/CNSM50824.2020.9269043.

2. Vasavi V. Carrier Supporting Carrier: With Customer Carrier Providing MPLS VPN Services to User Sites / V. Vasavi, M.K. Swaroopa Rani, M.D. Prasad // 2018 International Conference on Inventive Research in Computing Applications (ICIRCA). — Coimbatore, 2018. — P. 298–303. — DOI: 10.1109/ICIRCA.2018.8597314.

3. IP over satellite - The next generation: MPLS, VPN and DRM delivered services // IEE Seminar on IP Over Satellite — The next Generation: MPLS, VPN and DRM Delivered Services, 2003. — 2003. — P. 0_1–0_2.

4. Reza F. DDoS-Net: Classifying DDoS Attacks in Wireless Sensor Networks with Hybrid Deep Learning / F. Reza // 2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT). — Dhaka, 2024. — P. 487–492. — DOI: 10.1109/ICEEICT62016.2024.10534545.

5. Aliyev R. DDoS Simulation: Empowering Targets through Simulated Attacks / R. Aliyev // 2023 IEEE 17th International Conference on Application of Information and Communication Technologies (AICT). — Baku, 2023. — P. 1–4. — DOI: 10.1109/AICT59525.2023.10313188.

6. Sharma A.K. A Comprehensive survey of DDoS Attacks: Evolution, Mitigation and Emerging trend / A.K. Sharma, R. Kumar // 2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC). — Mathura, 2024. — P. 185–188. — DOI: 10.1109/PARC59193.2024.10486696.

7. Yoachimik O. 2025 Q4 DDoS threat report: A record-setting 31.4 Tbps attack caps a year of massive DDoS assaults / O. Yoachimik, J. Pachec // Cloudflare Blog. — 2026. — URL: https://blog.cloudflare.com/ddos-threat-report-2025-q4/ (accessed: 03.01.2026)

8. The Most Powerful Ever? Inside the 11.5 Tbps-Scale Mega Botnet AISURU // XLab Cyber Threat Insight and Analysis. — 2025. — URL: https://blog.xlab.qianxin.com/super-large-scale-botnet-aisuru-en/ (accessed: 03.01.2026)

9. 911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation / U.S. Department of Justice // DOJ Press Release. — 2024. — URL: https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation (accessed: 03.01.2026)

10. Beitis A. Haunted by Legacy: Discovering and Exploiting Vulnerable Tunnelling Hosts / A. Beitis, M. Vanhoef // SENIX Security Symposium 2025. — Seattle, 2025. — URL: https://papers.mathyvanhoef.com/usenix2025-tunnels.pdf (accessed: 03.01.2026)

11. TunnelVision (CVE-2024-3661): How Attackers Can Decloak Routing-Based VPNs For a Total VPN Leak / Leviathan Security Group // Leviathan Security Blog. — 2024. — URL: https://www.leviathansecurity.com/blog/tunnelvision (accessed: 03.01.2026)

12. Russia: Freedom on the Net 2024 Country Report // Freedom House. — 2024. — URL: https://freedomhouse.org/country/russia/freedom-net/2024 (accessed: 03.01.2026)

13. Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia // HRW Report. — 2025. — URL: https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation (accessed: 03.01.2026)

14. Liu Z. Communication Between Remote LANs Based on L2TP / Z. Liu, B. Tang // 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS). — Beijing, 2018. — P. 221–224. — DOI: 10.1109/ICSESS.2018.8663781.

15. Fitri R.N. OSPF-Driven Assessment of SSTP, PPTP, and L2TP/IPSec VPN Protocols for FTP-SFTP Services / R.N. Fitri, D. Pranindito, N. Amalia [et al.] // 2025 IEEE 15th Symposium on Computer Applications & Industrial Electronics (ISCAIE). — Penang, 2025. — P. 97–101. — DOI: 10.1109/ISCAIE64985.2025.11081144.

16. Dhanapal A. An effective mechanism to regenerate HTTP flooding DDoS attack using real time data set / A. Dhanapal, P. Nithyanandam // 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). — Kerala, 2017. — P. 570–575. — DOI: 10.1109/ICICICT1.2017.8342626.

17. Rao Varre D.N.M. A Secured Botnet Prevention Mechanism for HTTP Flooding Based DDoS Attack / D.N.M. Rao Varre, J. Bayana // 2022 3rd International Conference for Emerging Technology (INCET). — Belgaum, 2022. — P. 1–5. — DOI: 10.1109/INCET54531.2022.9824510.

18. Sonnenfeld J. Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain / J. Sonnenfeld, S. Tian, [et al.] // Yale School of Management, Chief Executive Leadership Institute, 2022–2025. — URL: https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain (accessed: 03.01.2026)

19. Chen I. Proxy-based Regional Registration for Integrated Mobility and Service Management in Mobile IP Systems / I. Chen, W. He, B. Gu // The Computer Journal. — 2007. — Vol. 50. — № 3. — P. 281–293. — DOI: 10.1093/comjnl/bxl083.

20. Frank D. Using an Interface Proxy to Host Versioned Web Services / D. Frank, L. Lam, L. Fong [et al.] // 2008 IEEE International Conference on Services Computing, Honolulu. — 2008. — P. 325–332. — DOI: 10.1109/SCC.2008.84.

21. Panda D. Strengthening IoT Resilience: A Study on Backdoor Malware and DNS Spoofing Detection Methods / D. Panda, N. Padhy, K. Sharma // 2025 International Conference on Emerging Systems and Intelligent Computing (ESIC). — Bhubaneswar, 2025. — P. 795–800, — DOI: 10.1109/ESIC64052.2025.10962564.

22. Jony A. Unveiling DNS Spoofing Vulnerabilities: An Ethical Examination Within Local Area Networks / A. Jony, M.N. Islam, I.H. Sarker // 2023 26th International Conference on Computer and Information Technology (ICCIT). — Cox's Bazar, 2023. — P. 1–6. — DOI: 10.1109/ICCIT60459.2023.10441649.

23. Yalda R. Enhancing IoT Security Affordably with Raspberry Pi and Open-Source IDS/IPS / R. Yalda, N. Nepal, T. El Hawari // *2024 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET).* — Hammamet, 2024. — P. 1–6. — DOI: 10.1109/IC_ASET61847.2024.10596202.

24. Rajora C.S. IoT Based Smart Home with Cutting-Edge Technology for IDS/IPS / C.S. Rajora, A. Sharm // 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE). — Bangalore, 2022. — P. 1–5. — DOI: 10.1109/ICATIECE56365.2022.10047483.

25. Guo Y. A Security Protection Technology Based on Multi-factor Authentication / Y. Guo [et al.] // 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC). — 2022. — P. 1–5. — DOI: 10.1109/ICMNWC56175.2022.10032006.

26. Zhang Y. Research on the Application of Multi Factor Authentication Technology for 5G Terminals in the Coal Industry / Y. Zhang, J. Zhou // 2025 6th International Conference on Computer Engineering and Application (ICCEA. — Hangzhou, 2025. — P. 1422–1426. — DOI: 10.1109/ICCEA65460.2025.11102227.

27. Chung W. Profiling and Visualizing Cyber-criminal Activities: A General Framework / W. Chung, G.A. Wang // 2007 IEEE Intelligence and Security Informatics. — New Brunswick, 2007. — P. 376–376. — DOI: 10.1109/ISI.2007.379512.

28. Wiyono R.T. Performance Analysis of Decision Tree C4.5 as a Classification Technique to Conduct Network Forensics for Botnet Activities in Internet of Things / R.T. Wiyono, N.D.W. Cahyani // 2020 International Conference on Data Science and Its Applications (ICoDSA). — Bandung, 2020. — P. 1–5. — DOI: 10.1109/ICoDSA50139.2020.9212932.