INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-27 14:07 UTC

FBI links First VPN Service to ransomware gangs, botnets, criminal dark web activity; calls for layered defensive controls

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0373
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Organizations with network exposure to First VPN Service anonymization infrastructure; any enterprise monitoring VPN egress traffic
Published	2026-05-27
Discovery Source	Gemini

Executive Summary

The FBI has identified 'First VPN Service' as a criminal anonymization platform active since 2014, linked to ransomware groups and used to conceal intrusion activity including credential abuse, network reconnaissance, and denial-of-service attacks. Any organization with internet-facing systems is potentially exposed, as threat actors use this infrastructure to mask their origin IP addresses and evade attribution during active campaigns. The primary business risk is ransomware deployment and operational disruption enabled by attackers who can bypass IP-based detection controls.

Technical Analysis

First VPN Service operates as a criminal anonymization facilitator, providing threat actors with rotating or obfuscated IP infrastructure to conceal intrusion origins. The FBI advisory links the service to ransomware groups and documents its use across multiple attack phases: initial reconnaissance (MITRE T1595), proxy-based obfuscation (T1090, T1090.003), infrastructure acquisition (T1583.003), valid account abuse (T1078), credential brute-force and stuffing (T1110), and ransomware deployment (T1486). Relevant weaknesses include CWE-287 (Improper Authentication), CWE-284 (Improper Access Control), and CWE-306 (Missing Authentication for Critical Function). No CVE is assigned; this is an infrastructure-level threat, not a software vulnerability. CVSS does not apply to infrastructure-level threats; severity is rated qualitatively as High based on attack scope and target criticality. The service complicates attribution by rotating egress IPs, rendering IP-reputation blocklists and origin-based detection insufficient as standalone controls. No patch applies;

mitigation is detection- and policy-based. FBI advisory documentation exists; direct URLs require human validation before treating as verified primary-source references.

Action Checklist

1. Step 1: Containment. Review firewall and proxy egress rules immediately. Block or alert on outbound connections to known anonymization and bulletproof VPN infrastructure. Per NIST AC-4 (Information Flow Enforcement), enforce approved egress paths and deny unapproved VPN tunnels at the perimeter. Apply CIS 4.4 and CIS 4.5 to confirm server and endpoint firewall rules enforce default-deny outbound posture.
2. Step 2: Detection. Query perimeter logs, SIEM, and DNS resolver logs for connections associated with First VPN Service IP ranges and domains (validate against the official FBI advisory URL or cross-reference with your threat intelligence feed provider before operationalizing IOCs). Look for behavioral indicators per NIST SI-4 (System Monitoring): high-frequency authentication failures (T1110), scanning patterns from unfamiliar IP ranges (T1595), and VPN connections not matching your approved VPN provider list. Enable CIS 8.2 (Collect Audit Logs) across all perimeter devices if not already active.
3. Step 3: Eradication. This is an infrastructure threat, not a patchable vulnerability. Eradication means policy enforcement: enforce an approved VPN allowlist per NIST AC-17 (Remote Access) and block unauthorized VPN protocols at the network boundary. Disable or restrict any accounts showing authentication anomalies correlated with First VPN Service egress IPs. Rotate credentials for any accounts flagged in log review per D3-CRO (Credential Rotation).
4. Step 4: Recovery. Validate that detection rules and egress blocks are active and logging correctly. Confirm SIEM is alerting on connections to anonymization infrastructure. Cross-reference any incidents flagged during containment against known ransomware precursor behaviors (T1078 valid account use followed by T1486 deployment). Monitor authentication logs for 72 hours post-containment for residual brute-force activity per NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Conduct a gap assessment against NIST AC-6 (Least Privilege) and AC-2 (Account Management) to identify over-privileged accounts that could be exploited via credential abuse. Evaluate whether your IP-reputation-based detections are supplemented by behavioral analytics, since anonymization infrastructure renders pure IP blocking insufficient. Document findings and update your threat intelligence feed with validated First VPN Service IOCs.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance immediately if any Windows Security Event ID 4624 (Successful Logon) or VPN gateway authentication success is confirmed from First VPN Service IP ranges against privileged accounts, or if ransomware precursor behaviors (T1486, shadow copy deletion, mass file enumeration) are detected during the 72-hour watch period — either condition indicates active intrusion beyond reconnaissance and may trigger breach notification obligations under HIPAA, PCI-DSS, or applicable state privacy laws.

Recovery Notes	Post-containment, verify egress blocks are enforced at both the perimeter firewall and host-based firewall layers by attempting a test connection from a monitored non-production host to a known First VPN Service IP and confirming the block fires and logs correctly. Monitor authentication logs (Windows Security Event IDs 4624, 4625, 4648) and VPN gateway session logs continuously for 72 hours, with particular focus on any accounts that had prior authentication anomalies correlated with First VPN Service IPs — residual access from a pre-containment successful login is the primary recovery risk. Given the FBI advisory links First VPN Service to 25+ ransomware groups with multi-year operational history, extend threat hunting for T1078 valid account persistence and T1053 scheduled task creation for a minimum of 30 days post-incident using Sysmon Event ID 1 and Windows Security Event ID 4698.
Forensic Artifacts	Firewall and proxy session logs (Palo Alto Traffic logs, Cisco ASA syslog, Squid access.log) filtered on First VPN Service IP ranges and ASNs — these will show the full timeline of inbound reconnaissance and outbound C2 or data exfiltration activity proxied through First VPN infrastructure, which is the primary evasion mechanism identified in the FBI advisory. | Windows Security Event Log Event ID 4625 (Failed Logon) and 4624 (Successful Logon, Types 3 and 10) from all internet-facing systems and VPN gateways — credential abuse via brute force (T1110) proxied through First VPN Service is the specific attack pattern identified by the FBI, making authentication logs the highest-value forensic source for this threat. | DNS resolver query logs (Windows DNS Server debug log at %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.etl, or BIND query log at /var/log/named/query.log) for any internal host resolving First VPN Service-associated domains — DNS queries precede connection establishment and may reveal compromised hosts that attempted to reach First VPN C2 infrastructure before network blocks were in place. | VPN gateway full session records including authentication method, source IP, assigned tunnel IP, session duration, and bytes transferred (Cisco ASA: `show vpn-sessiondb detail anyconnect`, Palo Alto GlobalProtect: Monitor > Logs > GlobalProtect) — successful VPN authentications originating from First VPN Service IP space directly evidence T1078 valid account abuse and establish the scope of potential unauthorized access. | Sysmon Event ID 1 (Process Creation) and Windows Security Event ID 4688 logs from hosts that had confirmed or suspected inbound connections from First VPN Service IPs — post-authentication process execution (cmd.exe, powershell.exe, net.exe, nltest.exe) on these hosts would evidence hands-on-keyboard activity consistent with the network reconnaissance behavior the FBI attributed to actors using First VPN infrastructure.

Per-Action IR Details

Step 1: Containment — Review firewall and proxy egress rules immediately. Block or alert on outbound connections to known anonymization and bulletproof VPN infrastructure. Per NIST AC-4 (Information Flow Enforcement), enforce approved egress paths and deny unapproved VPN tunnels at the perimeter. Apply CIS 4.4 and CIS 4.5 to confirm server and endpoint firewall rules enforce default-deny outbound posture.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use pfSense or iptables to enforce egress ACLs: `iptables -A OUTPUT -d -j DROP`. Pull First VPN Service IP ranges from the FBI advisory and feed them into a free threat-intel blocklist script using ipset for bulk blocking — `ipset create firstvpn_block hash:net && ipset add firstvpn_block && iptables -A OUTPUT -m set --match-set firstvpn_block dst -j DROP`. For endpoints without EDR, deploy Windows Firewall GPO rules blocking known anonymization port ranges (UDP/TCP 1194, 1723, 500, 4500) outbound where these ports are not required for

business operations.

Evidence: BEFORE blocking, capture a full 24-48 hour window of netflow or firewall session logs showing source IP, destination IP, destination port, bytes transferred, and session duration for any connections matching First VPN Service CIDRs or associated ASNs. Export proxy access logs (Squid: `/var/log/squid/access.log`; Zscaler/Bluecoat: connection detail reports) filtering on destination IPs in the FBI advisory. Preserve DNS resolver query logs (Windows DNS debug log or BIND query log) for any hostnames resolving to First VPN Service infrastructure — these may reveal internal hosts initiating outbound tunnels before the block is applied.

Step 2: Detection — Query perimeter logs, SIEM, and DNS resolver logs for connections associated with First VPN Service IP ranges and domains identified in the FBI advisory (validate the advisory URL with your team before treating IOCs as confirmed). Look for behavioral indicators per NIST SI-4 (System Monitoring): high-frequency authentication failures (T1110), scanning patterns from unfamiliar IP ranges (T1595), and VPN connections not matching your approved VPN provider list. Enable CIS 8.2 (Collect Audit Logs) across all perimeter devices if not already active.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1110 (Brute Force), MITRE ATT&CK T1595 (Active Scanning), MITRE ATT&CK T1078 (Valid Accounts)

Compensating: Without a SIEM, use PowerShell to query Windows Security Event Log for Event ID 4625 (Failed Logon) with source IPs matching First VPN Service CIDRs: `Get-WinEvent -FilterHashtable @{LogName='Security';Id=4625} | Where-Object {$_.Message -match ''} | Select-Object TimeCreated, Message`. For Linux SSH brute-force from First VPN IPs, run: `grep 'Failed password' /var/log/auth.log | awk '{print $11}' | sort | uniq -c | sort -rn`. Deploy the free Sigma rule 'Multiple Failed Logins from Single Source' (https://github.com/SigmaHQ/sigma) converted to Windows Event Log format. Use Zeek (formerly Bro) on a network tap to generate conn.log entries and filter on First VPN ASNs.

Evidence: Collect Windows Security Event Log entries for Event ID 4625 (Failed Logon), 4624 (Successful Logon — Type 3 Network and Type 10 RemoteInteractive), and 4648 (Logon Using Explicit Credentials) where the source IP falls within First VPN Service IP ranges — these are the credential abuse indicators the FBI advisory specifically attributes to actors using this infrastructure. Pull firewall deny/allow logs for T1595 scanning signatures: rapid sequential connection attempts across multiple destination ports from a single First VPN egress IP within a short time window (e.g., >100 distinct destination ports in 60 seconds). Capture VPN gateway authentication logs (Cisco ASA: `show vpn-sessiondb`, Palo Alto: Monitor > Logs > GlobalProtect) for sessions originating from First VPN Service IP space that authenticated successfully — these represent the highest-priority pivot for T1078 valid account abuse investigation.

Step 3: Eradication — This is an infrastructure threat, not a patchable vulnerability. Eradication means policy enforcement: enforce an approved VPN allowlist per NIST AC-17 (Remote Access) and block unauthorized VPN protocols at the network boundary. Disable or restrict any accounts showing authentication anomalies correlated with First VPN Service egress IPs. Rotate credentials for any accounts flagged in log review per D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-17 (Remote Access), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export your VPN gateway's allowed peer IP list and diff against your approved remote access CIDR allowlist — any session originating from First VPN Service ASNs that authenticated successfully requires immediate account disable. Use PowerShell: `Disable-ADAccount -Identity ` for each flagged account. For credential rotation without a PAM tool, force immediate password reset via AD: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)` combined with `Set-ADUser -Identity -ChangePasswordAtLogon $true`. Block unauthorized VPN protocols at the perimeter using firewall rules targeting OpenVPN (UDP/1194),

WireGuard (UDP/51820), and PPTP (TCP/1723) on non-approved destination IPs.

Evidence: Before disabling accounts, preserve a point-in-time export of Active Directory last logon timestamps, group memberships, and recent password change history for all flagged accounts: `Get-ADUser -Filter * -Properties LastLogonDate, MemberOf, PasswordLastSet | Export-CSV flagged_accounts.csv`. Capture RADIUS or VPN gateway session logs showing the full authentication chain for any successful logins from First VPN Service IPs — this establishes whether threat actors achieved persistent access prior to containment. If any flagged account has elevated privileges (Domain Admin, local Administrator), collect a shadow copy or VSS snapshot of the domain controller's NTDS.dit and SYSTEM hive BEFORE credential rotation to preserve forensic state: `ntdsutil 'activate instance ntds' 'ifm' 'create full C:\forensic_snapshot' quit quit`.

Step 4: Recovery — Validate that detection rules and egress blocks are active and logging correctly. Confirm SIEM is alerting on connections to anonymization infrastructure. Cross-reference any incidents flagged during containment against known ransomware precursor behaviors (T1078 valid account use followed by T1486 deployment). Monitor authentication logs for 72 hours post-containment for residual brute-force activity per NIST AU-6 (Audit Record Review, Analysis, and Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST CP-2 (Contingency Plan), CIS 7.2 (Establish and Maintain a Remediation Process), MITRE ATT&CK T1078 (Valid Accounts), MITRE ATT&CK T1486 (Data Encrypted for Impact)

Compensating: Without a SIEM, run a scheduled PowerShell task every 15 minutes for the 72-hour watch period that queries Event ID 4625 (Failed Logon) and 4624 (Successful Logon) and writes matches against First VPN IOC ranges to a centralized log file — alert via email using `Send-MailMessage` if threshold is exceeded. To verify egress blocks are holding, run periodic external lookups: `curl -s https://check.torproject.org/api/ip` from each monitored host as a canary — if this resolves through an anonymizer, your block has failed. For ransomware precursor detection without EDR, deploy Sysmon with the SwiftOnSecurity config and monitor Event ID 1 (Process Create) for `vssadmin.exe delete shadows` or `wbadmin.exe delete catalog` — both are near-universal ransomware pre-deployment indicators associated with the 25+ groups the FBI linked to First VPN Service.

Evidence: During the 72-hour monitoring window, continuously collect: Windows Security Event Log Event ID 4688 (Process Creation, requires audit policy enabled) filtering on `vssadmin.exe`, `wbadmin.exe`, `bcdedit.exe`, and `cipher.exe` with arguments indicating shadow copy deletion or encryption — these are ransomware staging behaviors attributed to the groups using First VPN infrastructure. Preserve firewall session logs in real-time to detect any re-establishment of connections to First VPN Service IP space that would indicate a persistent implant or second-stage C2 channel survived containment. Capture authentication logs (Windows Event ID 4624 Type 3) for any lateral movement from hosts that previously had inbound connections from First VPN Service egress IPs — post-containment lateral movement from an already-compromised internal host is the primary residual risk.

Step 5: Post-Incident — Conduct a gap assessment against NIST AC-6 (Least Privilege) and AC-2 (Account Management) to identify over-privileged accounts that could be exploited via credential abuse. Evaluate whether your IP-reputation-based detections are supplemented by behavioral analytics, since anonymization infrastructure renders pure IP blocking insufficient. Document findings and update your threat intelligence feed with validated First VPN Service IOCs.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST RA-3 (Risk Assessment), NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run a free BloodHound Community Edition analysis to map AD privilege paths and identify accounts reachable from internet-facing systems that have excessive rights — this directly addresses the credential abuse vector used by First VPN-proxied threat actors. Export all accounts with AdminCount=1 in AD: `Get-ADUser

-LDAPFilter '(adminCount=1)' -Properties AdminCount, LastLogonDate | Export-CSV privileged_accounts.csv` and review for accounts that had any authentication events correlated with First VPN Service IP ranges during the incident window. For behavioral detection improvement without a commercial SIEM, deploy the free OpenSearch SIEM stack with pre-built Sigma rules covering T1110 (Brute Force) and T1078 (Valid Accounts) converted using `sigmac` — this provides durable behavioral coverage that survives IP rotation by anonymization infrastructure.

Evidence: Retain all raw firewall session logs, DNS resolver query logs, VPN gateway authentication logs, and Windows Security Event Logs collected during this incident for a minimum of 12 months per NIST AU-11 (Audit Record Retention) — First VPN Service has been active since 2014 and linked actors may return using the same or rotated infrastructure. Compile a final IOC artifact package including: all First VPN Service IP ranges and ASNs observed in your environment, internal hostnames that initiated or received connections tied to this infrastructure, and account names associated with anomalous authentication events — format as STIX 2.1 or a simple CSV for ingestion into your threat intel feed. Preserve the full AD audit trail (Event ID 4720 account created, 4728/4732/4756 group membership changes, 4738 account modified) for the 30 days preceding detection to identify any persistence mechanisms established by actors who accessed your environment through First VPN Service infrastructure before you had visibility.

Detection Guidance

Query SIEM and firewall logs for outbound connections to IP ranges and domains listed in the FBI advisory (validate advisory URL before operationalizing IOCs). Detection priorities aligned to MITRE techniques: (1) T1110, alert on repeated authentication failures across VPN, RDP, and web application login endpoints; threshold: 5+ failures within 60 seconds per source IP (NIST AU-2 event logging required). (2) T1595, detect port scanning and service enumeration patterns originating from unfamiliar or newly observed external IP ranges. (3) T1090.003, flag connections matching known anonymization service infrastructure (Tor exit nodes, commercial anonymizer ranges, bulletproof hosting ASNs). (4) T1078, correlate successful logins from IP ranges associated with anonymization services with off-hours access or access from geographic anomalies. D3-LAM (Local Account Monitoring) should be applied to privileged accounts. D3-SFA (System File Analysis) can surface unauthorized configuration changes that may follow initial access. D3-MFA (Multi-factor Authentication) enrollment status should be audited for all externally-exposed accounts per CIS 6.3 and CIS 6.5.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`First VPN Service infrastructure — specific domains not confirmed in available sources`	FBI advisory identifies First VPN Service as the operator; specific IOCs (IPs, domains, hashes) should be obtained directly from the validated FBI advisory before operationalizing	LOW

Framework Mappings

MITRE-ATTACK

- **T1090.003** — Multi-hop Proxy
- **T1583.003** — Virtual Private Server
- **T1090** — Proxy

- **T1078** — Valid Accounts
- **T1595** — Active Scanning
- **T1486** — Data Encrypted for Impact
- **T1110** — Brute Force

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-7** — Unsuccessful Logon Attempts
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090.003	Multi-hop Proxy	Command-And-Control
T1583.003	Virtual Private Server	Resource-Development
T1090	Proxy	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1595	Active Scanning	Reconnaissance
T1486	Data Encrypted for Impact	Impact
T1110	Brute Force	Credential-Access

Sources

Source	URL	Tier
gemini	https://industrialcyber.com/fbi-links-first-vpn-service-to-ransomwa...	T3
FBI links First VPN Service to ransomware gangs, botnets, criminal ...	https://industrialcyber.co/ransomware/fbi-links-first-vpn-service-t...	T3
The #FBI has released an advisory on ransomware groups' use of ...	https://www.facebook.com/FBIBaltimore/posts/the-fbi-has-released-an...	T3
The FBI has released an advisory on ransomware groups' use of the ...	https://www.instagram.com/p/DYnrvQvjjvQ/	T3
First VPN Service / Criminal Anonymization Infrastructure	https://techjacksolutions.com/scc-vendor-rollup/first-vpn-service-c...	T3

Generated 2026-05-27 14:07 UTC by TJS Security Command Center