INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 19:02 UTC

Europol Dismantles 'First VPN' Cybercriminal Infrastructure in Operation Saffron

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0350
Type	Threat Campaign
Severity	HIGH
Affected Products	First VPN service infrastructure, 33 servers, 3 domains seized; users include ransomware operators, fraudsters, and data theft actors
Published	2026-05-21
Discovery Source	Gemini

Executive Summary

On May 19-20, 2026, Europol, French, and Dutch authorities seized 'First VPN,' a bulletproof VPN service that ransomware operators, fraudsters, and data thieves used to conceal attack origins. Thirty-three servers and three domains were taken offline, and at least one administrator was arrested. Organizations previously targeted by ransomware groups that relied on this infrastructure may see a temporary reduction in operational tempo from those actors, though the broader criminal ecosystem will adapt to alternative anonymization services.

Technical Analysis

Operation Saffron dismantled First VPN, a bulletproof hosting-adjacent VPN service that provided anonymization infrastructure to cybercriminal operators. The service offered no-log policies, cryptocurrency payment acceptance, and abuse-resistant hosting, consistent with MITRE ATT&CK T1090 (Proxy), T1090.003 (Multi-hop Proxy), T1583 (Acquire Infrastructure), and T1583.006 (Web Services). Thirty-three servers and three domains were seized across the May 19-20 operation. No CVE is associated; this is infrastructure-layer disruption rather than a software vulnerability. At least one administrator arrest was reported by Hackread. No confirmed IOC list (IPs, domains) has been publicly released by Europol or participating authorities as of this writing. Ransomware operators who relied on First VPN for operational security will migrate to alternative bulletproof VPN or proxy services; defenders should not treat this takedown as eliminating associated threat actors.

Action Checklist

1. Step 1: Preparation. Designate a threat intelligence monitor to watch for Europol or CISA publication of First VPN infrastructure IOCs (IPs, domains). Upon release, ingest confirmed indicators into firewall and endpoint blocklists per NIST SC-7 (Boundary Protection).
2. Step 2: Detection. Query DNS and proxy logs for connections to recently seized domains or flagged IP ranges once Europol releases official IOCs; monitor for multi-hop proxy patterns in network flow data consistent with T1090.003; enable logging per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) if not already active across all egress points.
3. Step 3: Eradication. No software patch applies. If your organization's assets were previously targeted by ransomware groups known to use bulletproof VPN infrastructure, audit for persistence mechanisms, unauthorized accounts, and lateral movement artifacts; reference NIST IR-4 (Incident Handling) procedures.
4. Step 4: Recovery. Validate that perimeter controls block confirmed First VPN infrastructure ranges once released; monitor for uptick in reconnaissance or phishing activity from actors who may be re-establishing operational infrastructure; review SIEM alerting rules for multi-hop proxy abuse (T1090.003) per NIST SI-4 (System Monitoring).
5. Step 5: Post-Incident. Treat this takedown as a prompt to audit reliance on network-level attribution for threat actor identification; threat actors will migrate to new anonymization infrastructure rapidly. Review controls against T1583 (Acquire Infrastructure) and T1583.006; assess whether your detection posture identifies malicious behavior independent of source IP reputation.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if forensic review of DNS, proxy, or NetFlow logs confirms that internal assets communicated with First VPN infrastructure during a known active ransomware campaign window against your organization, or if post-seizure phishing or reconnaissance volume increases >200% over 7-day baseline — either condition indicates your organization was a specific target of actors who relied on First VPN, triggering NIST IR-6 (Incident Reporting) obligations and potential breach notification assessment if PII/PHI was accessible on affected systems.
Recovery Notes	Monitor perimeter and DNS logs for 60 days post-May 20, 2026, as ransomware groups and fraud actors formerly reliant on First VPN are expected to reconstitute on alternative bulletproof providers (a pattern documented after VPNLab.net, Sky ECC, and DoubleVPN takedowns). Verify that detection rules targeting T1090.003 multi-hop proxy behavior remain active and are not generating false-positive suppression fatigue that would mask legitimate re-attack attempts. If any endpoint is confirmed to have received a ransomware precursor payload (dropper, Cobalt Strike beacon, or RAT) during the period First VPN was operational, treat that asset as compromised and reimage from known-good baseline before returning to production.

Forensic Artifacts	DNS resolver query logs (Windows DNS debug log at %SystemRoot%\System32\dns\dns.log, or BIND query log on Linux) covering February–May 2026: lookups to the three seized First VPN domains are direct evidence of attacker infrastructure use from within your network. | Firewall and proxy egress logs showing outbound TCP sessions to First VPN's 33 seized server IPs — specifically long-duration CONNECT tunnel sessions on ports 443, 1194, or 8080 consistent with VPN-over-HTTPS obfuscation used by bulletproof providers to blend with legitimate traffic. | Windows Security Event Log Event IDs 4624 (Logon Type 3/10), 4720 (Account Created), and 4776 (Credential Validation) from domain controllers during any window when First VPN was providing anonymization cover for an active campaign against your environment — these establish whether lateral movement occurred behind the VPN screen. | NetFlow or IPFIX records showing asymmetric bidirectional traffic ratios to First VPN CIDR blocks: ransomware operators exfiltrating data through the service would produce high-outbound-volume sessions inconsistent with browsing patterns, a behavioral artifact independent of IP reputation. | Linux `/var/log/auth.log` and Windows Security Event 4648 (Explicit Credential Use) on internet-facing hosts: threat actors using First VPN to anonymize RDP/SSH brute-force or credential-stuffing attacks would leave failed and successful authentication sequences in these logs even after the VPN infrastructure was seized.

Per-Action IR Details

Step 1: Containment — Review threat intelligence feeds for any First VPN-associated IPs or domains released by Europol or CISA post-operation; block confirmed indicators at perimeter firewall per NIST SC-7 (Boundary Protection) as soon as an authoritative IOC list is published.

NIST Phase: Containment

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

Controls: NIST SC-7 (Boundary Protection), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Monitor Europol and CISA for official First VPN IOC releases — as of this operation, no authoritative CISA advisory IOC list has been published; check https://www.cisa.gov/news-events/alerts and Europol press releases directly. Once IPs are confirmed, apply block rules via: `iptables -I INPUT -s -j DROP && iptables -I OUTPUT -d -j DROP`. For pfSense/OPNsense environments, import the confirmed CIDR list into Aliases > Bulk Import and apply to egress WAN rules. Do NOT preemptively block unverified ranges — First VPN infrastructure overlapped with legitimate hosting providers on shared infrastructure.

Evidence: Before blocking, capture current NetFlow or firewall state tables showing any active sessions to First VPN IP ranges to preserve evidence of prior connectivity. Export firewall connection logs covering the 90-day window preceding May 19, 2026 (the seizure date) — any outbound sessions to the 33 seized servers during active ransomware campaigns against your org are high-value artifacts. Preserve PCAP of any flagged sessions before the block rule terminates them: `tcpdump -w firstVPN_preflight_$(date +%Y%m%d).pcap -i eth0 dst `.

Step 2: Detection — Query DNS and proxy logs for connections to recently seized domains or flagged IP ranges once Europol releases official IOCs; monitor for multi-hop proxy patterns in network flow data consistent with T1090.003; enable logging per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) if not already active across all egress points.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Query DNS resolver logs (bind query log, Windows DNS debug log at %SystemRoot%\System32\dns\dns.log) for lookups against the three seized First VPN domains once officially named. For multi-hop proxy detection consistent with T1090.003, use Zeek (formerly Bro) with the conn.log to identify

sequential TCP sessions where the destination IP is a known VPN/proxy exit node, then immediately establishes an outbound session to a third host within the same flow window. Sigma rule hunting: apply SigmaHQ's 'proxy_connection_potential_ta0011' rule family filtered on egress traffic with TTL anomalies indicating double-encapsulation. On Windows endpoints, run: `Get-WinEvent -LogName 'Microsoft-Windows-DNS-Client/Operational' | Where-Object {$_.Message -match ''}` after enabling DNS client operational logging via `wevtutil sl Microsoft-Windows-DNS-Client/Operational /e:true`.

Evidence: Preserve 90-day DNS query logs from internal resolvers covering the pre-seizure period (February–May 2026) — lookups to First VPN domains during active threat actor campaigns against your environment are direct evidence of attacker C2 routing. Capture proxy/Squid access logs showing CONNECT tunnel establishments to First VPN IP ranges with destination port 443 or 1194, which ransomware operators used to proxy RDP and C2 traffic through this bulletproof service. Export NetFlow records showing asymmetric session durations (long-lived outbound TCP connections characteristic of VPN tunneling) to First VPN CIDR blocks.

Step 3: Eradication — No software patch applies. If your organization's assets were previously targeted by ransomware groups known to use bulletproof VPN infrastructure, audit for persistence mechanisms, unauthorized accounts, and lateral movement artifacts; reference NIST IR-4 (Incident Handling) procedures.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Since First VPN was used by ransomware operators, fraudsters, and data theft actors to conceal attack origins, the seizure is a trigger — not a cause — for compromise auditing. Run Autoruns (Sysinternals) on all endpoints that communicated with First VPN IPs to identify persistence: `autorunsc.exe -a * -c -h -s > autoruns_output.csv`. Query Active Directory for accounts created or modified during the window when your org's data was potentially accessed via First VPN-anonymized sessions: `Get-ADUser -Filter * -Properties Created,LastLogonDate | Where-Object {$_.Created -gt (Get-Date).AddDays(-90)}`. For Linux hosts, check `/etc/cron*`, `/etc/systemd/system/`, and `~/.ssh/authorized_keys` for unauthorized entries. Use YARA rules from the YARA-Forge project targeting common ransomware dropper patterns associated with groups (LockBit, BlackCat/ALPHV, Play) known to use bulletproof VPN services.

Evidence: Before any remediation, image affected systems using FTK Imager or `dd` to preserve forensic state. Collect Windows Security Event Log Event ID 4720 (account created), 4728/4732 (group membership changes), and 4624 Type 3/10 (network/remote interactive logons) from domain controllers covering the period threat actors may have operated through First VPN. On Linux, collect `/var/log/auth.log` and `/var/log/secure` for SSH authentication events and `last -F` output. Export scheduled tasks (`schtasks /query /fo CSV /v > tasks.csv`) and services (`sc query type= all state= all > services.csv`) from all servers that had any connectivity to First VPN IP ranges.

Step 4: Recovery — Validate that perimeter controls block confirmed First VPN infrastructure ranges once released; monitor for uptick in reconnaissance or phishing activity from actors who may be re-establishing operational infrastructure; review SIEM alerting rules for multi-hop proxy abuse (T1090.003) per NIST SI-4 (System Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST SC-7 (Boundary Protection), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Historical precedent from similar bulletproof VPN takedowns (VPNLab.net, 2022; Sky ECC, 2021) shows threat actors reconstitute infrastructure within 2–8 weeks. Establish a 60-day elevated monitoring window from May 20, 2026. Deploy Suricata with ET Open ruleset and enable rules in the 'policy' and 'trojan' categories targeting proxy chaining and VPN tunneling heuristics. For phishing surge detection without a SIEM, configure a cron job to parse MTA logs (`grep 'status=bounced\|reject' /var/log/mail.log | awk '{print $7}' | sort | uniq -c | sort -rn`) and alert on volume spikes exceeding 2x baseline. Validate firewall block rules are active: `iptables -L OUTPUT -n -v | grep ` and

confirm zero-byte counters are incrementing on match.

Evidence: Monitor IDS/IPS alert logs for signatures matching T1090.003 multi-hop proxy patterns — specifically sequential connection chains where your hosts appear as an intermediate relay rather than a true source or destination. Capture any new phishing lures received post-May 20, 2026 and check sending infrastructure against emerging IOCs from threat intel feeds (OTX, MISP community) for overlap with actors previously attributed to First VPN usage. Log all firewall rule hits on First VPN CIDR blocks for 60 days; non-zero hit counts post-seizure may indicate a threat actor retrying from habit or testing whether your defenses changed.

Step 5: Post-Incident — Treat this takedown as a prompt to audit reliance on network-level attribution for threat actor identification; threat actors will migrate to new anonymization infrastructure rapidly. Review controls against T1583 (Acquire Infrastructure) and T1583.006; assess whether your detection posture identifies malicious behavior independent of source IP reputation.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a detection coverage gap analysis against T1583.006 (Web Services infrastructure acquisition) using ATT&CK Navigator — export your current detection layer coverage and identify blind spots in infrastructure acquisition TTPs that would expose you when actors like those using First VPN migrate to new bulletproof services. As a concrete behavioral detection not reliant on IP reputation: deploy a Sigma rule detecting anomalous outbound connection volume from a single internal host to >5 distinct /24 subnets within a 10-minute window (`sigma/rules/network/net_connection_win_many_unique_destinations.yml` from SigmaHQ). Document lessons learned within 30 days per NIST 800-61r3 §4 — specifically: did any detection fire on First VPN traffic during the pre-seizure period, or did the bulletproof VPN successfully obscure attacker origin entirely? That answer determines your detection posture gap severity.

Evidence: Pull historical SIEM or firewall alert data to determine whether any behavioral detections (not IP-reputation-based) fired for sessions routed through First VPN infrastructure during its operational period — this retrospective analysis reveals whether your detection program would have caught the underlying malicious behavior absent the takedown news. Review threat intel platform (MISP, OpenCTI, or manual TIP) tagging to assess how many of your current threat actor profiles rely primarily on IP/domain IOCs versus behavioral TTPs; if >60% of your actor profiles are IOC-anchored rather than TTP-anchored, that is a structural detection gap this operation has exposed.

Detection Guidance

No official IOC list (IPs, domains, hashes) has been publicly confirmed by Europol as of this writing, this is a critical gap. Detection should focus on behavioral indicators rather than static blocklists until official indicators are released. Monitor for: (1) outbound connections traversing multiple anonymizing proxy hops (T1090.003) in network flow/proxy logs; (2) use of VPN exit nodes with no-log reputation in threat intelligence enrichment; (3) anomalous encrypted tunnel establishment to non-business-purpose infrastructure. Reference NIST AU-6 (Audit Record Review) for log analysis cadence and AU-12 (Audit Record Generation) to confirm logging is active on perimeter and endpoint systems. Apply local account monitoring to detect any lateral movement artifacts if your environment was previously a ransomware target. When Europol or CISA publish confirmed infrastructure IOCs, ingest immediately into SIEM and firewall blocklists.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`first.vpn (unconfirmed — representative of seized domains; official domain list not yet publicly released by Europol)`	Three domains seized during Operation Saffron; authoritative list not yet published	LOW

Framework Mappings

MITRE-ATTACK

- **T1090** — Proxy
- **T1583** — Acquire Infrastructure
- **T1583.006** — Web Services
- **T1090.003** — Multi-hop Proxy

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

NIST-800-53R5

- **CP-9** — System Backup
- **IR-4** — Incident Handling

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090	Proxy	Command-And-Control
T1583	Acquire Infrastructure	Resource-Development
T1583.006	Web Services	Resource-Development
T1090.003	Multi-hop Proxy	Command-And-Control

Sources

Source	URL	Tier
Authorities dismantle First VPN, used by ransomware actors	https://www.helpnetsecurity.com/2026/05/21/operation-saffron-first-...	T3
Police seize “First VPN” service used in ransomware, data theft attacks	https://www.bleepingcomputer.com/news/security/police-seize-first-v...	T3
Police op targets VPN service favoured by ransomware gangs	https://www.computerweekly.com/news/366643536/Police-op-targets-VPN...	T3
Global law enforcement operation takes First VPN offline	https://securityaffairs.com/192491/cyber-crime/global-law-enforceme...	T3
Europol Seizes First VPN Used by Ransomware Gangs, Arrests ...	https://hackread.com/europol-seizes-first-vpn-ransomware-administra...	T3

Generated 2026-05-21 19:02 UTC by TJS Security Command Center