INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-22 18:53 UTC

Criminal VPN Infrastructure Serving 25 Ransomware Groups Dismantled in 18-Nation Operation

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0352
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	First VPN Service (1vpns[.]com, 1vpns[.]net, 1vpns[.]org); 32-node, 27-country exit network; protocols: OpenVPN, WireGuard, Outline, VLESS/Reality, L2TP/IPSec, PPTP
Published	2026-05-22T13:35:02
Discovery Source	Rss

Executive Summary

A coordinated 18-nation law enforcement operation on May 19-20, 2026, dismantled First VPN Service, a criminal anonymization platform operational since 2014 that served as shared infrastructure for at least 25 ransomware affiliate groups. Thirty-three servers were seized across 27 countries, three domains (1vpns[.]com, 1vpns[.]net, 1vpns[.]org) were seized and taken offline, and the service administrator was identified and interviewed by Ukrainian authorities. The disruption removes a key anonymization layer from active ransomware campaigns, but the underlying threat groups retain operational capability and will likely migrate to alternative infrastructure.

Technical Analysis

First VPN Service (1vpns[.]com, 1vpns[.]net, 1vpns[.]org) operated a 32-node exit network spanning 27 countries, providing anonymized egress routing to ransomware affiliates. The service supported OpenVPN, WireGuard, Outline, VLESS/Reality, L2TP/IPSec, and PPTP. PPTP is a deprecated protocol with documented cryptographic weaknesses per RFC 3748 and related analyses. MS-CHAPv2, commonly used with PPTP, has known vulnerabilities documented in academic cryptographic analysis. RC4 encryption is prohibited by NIST per RFC 7465 and offers no meaningful confidentiality. The deliberate support for legacy protocols indicates an effort by the service operators to maximize affiliate compatibility across heterogeneous client bases. MITRE ATT&CK techniques associated with this infrastructure include T1090 (Proxy), T1090.003 (Multi-hop Proxy), T1583 (Acquire Infrastructure), T1583.003 (Virtual Private Server), T1041 (Exfiltration Over C2 Channel),

T1071.001 (Web Protocols), T1665 (Hide Infrastructure), T1046 (Network Service Discovery), and T1486 (Data Encrypted for Impact). No CVE or CWE identifiers are associated with this campaign. The operation was led by France and the Netherlands, coordinated through Europol, Eurojust, and the FBI. Primary source: FBI/IC3 Joint Cybersecurity Advisory (ic3.gov/CSA/2026/260521.pdf).

Action Checklist

1. Containment: Block the three confirmed domains (1vpns[.]com, 1vpns[.]net, 1vpns[.]org) at DNS and perimeter firewall immediately. Add to deny lists in your SIEM, EDR, and proxy. These domains are seized but historical DNS resolutions may still appear in log data as indicators of prior compromise.
2. Detection: Query firewall, proxy, and DNS logs for any connections to 1vpns[.]com, 1vpns[.]net, or 1vpns[.]org going back at least 90 days. Hunt for outbound PPTP (TCP/1723, GRE protocol 47) connections to external IPs, PPTP has no legitimate business use in 2026 and should be disabled. Flag L2TP/IPSec (UDP/500, UDP/4500, UDP/1701) if not explicitly authorized for legacy VPN concentrators; most organizations have migrated to IPSec or WireGuard. Cross-reference against NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs) to confirm log coverage exists for the relevant timeframes.
3. Eradication: If any internal systems show connections to this infrastructure, treat them as potentially compromised. Isolate affected hosts, rotate credentials for any accounts active on those systems (NIST AC-2: Account Management; CISA D3-CRO: Credential Rotation), and initiate your ransomware incident response playbook. Disable PPTP on all internal VPN concentrators and gateways, it poses unacceptable cryptographic risk and viable modern alternatives exist (WireGuard, IKEv2, OpenVPN). No new deployments should use PPTP.
4. Recovery: After credential rotation and host remediation, validate that no unauthorized persistence mechanisms remain (CISA D3-SICA: System Init Config Analysis; D3-SFA: System File Analysis). Monitor for renewed outbound multi-hop proxy activity (T1090.003) for a minimum of 30 days post-remediation. Confirm audit logging is intact and tamper-evident per NIST AU-9 (Protection of Audit Information).
5. Post-Incident: The 25+ affiliated ransomware groups retain operational capability and will migrate to replacement anonymization infrastructure. Update threat hunt hypotheses to target VLESS/Reality and WireGuard traffic patterns. WireGuard uses minimal protocol overhead, reducing behavioral signatures available for detection compared to legacy protocols; focus hunt rules on destination IP anomaly and egress volume patterns rather than protocol-level fingerprinting. Review whether your organization enforces least-privilege egress (NIST AC-6) and has documented procedures for identifying unauthorized VPN software on endpoints (CIS 2.3: Address Unauthorized Software; CIS 2.1: Establish and Maintain a Software Inventory).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate to senior IR leadership and legal counsel immediately if any internal host shows confirmed DNS resolution or network-layer connection to First VPN Service infrastructure (1vpns[.]com/net/org or the 32-node exit network IPs), as this constitutes potential shared infrastructure overlap with active ransomware affiliate operations and may trigger mandatory breach notification obligations under HIPAA, state privacy statutes, or SEC Incident Disclosure rules if sensitive data was accessible on affected systems during the exposure window.
Recovery Notes	Post-containment recovery must include a 30-day behavioral monitoring period on all systems that touched First VPN Service infrastructure, with specific detection rules tuned for T1090.003 (Multi-hop Proxy) egress and unauthorized WireGuard or VLESS/Reality client execution, since the 25+ affiliated ransomware groups will migrate to replacement anonymization platforms rapidly following the May 19-20, 2026 disruption. Verify that all VPN concentrators and gateways have PPTP and L2TP/IPSec disabled and confirm via authenticated configuration audits rather than policy review alone, as these protocols may have been re-enabled by threat actors with prior access to gateway management interfaces. Treat any re-emergence of multi-hop proxy traffic patterns or unauthorized VPN client processes on previously affected hosts as a strong indicator of ransomware pre-positioning that survived the initial remediation and escalate immediately to full incident declaration.
Forensic Artifacts	DNS query logs (Windows DNS Server Event ID 3020 or Bind/Unbound query.log) for resolutions of 1vpns[.]com, 1vpns[.]net, 1vpns[.]org and any subdomains — timestamps establish the full window of First VPN Service client activity and anchor the exposure timeline against the known operational period of the 25+ affiliated ransomware groups | Firewall session logs showing outbound TCP/1723 (PPTP control), IP protocol 47 (GRE data channel), and UDP/1701 (L2TP) flows to non-RFC1918 destinations — PPTP's split control/data-plane design means both must appear together for a successful tunnel, and GRE flows without corresponding TCP/1723 may indicate blocked tunnel attempts that still confirm tooling presence | Windows Security Event Log Event ID 4688 (Process Creation) on any host that connected to First VPN Service infrastructure, filtered for parent-child process relationships involving cmd.exe, powershell.exe, wscript.exe, or mshta.exe — ransomware affiliates using this anonymization service were in active pre-ransomware campaign stages and these process chains indicate staging, reconnaissance, or lateral movement activity | Volatile memory images (WinPmem/LiME) from confirmed affected hosts captured before isolation, preserving in-memory artifacts of ransomware loaders, encryptors, or C2 implants that operators connected through First VPN Service may have staged but not yet executed at the time of the law enforcement disruption | Osquery or manual process enumeration results (`SELECT name, path, pid, cmdline FROM processes`) and installed software registry keys (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall) on affected hosts for WireGuard, Outline, xray, v2ray, or OpenVPN client binaries — these represent the specific client-side tooling distributed by First VPN Service and indicate an internal user or threat actor actively enrolled in the service

Per-Action IR Details

Containment — Block the three confirmed domains (1vpns[.]com, 1vpns[.]net, 1vpns[.]org) at DNS and perimeter firewall immediately. Add to deny lists in your SIEM, EDR, and proxy. These domains are seized but historical DNS resolutions may still appear in log data as indicators of prior compromise.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on

End-User Devices)

Compensating: On Linux/pfSense gateways run: `iptables -A OUTPUT -d 1vpns.com -j DROP && iptables -A OUTPUT -d 1vpns.net -j DROP && iptables -A OUTPUT -d 1vpns.org -j DROP`. For Windows DNS blocking without enterprise tooling: add all three domains to the local DNS server's Response Policy Zone (RPZ) or add them to Windows hosts files via GPO pointing to 0.0.0.0. For proxy-less environments, use Pi-hole or bind9 RPZ to sinkhole the three domains and capture any future resolution attempts for forensic value — the sinkholes will generate alerts on hosts that still attempt to beacon.

Evidence: Before blocking, capture and preserve all historical DNS query logs showing resolutions of 1vpns[.]com, 1vpns[.]net, and 1vpns[.]org — these timestamps establish the window of potential First VPN Service use and anchor your compromise timeline. Export firewall session state tables showing any active or recently terminated sessions to the 32-node exit network's IP ranges before the block rules are applied, as active sessions may indicate currently running ransomware-affiliated tooling. Document the resolved IP addresses returned by these three domains in your environment's DNS cache prior to block deployment, since those IPs may map to specific seized server nodes and help correlate with threat intel from the law enforcement seizure.

Detection — Query firewall, proxy, and DNS logs for any connections to 1vpns[.]com, 1vpns[.]net, or 1vpns[.]org going back at least 90 days. Hunt for outbound PPTP (TCP/1723, GRE protocol 47) and L2TP (UDP/1701) connections to external IPs — neither protocol should be in use for legitimate business egress. Cross-reference against NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs) to confirm log coverage exists for the relevant timeframes.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For DNS log hunting without a SIEM, use PowerShell against Windows DNS Server analytical logs: `Get-WinEvent -LogName 'Microsoft-Windows-DNS-Client/Operational' | Where-Object {$_.Message -match '1vpns'}`. On Linux with systemd-resolved, run: `journalctl -u systemd-resolved --since '90 days ago' | grep -i '1vpns'`. For PPTP/L2TP protocol hunting on a network tap, use Wireshark/tshark: `tshark -r capture.pcap -Y 'tcp.port==1723 or udp.port==1701 or ip.proto==47'`. Deploy the Sigma rule for anomalous outbound VPN protocol traffic (sigma rule category: network_connection) tuned to flag GRE protocol 47 and TCP/1723 egress to non-RFC1918 destinations. Use Zeek (formerly Bro) conn.log filtered on proto=gre or service=pptp for retrospective PCAP analysis if full packet capture is available.

Evidence: Firewall flow logs (NetFlow/IPFIX or firewall session logs) for TCP/1723, UDP/1701, and IP protocol 47 (GRE) egress to non-RFC1918 space — PPTP specifically uses GRE as its data channel, so TCP/1723 control-plane hits without corresponding GRE flows may indicate blocked but attempted PPTP tunnels. Proxy access logs (Squid, BlueCoat, Zscaler) for HTTP CONNECT or direct GET requests to 1vpns[.]com, 1vpns[.]net, 1vpns[.]org, which would indicate a host using the First VPN Service's web-based Outline or VLESS/Reality configuration endpoints. DNS query logs (Windows DNS Server event 3020 for DNS query received, or Bind query.log) for any resolution of the three seized domains, including subdomains, for the full 90-day window — First VPN's multi-protocol architecture means enrolled clients queried these domains for configuration and authentication prior to tunnel establishment.

Eradication — If any internal systems show connections to this infrastructure, treat them as potentially compromised. Isolate affected hosts, rotate credentials for any accounts active on those systems (NIST AC-2, Account Management; D3-CRO, Credential Rotation), and initiate your ransomware incident response playbook. Disable PPTP on all internal VPN concentrators and gateways — there is no legitimate use case for it in 2026.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), CIS 4.7 (Manage Default Accounts on Enterprise Assets and

Software), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: To disable PPTP on Windows Server RRAS without enterprise tooling: `Set-VpnServerConfiguration -TunnelType Pptp -PassThru` followed by disabling the RRAS service role for PPTP in Server Manager, or via PowerShell: `Disable-NetAdapterBinding -Name '*' -ComponentID ms_pppoe`. On Linux/StrongSwan or xl2tpd gateways, comment out all `[lns default]` blocks in `/etc/xl2tpd/xl2tpd.conf` and restart the service. For credential rotation without a PAM tool, prioritize accounts with any logon events (Windows Security Event ID 4624) on isolated hosts within the 90-day detection window — export via: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.TimeCreated -gt (Get-Date).AddDays(-90)}` and triage all interactive and network logon types (Type 2, Type 3) from the affected host list.

Evidence: Before isolating any host that connected to First VPN Service infrastructure, capture a full volatile memory image using WinPmem (Windows) or LiME (Linux) — ransomware affiliates using this service likely staged tooling including encryptors, loaders, or C2 agents that may exist only in memory if the operator was mid-campaign at time of the law enforcement action. Collect Windows Security Event Log entries for Event ID 4624 (Successful Logon), 4648 (Logon with Explicit Credentials), and 4688 (Process Creation) filtered on the affected host for the full 90-day window — these will show which accounts were active and what processes ran during the period of First VPN Service connectivity. Export scheduled tasks (`schtasks /query /fo LIST /v > tasks.txt`) and run key persistence registry paths (`reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and `HKCU` equivalent) before isolation — ransomware pre-positioning commonly uses these mechanisms and they survive reboot-based remediation if not explicitly removed.

Recovery — After credential rotation and host remediation, validate that no unauthorized persistence mechanisms remain (D3-SICA, System Init Config Analysis; D3-SFA, System File Analysis). Monitor for renewed outbound multi-hop proxy activity (T1090.003) for a minimum of 30 days post-remediation. Confirm audit logging is intact and tamper-evident per NIST AU-9 (Protection of Audit Information).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Deploy Sysmon with SwiftOnSecurity's configuration (github.com/SwiftOnSecurity/sysmon-config) on all remediated hosts and enable Event ID 3 (Network Connection) logging — this will capture any renewed outbound tunneling attempts to replacement First VPN Service infrastructure or successor anonymization platforms used by the 25+ affiliated ransomware groups. For persistence validation without an EDR, run Sysinternals Autoruns (`autorunsc.exe -a * -c -h -s > autoruns_baseline.csv`) on all remediated hosts and diff against a known-good baseline — focus on the 'Scheduled Tasks,' 'Services,' and 'Boot Execute' tabs which ransomware loaders commonly abuse. Validate audit log integrity by checking Windows Event Log file hashes: `certutil -hashfile C:\Windows\System32\winevt\Logs\Security.evtx SHA256` and storing the output in a tamper-evident location (write-once S3 bucket, offline USB) per NIST AU-9.

Evidence: Before returning remediated hosts to production, collect and preserve a second Autoruns snapshot and compare it against the pre-remediation snapshot to confirm all unauthorized scheduled tasks, services, and registry run keys identified during eradication were successfully removed — pay specific attention to tasks with randomized names or Base64-encoded command arguments, which are characteristic of ransomware affiliate staging tooling. Run a file system timeline analysis using fls/mactime (Sleuth Kit) or Velociraptor's 'Windows.Forensics.Usn' artifact on remediated hosts to confirm no new executables were written to %TEMP%, %APPDATA%, or %PROGRAMDATA% after the isolation timestamp — post-isolation file writes would indicate a persistence mechanism survived the remediation. Verify that outbound NetFlow/IPFIX records from remediated hosts show no traffic to Tor exit node IP ranges, commercial VPN provider IP blocks, or the VLESS/Reality and WireGuard port ranges (UDP/51820 for WireGuard default) during the 30-day monitoring window, as the surviving 25+ ransomware groups are expected to migrate to replacement infrastructure rapidly.

Post-Incident — The 25+ affiliated ransomware groups retain operational capability and will migrate to replacement anonymization infrastructure. Update threat hunt hypotheses to target VLESS/Reality and WireGuard traffic patterns, which are harder to fingerprint than legacy protocols. Review whether your organization enforces least-privilege egress (NIST AC-6) and has documented procedures for identifying unauthorized VPN software on endpoints (CIS 2.3, Address Unauthorized Software; CIS 2.1, Establish and Maintain a Software Inventory).

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST RA-3 (Risk Assessment), NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For WireGuard traffic detection without a commercial NDR, use tshark/Zeek to hunt for UDP flows with consistent packet sizing (WireGuard handshake initiation is always 148 bytes, response is 92 bytes) and the WireGuard handshake cookie pattern on any UDP port — command: `tshark -r capture.pcap -Y 'udp and data.len==148'`. For VLESS/Reality fingerprinting, hunt for TLS ClientHello messages where the SNI field does not match the destination IP's reverse DNS — this is the core evasion mechanism Reality uses, and it will surface as SNI/IP mismatches in Zeek ssl.log or Suricata TLS metadata logs. For unauthorized VPN software inventory, deploy osquery with the query: `SELECT name, path, pid FROM processes WHERE name IN ('wg', 'wireguard', 'openvpn', 'outline-client', 'xray', 'v2ray')` — this directly targets the client-side tooling First VPN Service distributed and that successor services will similarly deploy.

Evidence: Conduct a lessons-learned review documenting the specific timeframe during which your organization had DNS resolutions or network connections to First VPN Service infrastructure, and map that window against the operational timeline of the 25+ ransomware groups known to have used this platform — the law enforcement action establishes May 19-20, 2026 as the disruption point, so any connections prior to that date represent confirmed exposure to infrastructure shared with active ransomware affiliates. Extract and retain all PCAP segments, DNS logs, firewall flows, and endpoint artifacts collected during this incident in a write-protected evidence repository for a minimum of 12 months in anticipation of potential law enforcement requests, given that the Ukrainian administrator interview and multi-nation seizure indicate active criminal prosecution that may require organizational cooperation. Update your threat hunt playbook with behavioral hypotheses specifically targeting VLESS/Reality (TLS SNI mismatch to non-existent or spoofed domains), WireGuard (anomalous UDP flows with 148/92-byte handshake patterns on non-standard ports), and multi-hop proxy chains (MITRE ATT&CK T1090.003) as the expected successor TTPs of the 25+ ransomware groups that have lost their First VPN Service anonymization layer and will rebuild operational infrastructure within days to weeks.

Detection Guidance

Primary IOC hunt: query DNS, proxy, and firewall logs for resolution or connection attempts to 1vpns[.]com, 1vpns[.]net, and 1vpns[.]org; any hit, even historical, warrants investigation. Secondary behavioral hunt: flag outbound PPTP (TCP/1723, GRE/47) to external IPs, as it should not appear in legitimate outbound traffic on a hardened network. Flag L2TP/IPSec (UDP/500, UDP/4500, UDP/1701) if not explicitly authorized for legacy infrastructure; evaluate migration timelines if found. Tertiary hunt: look for multi-hop proxy patterns (T1090.003), connections that chain through multiple external IPs in rapid succession, particularly to exit nodes in jurisdictions inconsistent with your business footprint. For environments with NDR or UEBA, create detection rules for the MITRE techniques T1665 (Hide Infrastructure) and T1090 (Proxy) using baseline deviations in egress volume and destination diversity. Validate that log sources cover the full 32-node, 27-country exit network scope; gaps in cloud or remote-site logging are the most likely blind spots. Reference NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation) to confirm required event types are captured.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`1vpns[.]com`	First VPN Service operator domain — seized May 2026; historical connections indicate prior use of criminal anonymization infrastructure	HIGH
DOMAIN	`1vpns[.]net`	First VPN Service operator domain — seized May 2026	HIGH
DOMAIN	`1vpns[.]org`	First VPN Service operator domain — seized May 2026	HIGH

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1090.003** — Multi-hop Proxy
- **T1583** — Acquire Infrastructure
- **T1071.001** — Web Protocols
- **T1583.003** — Virtual Private Server
- **T1665** — Hide Infrastructure
- **T1046** — Network Service Discovery
- **T1090** — Proxy
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

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

HIPAA-SECURITY

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1090.003	Multi-hop Proxy	Command-And-Control
T1583	Acquire Infrastructure	Resource-Development
T1071.001	Web Protocols	Command-And-Control
T1583.003	Virtual Private Server	Resource-Development
T1665	Hide Infrastructure	Command-And-Control
T1046	Network Service Discovery	Discovery
T1090	Proxy	Command-And-Control
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/first-vpn-dismantled-in-global-ta...	T3
[PDF] “First VPN Service” Used by Ransomware Actors to Compromise ...	https://www.ic3.gov/CSA/2026/260521.pdf	T1
What Are the Different Types of VPN Protocols? - Palo Alto Networks	https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols	T3
PPTP isn't industry standard....right?? : r/networking - Reddit	https://www.reddit.com/r/networking/comments/1p5p0xi/pptp_isnt_indu...	T3
Common VPN protocols and their security levels - Facebook	https://www.facebook.com/groups/GroupWhiteHat/posts/3533053460356156/	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-22 18:53 UTC by TJS Security Command Center