

Karachi, Dated: 14th September, 2026

To

1. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
2. The Chairman, Planning & Development Board, Govt. of Sindh, Karachi
3. The Chairman Sindh HEC Karachi.
4. The Senior Member Board of Revenue (BOR) Sindh, Karachi.
5. The Additional Chief Secretary, Govt of Sindh _____
6. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
7. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
8. The Administrative Secretary, Government of Sindh (All) _____
9. The Provincial Ombudsman, Sindh.
10. The Inspector General of Police Sindh, Karachi
11. The Divisional Commissioner (All) in Sindh _____

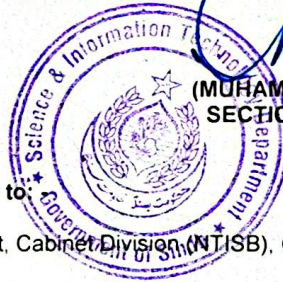
SUBJECT: CYBERSECURITY ADVISORY ON SECURITY RISKS ASSOCIATED WITH THIRD-PARTY AND HOSTILE VPN SERVICES - NECESSARY PRECAUTIONARY MEASURES

In view of the widespread use of Virtual Private Networks (VPNs) for remote connectivity and bypassing network restrictions, the attached Advisory titled "**NCA-40.310726 Security Risks Associated with Third-Party and Hostile VPN Services**" (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT Pakistan). The advisory is intended as a critical precautionary measure to address the severe privacy and national security risks introduced by third-party and free VPN services operated by hostile countries.

2. The Advisory outlines that Threat Actors (TAs) from hostile countries-specifically noting a compiled list of VPNs operated by India and Israel (Annexure A)- deliberately offer free VPN services to exploit users. It highlights severe implications, including the monitoring of all internet traffic, credential theft, data exfiltration, user profiling, and the injection of spyware or Remote Access Trojans (Rats) into enterprise systems. The advisory explicitly warns that personnel employed at sensitive setups including military, intelligence, Law Enforcement Agencies (LEAs), and government organizations at high risk of exposing operational information mission planning, and classified communications patterns if these compromised services are utilized.

3. It is requested that the attached Advisory and be associated list of hostile VPNs (Annexure A) may kindly be disseminated among all relevant departments, organizations, and personnel under your administrative oversight. Clear directives must be issued to prohibit the use of unapproved, third-party, and free VPN applications on both official systems and personal devices used by personnel in sensitive setups to safeguard national security and prevent intelligence collection by hostile entities.

Annexure: NCA-40.310726 - National CERT Advisory - Security Risks Associated with Third-Party and Hostile VPN services



(MUHAMMAD AKBAR KHAN)
SECTION OFFICER (TECH)

A copy is forwarded for information and necessary action to:

1. AS(Staff) to Chief Minister Sindh, Karachi.
2. The Assistant Secretary (NTISB), Cabinet Secretariat, Cabinet Division (NTISB), GoP.
3. PS to Chief Secretary, Sindh.
4. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
5. Staff Officer to S&IT Department, Govt. of Sindh, Karachi.
6. Webmaster, for uploading the advisory on url: <https://www.sindh.gov.pk/>

SECTION OFFICER (TECH)



National Cyber Emergency Response Team

Government of Pakistan



Annexure: NCA-40.310726

NCA-40.310726 – National CERT Advisory - Security Risks Associated with Third-Party and Hostile VPN Services

Virtual Private Networks (VPNs) are widely used to provide secure remote connectivity, protect user privacy, and bypass network restrictions. However, the use of third-party VPNs introduces distinct privacy and cybersecurity risks. These vulnerabilities are actively exploited by Threat Actors (TAs) from hostile countries who deliberately offer free VPN services to intercept and exfiltrate data.

Recently, a list of VPNs operated by hostile nations has been compiled (refer to **Annexure A**). The use of these specific VPNs poses serious cybersecurity and national security risks to Pakistan's digital infrastructure.

1. DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-40.310726
Threat Type	Cyber Espionage / Data Exfiltration / Malware Ingress
Threat Actor	State-Sponsored TAs / Hostile Intelligence Services
Attack Vector	Malicious Third-Party & Free VPN Applications
Authentication Required	None (Relies on user-initiated installation)
User Interaction	Required (Downloading and routing traffic through the VPN)
Severity	Critical (Direct Threat to National Security and Classified Operations)
Target Scope	Government, Military, Intelligence, LEAs, and Corporate Setups

2. IMPACT ANALYSIS & IMPLICATIONS

The use of free and untrusted VPNs carries severe national security risks. Following are the direct implications associated with the use of these hostile services:

- Traffic Monitoring & Interception:** Complete monitoring of internet activity by VPN operators. All internet traffic—including communications, messages, social media logs, and browsing history—passes through hostile VPN servers specifically designed to exfiltrate sensitive information.
- Credential Theft:** Harvesting of user credentials by cracking authentication tokens, session cookies, and other sensitive login data using malicious VPN infrastructure.

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad, Pakistan
+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

National Cyber Emergency Response Team

Government of Pakistan



- c. **Espionage & Intelligence Collection:** Intercepting government, military, diplomatic, and corporate information transmitted through these VPNs. This intercepted data may be utilized to support further hostile intelligence operations.
- d. **Data Exfiltration:** Covert transmission of sensitive organizational documents, internal emails, and research data to external servers operated by threat actors.
- e. **Malware & Backdoor Ingress:** Malicious VPN apps (installed on personal phones or PCs) may inject spyware, malware, Remote Access Trojans (RATs), or other backdoors directly into enterprise systems.
- f. **User Profiling & Surveillance:** Capturing user behavior, device identifiers, geolocation data, communication patterns, and app usage to build detailed intelligence profiles on key personnel.
- g. **Exposure of Sensitive Operations:** Persons employed at sensitive setups (including military, intelligence, LEAs, and government departments) using hostile/compromised VPN services may inadvertently expose operational information, mission planning, or classified communication patterns.

3. THREAT CHARACTERISTICS

Sr. No.	Characteristic	Details
a.	Threat Category	State-Sponsored Espionage / Malicious Infrastructure
b.	Threat Status	Active / Ongoing Operational Risk
c.	Root Cause	Unregulated use of third-party and free VPN applications
d.	Target Scope	Personnel in sensitive government, military, and intelligence sectors
e.	Attack Complexity	Low (Relies on voluntary download by the end-user)
f.	Affected Systems	Personal Mobile Phones, Official PCs, Laptops, Enterprise Networks
g.	Operational Risk	Covert surveillance, traffic decryption, and unauthorized access

4. INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations and IT administrators should actively monitor for:

- a. Presence of unapproved, free, or third-party VPN applications installed on official enterprise endpoints.
- b. Applications or web traffic matching the hostile VPNs listed in **Annexure A**.
- c. Unexpected outbound network connections to IP blocks geolocated to hostile territories (India, Israel) or known anonymizer nodes.
- d. Anomalous spikes in data transfers originating from devices when a VPN connection is initiated.

5. REMEDIATION ACTIONS & SUGGESTED MEASURES

5.1 Immediate Defensive Controls

Category	Suggested Actions
----------	-------------------

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad, Pakistan
+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



Annexure-A

LIST OF VPNS

Sr. No.	VPN	Origin
1	Urban VPN	Israel Origin/ Israel Ownership
2	Safer VPN	
3	Express VPN	
4	Cyber Ghost	
5	Private Internet Access	
6	Zenmate	
7	Perimter 81	
8	Cato Networks	
9	SnT Hosting	Indian Origin

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad, Pakistan
+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk