

● THREAT ALERT

# Indo–Pak Geopolitical Tensions Trigger Massive Cyber Onslaught on India's Critical Digital Infrastructure

In May 2025, amid rising Indo–Pak geopolitical tensions, India's critical digital infrastructure came under a coordinated cyber onslaught. Hacktivist groups launched large-scale multi-vector DDoS attacks targeting government portals, transport hubs, and financial services during a high-sensitivity operational window.

● Multi-Vector DDoS Surge

● Globally Distributed Botnets

● National Digital Services Stabilized

**85M+**

Malicious Requests  
Peak attack volume in a 10-hour window

**10 Hours**

Sustained Attack Window  
Continuous multi-vector assault phase

**0 sec**

Downtime  
Critical citizen services remained fully operational

**Real-Time**

Mitigation Response  
Threats detected and neutralized instantly

# A National Digital Infrastructure Under Coordinated Cyber Assault

A surge of coordinated cyberattacks targeted India's government portals, transport systems, and financial services during Indo-Pak geopolitical tensions. Systems experienced heavy load, instability, and service risk as traffic rapidly escalated.

Over 85 million malicious requests flooded critical infrastructure within 10 hours. The attack disrupted digital workflows, increased the risk of service failure, and put citizen access under pressure.

Layer 7 Attacks

API Exploits

Zero-Day Exploits

Credential Stuffing

Data Scraping

Bot Traffic

 Service Disruptions

 Infrastructure Load Pressure

 Operational Instability



### **Volumetric DDoS Floods Overwhelmed Systems**

85M+ malicious requests were generated within hours, exhausting traditional mitigation capacity.



### **Globally Distributed Botnets Masked Origins**

Attack traffic originated from thousands of IPs across multiple regions.



### **Static Defenses Failed Against Evolving Patterns**

Rule-based firewalls and manual blocking could not respond fast enough.



### **Critical Services Were Under Continuous Pressure**

Government and transport systems faced instability during peak attack conditions.

# Prophaze WAAP: Autonomous Defense for National-Scale Threat Environments

Three coordinated capabilities ensured continuous protection across India's critical infrastructure.



## Stop Threats Across All Layers

- ✓ Protected APIs and application layers simultaneously
- ✓ Analyzed traffic behavior under extreme load
- ✓ Blocked malicious requests before impact
- ✓ No manual intervention required



## AI That Detects Hidden Threats

- ✓ Identified anomalies in user and API behavior
- ✓ Detected bot-driven and automated attacks
- ✓ Adapted instantly to evolving attack patterns
- ✓ Continuously improved detection accuracy



## Secure APIs and Critical Endpoints

- ✓ Validated and sanitized every request
- ✓ Discovered exposed and shadow APIs
- ✓ Applied rate limiting at endpoint level
- ✓ Ensured only legitimate traffic passed through

# National Digital Systems Stabilized. Services Continued.

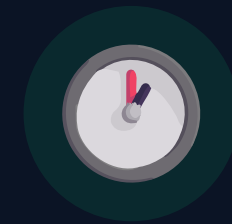
Here's what was achieved during the attack:



**85M+**

**Malicious Requests Blocked**

Neutralized across multiple attack vectors within hours



**10  
Hours**

**Continuous Attack Window**

Fully mitigated without service degradation



**0 sec**

**Zero Downtime**

Government, transport, and financial systems remained accessible



**Real-  
Time**

**Global Threat Containment**

Distributed botnets neutralized instantly across regions



**100%**

**Service Availability**

Citizen services remained fully operational throughout the attack

# What Changed When Prophaze Was in Place

✘ BEFORE PROPHAZE	✔ AFTER PROPHAZE
<p>Attack Surface Exposure</p> <ul style="list-style-type: none"><li>✘ Legacy perimeter systems struggled with multi-vector DDoS and globally distributed botnets, leaving critical government and infrastructure APIs vulnerable to saturation and disruption.</li></ul>	<p>Attack Surface Exposure</p> <ul style="list-style-type: none"><li>✔ Prophaze delivered AI-native, real-time protection across application and API layers, neutralizing attack traffic before it impacted services.</li></ul>
<p>Threat Detection &amp; Response</p> <ul style="list-style-type: none"><li>✘ Static rule-based systems failed to adapt to rapidly shifting attack patterns, delaying response during peak attack intensity.</li></ul>	<p>Threat Detection &amp; Response</p> <ul style="list-style-type: none"><li>✔ Autonomous detection engine identified anomalies instantly and triggered real-time mitigation without manual intervention.</li></ul>
<p>Traffic Handling &amp; Scalability</p> <ul style="list-style-type: none"><li>✘ Infrastructure became unstable under 85M+ request floods, leading to potential service degradation across key digital platforms.</li></ul>	<p>Traffic Handling &amp; Scalability</p> <ul style="list-style-type: none"><li>✔ Kubernetes-native scaling absorbed massive traffic spikes while maintaining consistent performance and availability.</li></ul>

*"The question is not if national systems will be targeted  
— it is whether they can stay operational under attack.  
Static defenses cannot protect modern digital  
infrastructure."*



Trusted by critical infrastructure to protect national digital ecosystems with AI-driven unified WAAP protection and real-time resilience.



**Protect Your Applications with AI-Driven Unified WAAP Platform in Minutes**