Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

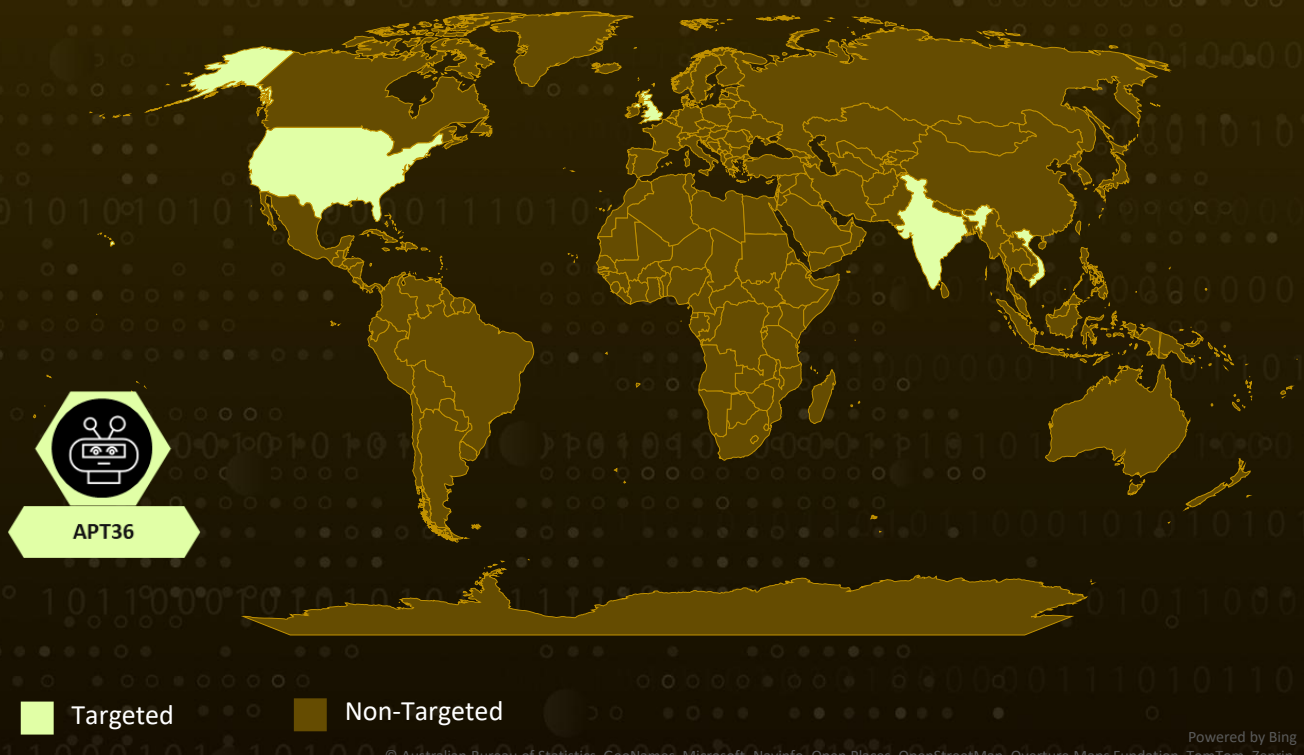
Operation TrustTrap: APT36 Weaponizes 16,800 Spoofed Domains

Date of Publication	Admiralty Code	TA Number
April 27, 2026	A1	TA2026116

Summary

First Seen: Early 2026
Targeted Regions: United States, India, Vietnam, United Kingdom
Targeted Industries: Government, Defense, Diplomatic, Transportation, Department of Motor Vehicles (DMV), Toll Payment, Healthcare (NHS-themed lures)
Threat Actor: APT36 (alias Transparent Tribe, ProjectM, TEMP.Lapis, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco)
Campaign: Operation TrustTrap
Attack: Operation TrustTrap, a coordinated phishing infrastructure of more than 16,800 malicious domains active since early 2026 that impersonates government services across the United States, India, Vietnam, and the United Kingdom. Rather than relying on technical exploits, the operators weaponize the visual trust of the ".gov" string by embedding government labels as non-root subdomain components, combined with hyphen manipulation and benign-word insertion to defeat regex-based detection while remaining legible to human readers. Spoofed portals resolve to infrastructure concentrated in Tencent Cloud and Alibaba Cloud APAC ASNs, and a distinct cluster within the dataset, including domains impersonating the National Investigation Agency (NIA) of India, exhibits TTPs consistent with the Pakistan-nexus threat actor APT36.

Attack Regions



Attack Details

#1

Operation TrustTrap is a coordinated phishing infrastructure of more than 16,800 malicious domains, active since early 2026, that impersonates government services across the United States, India, Vietnam, and the United Kingdom. The operation begins not with an exploit but with a registration. Operators bulk-register thousands of domains on cheap, disposable TLDs, holding many of them dormant as a pre-provisioned reserve until a campaign wave is triggered. Lures are then distributed through SMS, email, and adjacent social-engineering vectors, with each link engineered to look like an authentic government URL. The campaign weaponizes how humans interpret URLs rather than how machines parse them.

#2

Once a victim clicks a lure, they are redirected to a spoofed portal hosted on infrastructure concentrated within Tencent Cloud and Alibaba Cloud APAC ASN ranges. Active phishing URLs across the infrastructure consistently use a double-query-string parameter pattern that serves as a session-tracking mechanism, assigning unique identifiers to individual victims and monitoring engagement. The uniformity of this pattern across hundreds of URLs confirms a kit-driven, centrally managed operation rather than ad hoc activity. Cloned portals replicate the visual identity of the impersonated agency, often presenting fake DMV, toll, or citizen-services payment forms designed to harvest personally identifiable information, payment-card data, and credentials.

#3

The attribution-significant cluster within the dataset narrows the focus to Indian government targets and aligns operationally with APT36, a Pakistan-nexus actor with a documented record of targeting Indian government entities, defense personnel, and diplomatic infrastructure. The cluster includes APT36 impersonation domains, such as one masquerading as the National Investigation Agency. The random suffix characters mirror the automated domain-generation behavior documented in prior APT36 bulk-registration events, and the shared hosting IPs in Tencent Cloud and Alibaba APAC overlap with APT36 staging infrastructure observed in 2024 and 2025 campaigns. Attribution is assessed at moderate-to-high confidence based on the convergence of campaign overlap, infrastructure reuse, TLD and registrar patterns, India-specific trust-injection cues in the URL structure, and subdomain construction logic.

#4 The operational endgame across the broader dataset is credential and payment-data theft at scale, with secondary potential for follow-on intrusion against high-value targets in the APT36 sub-cluster. Because the campaign relies on cognitive deception rather than payload execution, traditional binary-focused detection layers see little to act on; the kit's session-tracking parameters and shared cloud-hosting infrastructure are the most reliable pivots for hunting and takedown across the campaign cluster.

Recommendations

Hunt by eTLD+1, Not by Substring: Reconfigure URL inspection to evaluate the registered eTLD+1 of every link rather than substring-matching for ".gov" or ".gov.in." Treat any URL where a government label appears as a subdomain of a non-government registered domain as high-risk by default.

Detect the Kit's Session-Tracking Pattern: Author proxy and SIEM rules that flag URLs containing the characteristic double-query-string pattern ?var1=xxxxx?var2=xxxxx, which has been observed consistently across hundreds of Operation TrustTrap phishing URLs and provides a high-confidence campaign signature.

Strengthen Domain Takedown Workflows: Establish or expand relationships with abuse contacts at Gname.com Pte. Ltd., the .bond and .cc registry operators, and Tencent Cloud and Alibaba Cloud abuse desks to accelerate takedowns of newly identified Operation TrustTrap infrastructure as the campaign continues to evolve.

Enforce Email and Messaging Authentication on Brand Properties: Government bodies and impersonated brands should enforce DMARC, SPF, and DKIM on official communication channels and publish clear citizen-facing reference URLs to reduce the success rate of look-alike-domain lures.

Deploy eTLD+1-Aware Detection Tooling: Replace legacy substring-based phishing filters with detection logic that operates on the public-suffix-list-resolved registered domain, ensuring that subdomain spoofing of government labels is treated as suspicious regardless of how the rest of the hostname is constructed.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.006: Web Services
		T1583.003: Virtual Private Server
	T1587: Develop Capabilities	
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.005: Link Target
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
	T1189: Drive-by Compromise	
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1027: Obfuscated Files or Information	
	T1656: Impersonation	
Credential Access	T1056: Input Capture	T1056.003: Web Portal Capture
Collection	T1185: Browser Session Hijacking	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	www[.]mass[.]gov-suc[.]cc, www[.]mass[.]gov-ypk[.]cc, www[.]mass[.]gov-wkg[.]cc, www[.]mass[.]gov-odb[.]cc, www[.]mass[.]gov-icw[.]cc, www[.]mass[.]gov-hjc[.]cc, www[.]mass[.]gov-emz[.]cc, www[.]gov-lzk[.]cc, www[.]az[.]gov-lzk[.]cc, www[.]az[.]gov-huv[.]cc, www[.]az[.]gov-ocq[.]cc, www[.]az[.]gov-cgt[.]cc, www[.]az[.]gov-swy[.]cc, www[.]mass[.]gov-raj[.]cc, www[.]mass[.]gov-kzc[.]cc, www[.]mass[.]gov-bza[.]cc, www[.]mass[.]gov-yta[.]cc, www[.]mass[.]gov-cen[.]cc, www[.]gov-tda[.]cc, www[.]mass[.]gov-btx[.]cc, www[.]mass[.]gov-ktx[.]cc, nh[.]gov-nde[.]cc, mass[.]gov-xct[.]cc, www[.]mass[.]gov-ufa[.]cc, www[.]mass[.]gov-iua[.]cc, www[.]mass[.]gov-nha[.]cc, www[.]mass[.]gov-uva[.]cc, www[.]mass[.]gov-ngx[.]cc, www[.]gov-cbv[.]cc, www[.]gov-wyx[.]cc, www[.]mass[.]gov-bjw[.]cc, www[.]mass[.]gov-uce[.]cc, www[.]mass[.]gov-hva[.]cc, wv[.]gov-hng[.]cc, wv[.]gov-hna[.]cc, wv[.]gov-hnd[.]cc, az[.]gov-nci[.]cc, www[.]gov-jyd[.]cc, www[.]gov-ckw[.]bond, az[.]gov-ncq[.]cc, az[.]gov-nco[.]cc,

TYPE	VALUE
Domains	www[.]gov-iop[.]cc, www[.]gov-hxi[.]cc, www[.]gov-ejx[.]bond, www[.]mass[.]gov-xct[.]cc, mass[.]gov-raj[.]cc, www[.]mass[.]gov-kse[.]cc, www[.]mass[.]gov-uca[.]cc, mass[.]gov-ucq[.]cc, mass[.]gov-nka[.]cc, wv[.]gov-qwd[.]cc, mass[.]gov-wjd[.]cc, az[.]gov-sxa[.]cc, www[.]mass[.]gov-nka[.]cc, www[.]mass[.]gov-wmc[.]cc, wv[.]gov-nvk[.]cc, az[.]gov-sxs[.]cc, www[.]michigan[.]gov-nju[.]cc, mass[.]gov-ktx[.]cc, mass[.]gov-wmc[.]cc, mass[.]gov-cre[.]cc, www[.]mass[.]gov-ucq[.]cc, ri[.]gov-jhd[.]cc, ncdot[.]gov-stmv[.]cc, ncdot[.]gov-stmn[.]cc, az[.]gov-sxb[.]cc, az[.]gov-sxc[.]cc, mass[.]gov-kzc[.]cc, az[.]gov-sxv[.]cc, az[.]gov-ncp[.]cc, mass[.]gov-tvz[.]cc, www[.]mass[.]gov-wjd[.]cc, www[.]mass[.]gov-tvz[.]cc, wv[.]gov-nvf[.]cc, mass[.]gov-uva[.]cc, mass[.]gov-ngx[.]cc, mass[.]gov-iua[.]cc, mass[.]gov-uce[.]cc, az[.]gov-sxz[.]cc, az[.]gov-sxm[.]cc, www[.]mass[.]gov-cre[.]cc, mass[.]gov-hva[.]cc, mass[.]gov-bjw[.]cc, az[.]gov-ncr[.]cc, mass[.]gov-kse[.]cc,

TYPE	VALUE
Domains	az[.]gov-sxn[.]cc, www[.]gov-yex[.]cc, www[.]az[.]gov-txb[.]bond, www[.]gov-gva[.]cc, www[.]gov-uxs[.]bond, www[.]gov-gos[.]cc, www[.]gov-tca[.]cc, ncdot[.]gov-stwt[.]cc, www[.]gov-hxw[.]cc, www[.]gov-jdz[.]bond, www[.]gov-lnx[.]bond, mass[.]gov-btx[.]cc, mass[.]gov-uca[.]cc, az[.]gov-nct[.]cc, mass[.]gov-nha[.]cc, mass[.]gov-aun[.]cc, michigan[.]gov-nju[.]cc, www[.]gov-twh[.]bond, mass[.]gov-yta[.]cc, mass[.]gov-ufa[.]cc, mass[.]gov-bza[.]cc, mass[.]gov-cen[.]cc, wv[.]gov-tqj[.]cc, ncdot[.]gov-kfo[.]cc, wv[.]gov-hns[.]cc, ncdot[.]gov-kfy[.]cc, ncdot[.]gov-uji[.]cc, ncdot[.]gov-tgy[.]cc, ncdot[.]gov-stwi[.]cc, ncdot[.]gov-stms[.]cc, ncdot[.]gov-stmf[.]cc, ncdot[.]gov-stmd[.]cc, ncdot[.]gov-stmb[.]cc, ncdot[.]gov-stma[.]cc, ncdot[.]gov-olp[.]cc, ncdot[.]gov-kfw[.]cc, ncdot[.]gov-stmc[.]cc, ncdot[.]gov-kfe[.]cc, ncdot[.]gov-yhu[.]cc, ncdot[.]gov-stmx[.]cc, ncdot[.]gov-kft[.]cc, ncdot[.]gov-iko[.]cc, ncdot[.]gov-dcf[.]cc, ncdot[.]gov-rfd[.]cc,

TYPE	VALUE
Domains	ncdot[.]gov-kfr[.]cc, ncdot[.]gov-saz[.]cc, ncdot[.]gov-kfp[.]cc, wv[.]gov-hny[.]cc, wv[.]gov-hno[.]cc, wv[.]gov-hni[.]cc, www[.]mass[.]gov-tia[.]cc, wv[.]gov-qwg[.]cc, www[.]gov-zsr[.]bond, wv[.]gov-qwk[.]cc, wv[.]gov-qwc[.]cc, utah[.]gov-aps[.]cc, www[.]gov-icw[.]cc, www[.]gov-odb[.]cc, www[.]gov-lzp[.]cc, www[.]gov-emj[.]cc, www[.]gov-enu[.]cc, www[.]gov-hjc[.]cc, www[.]gov-emz[.]cc, www[.]gov-ypk[.]cc, www[.]gov-wkg[.]cc, www[.]gov-aix[.]cc, www[.]gov-suc[.]cc, ncdot[.]gov-stda[.]cc, ncdot[.]gov-stds[.]cc, ncdot[.]gov-vro[.]cc, ncdot[.]gov-stdm[.]cc, wv[.]gov-hyj[.]cc, wv[.]gov-tlo[.]cc, wv[.]gov-cmi[.]cc, ncdot[.]gov-stdb[.]cc, ncdot[.]gov-mip[.]cc, ncdot[.]gov-gop[.]cc, az[.]gov-hae[.]cc, ncdot[.]gov-cqo[.]cc, ncdot[.]gov-stnz[.]cc, ncdot[.]gov-cqa[.]cc, ncdot[.]gov-stdx[.]cc, ncdot[.]gov-stdn[.]cc, ncdot[.]gov-cqr[.]cc, ncdot[.]gov-iop[.]cc, ncdot[.]gov-stdz[.]cc, ncdot[.]gov-stdc[.]cc, ncdot[.]gov-cqw[.]cc,

TYPE	VALUE
Domains	co[.]gov-uji[.]cc, ncdot[.]gov-stdv[.]cc, utah[.]gov-apd[.]cc, www[.]mass[.]gov-wtb[.]cc, www[.]mass[.]gov-qht[.]cc, www[.]mass[.]gov-xmj[.]cc, www[.]mass[.]gov-khw[.]cc, expresstoll[.]gov-dmre[.]cc, ncdot[.]gov-gjk[.]cc, www[.]ut[.]gov-eny[.]cc, www[.]gov-lrq[.]bond, www[.]gov-poy[.]bond, www[.]gov-tuo[.]bond, ut[.]gov-eny[.]cc, mass[.]gov-nve[.]cc, www[.]mass[.]gov-bjk[.]cc, www[.]gov-nka[.]cc, www[.]gov-uca[.]cc, www[.]gov-laq[.]bond, www[.]gov-lil[.]bond, www[.]gov-opr[.]bond, www[.]gov-ltv[.]bond, www[.]gov-btx[.]cc, www[.]gov-lrm[.]bond, www[.]gov-imk[.]bond, www[.]gov-bjk[.]cc, www[.]gov-nha[.]cc, www[.]gov-kzc[.]cc, www[.]gov-wmc[.]cc, www[.]gov-xct[.]cc, www[.]gov-hva[.]cc, www[.]gov-uva[.]cc, www[.]gov-ucq[.]cc, www[.]gov-ouo[.]bond, www[.]gov-ngx[.]cc, www[.]gov-yuq[.]bond, www[.]gov-raj[.]cc, www[.]gov-wjd[.]cc, www[.]gov-tvz[.]bond, www[.]gov-cen[.]cc, www[.]gov-ktx[.]cc, www[.]gov-ufa[.]cc, www[.]gov-uce[.]cc, www[.]gov-tia[.]cc,

TYPE	VALUE
Domains	www[.]gov-kse[.]cc, www[.]gov-nve[.]cc, www[.]gov-cre[.]cc, www[.]gov-tvz[.]cc

References

https://cyble.com/blog/operation-trusttrap-domain-spoofing-campaign/

Note: This is a representative sample of the 16,800+ domains identified in the campaign. The complete IoC list is available on the Uni5Xposure platform.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

April 27, 2026 • 06:00 AM

More at www.hivepro.com