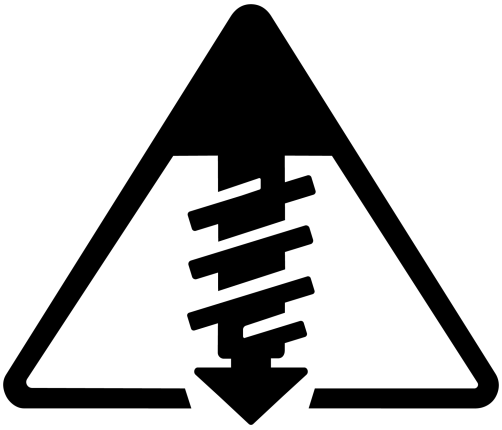
Underminr Impact Report

20260512

Date: April, 2026
Updated Datapoints: May 12, 2026
Authors: ADAMnetworks Research Team



Tags: underminr, sni-deception, cdn, pdns, preemptive-security, ech, domain-fronting

Testing Sample

4,143,199 domains in the reporting population. 1,737,903 map to CDN providers that produced a vulnerable SNI deception result. 73 CDN providers were tested at the provider level (33 vulnerable, 40 not vulnerable).

Scope of Impact

Using the following methodology we can estimate exposure beyond the measured Tranco reporting population without treating third-party market data as a secondary vulnerability scan.

The Tranco dataset establishes which providers produced a vulnerable SNI deception result. BuiltWith is then used solely to estimate how broadly those providers are deployed across live public-facing websites. This produces a provider-level exposure estimate, not a domain-level confirmation for every website represented in BuiltWith's dataset.

The most conservative external estimate focuses on providers where BuiltWith has a closely aligned CDN, WAF, or reverse-proxy category match. This mapping represents approximately 58,182,883 live websites. An expanded mapping, which also includes hosting, hosted CMS, commerce, and cloud-provider categories for providers that tested vulnerable, represents approximately 88,386,901 live websites.

These figures should be interpreted as gross provider footprint estimates. They are not deduplicated counts of unique domains, and individual websites may appear under multiple BuiltWith technology categories. The value of the estimate is directional scale: the measured Tranco results demonstrate that the vulnerability class is concentrated among major shared-edge providers, while BuiltWith data indicates those same providers collectively support tens of millions of live websites beyond the measured corpus.

External Exposure Estimate

Estimate	Current Status	Interpretation
Conservative CDN/WAF Mapping	58,182,883	Closest BuiltWith matches for CDN, WAF, or reverse-proxy providers that produced a vulnerable Underminr result.
Expanded Provider Mapping	88,386,901	Includes hosting, hosted CMS, commerce, and cloud-provider categories where the provider produced a vulnerable Underminr result.
Top 10 Vulnerable Providers	85,377,520	The top ten vulnerable providers in the Tranco report account for 98.7% of vulnerable tested domains and provide the strongest external scale signal.

research@adamnet.works

Underminr - Available Data for Visualization - Filtered Tranco Reporting Population

Data as of 2026-03-31. Source: Tranco daily full list (L7QY4). The reporting population removes .arpa names and keeps apex domains plus exact www hosts. Domains were then resolved, mapped to ASN and provider ownership, and scored from provider-level SNI deception results.

Headline Stats

Stat	Value
Source Entries	5,099,409
Domains Tested	4,143,199
Domains Vulnerable	1,737,903
Immune CDN Domains	233,767
Traditional Hosting / Not Applicable	2,105,343
CDN Providers Tested Vulnerable	33
CDN Providers Not Vulnerable	40
Data Source	Tranco daily full list (L7QY4)

Domains Vulnerable counts tested domains assigned to providers that produced a vulnerable SNI deception result. Immune CDN Domains counts tested domains on providers that did not. Traditional Hosting / Not Applicable covers 2,105,343 reviewed domains that were not on CDN infrastructure. Immune in the split below includes both the 233,767 immune CDN domains and that traditional-hosting group.

Global Domain Split

Segment	Domains	% of Tested
Vulnerable	1,737,903	42.6%
Immune	2,339,110	57.4%

Immune combines 233,767 domains on CDN/shared-edge providers that did not test vulnerable and 2,105,343 reviewed domains on traditional hosting or not-applicable infrastructure.

research@adamnet.works

Domain Coverage Breakdown

Each source entry moves through three steps: DNS resolution, ASN and provider mapping, and provider-level SNI deception classification where applicable. The tables below show where domains dropped out and how the final counts were assigned.

DNS Resolution

DNS Status	Domains	% of Source
Resolved (A record)	4,141,544	81.2%
Resolved (AAAA only, no A)	1,655	0.0%
Unresolved	956,210	18.8%

Classification of Resolved Domains

Classification	Domains	% of Reviewed
Vulnerable (on a vulnerable CDN/edge)	1,737,903	42.6%
Immune (on a CDN/edge, not vulnerable)	233,767	5.7%
Not on a CDN/shared edge (traditional hosting)	2,105,343	51.6%

Among the 1,971,670 domains that mapped to reviewed CDN/shared-edge providers, 88.1% are on providers or ASNs that produced a vulnerable SNI deception result.

research@adamnet.works

Vulnerable CDN Providers

Provider-level and ASN-level SNI deception testing produced a vulnerable result for 33 ASNs across the provider rows below. Counts show how many reviewed domains map to each provider row.

CDN / Provider	Vulnerable Domains	% of Vulnerable Domains
Cloudflare	1,281,217	73.7%
OVHcloud	91,093	5.2%
Google	90,485	5.2%
AWS CloudFront	79,377	4.6%
Hostinger	61,529	3.5%
Fastly	32,299	1.9%
Squarespace	21,341	1.2%
Wix	21,012	1.2%
Automattic/WordPress	11,871	0.7%
Akamai	10,911	0.6%
Incapsula/Imperva	10,349	0.6%
Sucuri	9,545	0.5%
Akamai/Linode	4,031	0.2%
Bigcommerce	3,395	0.2%
AbrArvan	3,128	0.2%
NAMESHIELD SAS	1,939	0.1%
Optimizely	1,556	0.1%
GMO GlobalSign Holdings K.K.	1,444	0.1%
Render	850	0.0%
Azion	175	0.0%
NuCDN	126	0.0%
BunnyCDN	124	0.0%
Alibaba Cloud	59	0.0%
Transparent Edge	21	0.0%
Medianova	12	0.0%
CacheFly	10	0.0%
Gcore	4	0.0%

Cloudflare accounts for 73.7% of the vulnerable-domain total. The top ten vulnerable provider rows account for 1,701,135 vulnerable domains, or 97.9% of the vulnerable-domain total.

research@adamnet.works

CDN Providers That Did Not Test Vulnerable

Provider-level and ASN-level SNI deception testing did not produce a vulnerable result for 40 ASNs across the provider rows below. Counts show how many reviewed domains map to each provider row.

CDN / Provider	Immune Domains
Akamai	51,466
Microsoft/Azure	46,836
IONOS	40,902
Alibaba Cloud	38,695
DDoS-Guard	29,272
Tencent Cloud	10,823
Cloudie Limited	2,958
Huawei Cloud	2,370
Tcloudnet	1,977
WIIT AG	1,519
NAVER BUSINESS PLATFORM ASIA PACIFIC PTE. LTD.	1,386
F5 Networks SARL	1,199
Baidu Cloud	960
Qrator	589
Fly.io	551
Link11 GmbH	507
Radware Ltd	371
RADWARE INC.	330
Yandex	310
StormWall	259
Gcore	234
AbrArvan	143
CDNetworks	49
CDNvideo	33
OVHcloud	15
BunnyCDN	8
Netlify	5

research@adamnet.works

Regional Heatmap

Regions are assigned from public suffix and TLD mapping. Vuln % is calculated as vulnerable domains divided by total classified domains in each row. Immune covers every classified domain in that row that is not counted as vulnerable.

Region	Total Domains	Vulnerable	Immune	Vuln %
Global / non-geo TLDs	2,656,407	1,257,841	1,398,566	47.4%
United States	26,366	13,556	12,810	51.4%
Canada	35,298	16,534	18,764	46.8%
Latin America & Caribbean	156,025	63,536	92,489	40.7%
Western & Northern Europe	465,199	126,066	339,133	27.1%
United Kingdom	88,485	47,374	41,111	53.5%
Eastern Europe	143,357	48,977	94,380	34.2%
Russia & CIS	233,613	53,033	180,580	22.7%
Middle East & North Africa	24,506	8,695	15,811	35.5%
Sub-Saharan Africa	24,108	9,396	14,712	39.0%
China	43,992	3,763	40,229	8.6%
Asia Pacific	241,855	89,132	152,723	36.9%

Global (gTLDs) covers generic suffixes such as .com, .net, and .org that cannot be assigned to one geography from the suffix alone. It covers 2,656,407 domains. The table uses tested domains as the denominator, which puts this bucket at 47.4%.

Mapping gTLDs to Region

Inference of gTLDs to region for additional regionalized vulnerability visualization can be done based on:
https://www.internetx.com/fileadmin/files/whitepaper_reports_pdfs/Global_Domain_Report_2023.pdf

https://www.sidn.nl/downloads/59TDj5jUtLH8FeC7XOptG3/1795894a2bb7ff5e19782d454de0900c/Global_Domain_Report_2020_Sedo.pdf

https://tranco-list.eu/assets/tranco-ndss19.pdf

research@adamnet.works

Estimation

Region	% / gTLD
USA	52%
Western Europe	11%
Canada	4%
UK	4%
Asia (ex-China)	9%
China	9%
Latin America	3%
Middle East	3%
Eastern Europe	2%
Russia & CIS	2%
Africa	1%

Notes: The breakdown of gTLD are informed estimates and not on raw counts. Actual figures could vary ±5-10% depending on exact ranking methodology (e.g., Tranco traffic-based vs. registration volume) and whether "origin" prioritizes registrant WHOIS (scarce), company HQ, or hosting IP geolocation. New gTLDs (smaller portion of top 5M) pull Asia/China higher, while legacy gTLDs/.com pull strongly toward USA/Western Europe. Data is current as of late 2022–2025 reports; trends show slow shifts toward greater Asia participation.

Contact

research@adamnet.works

https://adamnet.works
https://underminr.ai