



https://vio.com/

SUSPICIOUS

AI: 25/100 · MEDIUM RISK

Resolved IP: 34.250.237.250 · Server: CloudFront

MALWARE

Clean

SAFE BROWSING

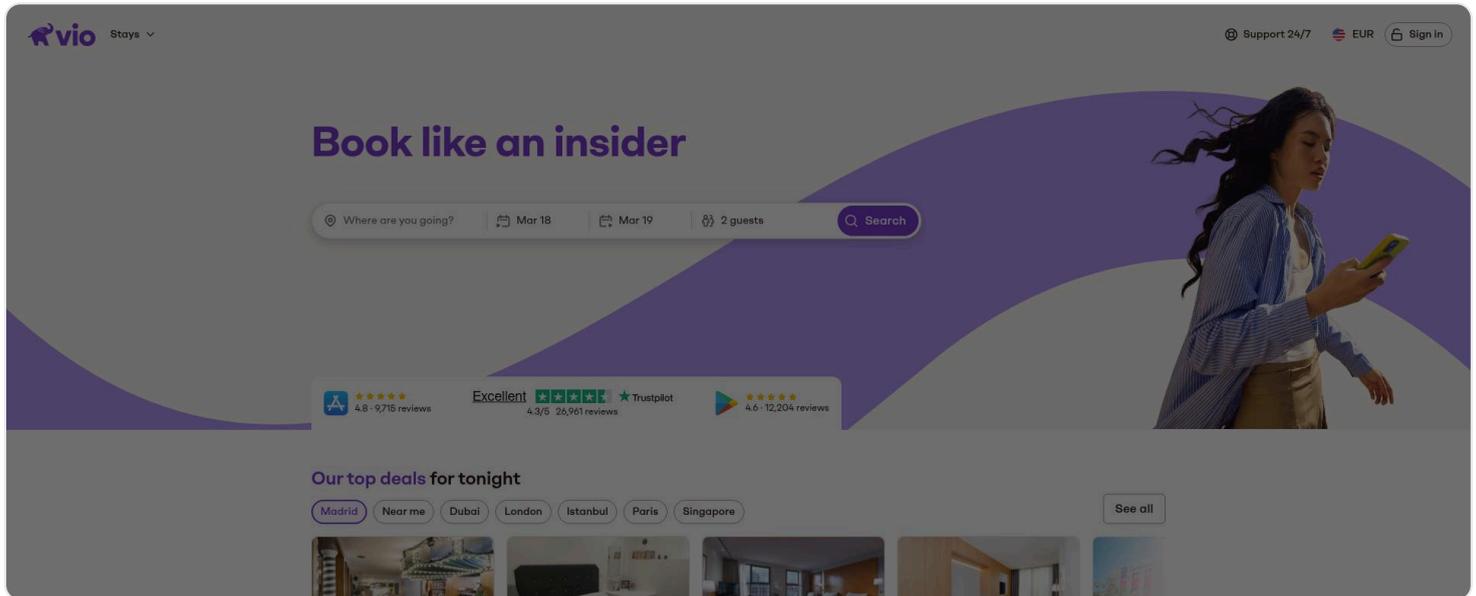
Clean

SSL

Valid

DOMAIN AGE

10227d



Desktop view — vio.com

THREAT DETECTION

URLhaus	CLEAN
Google Safe Browsing	CLEAN
Spamhaus	NOT LISTED
SURBL	NOT LISTED
Checked IP	52.211.86.198

SSL CERTIFICATE

Status	VALID
Protocol	TLSv1.3
Cipher Suite	TLS_AES_128_GCM_SHA256
Subject	vio.com
Issuer	Amazon RSA 2048 M04 (Amazon)
Valid From	Jun 26 00:00:00 2025 GMT
Expires	Jul 25 23:59:59 2026 GMT (129 days remaining)
HSTS	Enabled max-age=31536000; includeSubDomains
OCSP	unknown
Key	RSA 2048 bits
Serial Number	037D46892C14CE088A16FDB91B3B145B
SANs	vio.com, www.vio.com

HTTP SECURITY HEADERS

Status: **200 OK** · Final URL: <https://www.vio.com/>

HEADER	STATUS	VALUE
HSTS	present	max-age=31536000; includeSubDomains
X-Content-Type-Options	present	nosniff
X-Frame-Options	present	SAMEORIGIN
CSP	present	frame-ancestors 'self'; report-uri https://o28929.ingest.us.sentry.io/api/676675/security/?sentry_key=ece733f80e4d4958a8c9cfc1f5a6a5db
Referrer-Policy	present	strict-origin-when-cross-origin
Permissions-Policy	missing	-
COOP	missing	-
COEP	missing	-
CORP	missing	-
X-XSS-Protection	missing	-

Type	Name	Value	TTL
A	vio.com	34.250.237.250	59
A	vio.com	52.211.86.198	59
A	vio.com	63.32.187.27	59
MX	vio.com	alt1.aspmx.l.google.com	0
MX	vio.com	alt2.aspmx.l.google.com	0
MX	vio.com	aspmx.l.google.com	0
MX	vio.com	alt3.aspmx.l.google.com	0
MX	vio.com	alt4.aspmx.l.google.com	0
NS	vio.com	ns-1898.awsdns-45.co.uk	0
NS	vio.com	ns-220.awsdns-27.com	0
NS	vio.com	ns-842.awsdns-41.net	0
NS	vio.com	ns-1389.awsdns-45.org	0
TXT	vio.com	Probely=b22dfb8d-ef45-4355-8c49-4e43d83e03ff	0
TXT	vio.com	_68szk009bx3ew87o1cannixnc90rcdj	0
TXT	vio.com	amazonses:b0fQYbndONChUCDKBJXa4DwYmspMxjA40BnHEkfW6CQ=	0
TXT	vio.com	v=spf1 include:_spf.vio.com._d.easydmarc.pro ~all	0
TXT	vio.com	stripe- verification=2e8f86e7c60ffb6ef3ccc085ccabe788f6c7fdf909c1cc47872c14da58fc88ae	0
TXT	vio.com	google-site-verification=F6g1IXP0P_THSJkR6UYA654K7LuCLfqdkscVKNqwLTU	0
TXT	vio.com	openai-domain-verification=dv-QeiW5KudAjp9DSnVEJaeXyRr	0
TXT	vio.com	stripe- verification=8f237bc8d67b07b44e0f08770bf84701bc63f36620e3a04e78b43f98f6f7ec3c	0
TXT	vio.com	openai-domain-verification=dv-IdIgcT34HdDb1Z3GaM1Xc1SR	0
TXT	vio.com	google-site-verification=_lZ87y6-6wOZU7CkGwqIAC_JQFYebmMGEzV40jMxWfc	0
TXT	vio.com	openai-domain-verification=dv-CnSJqmg7hMkkqwPPxqNTSmo4	0
TXT	vio.com	e22cb9d6bbb4c290a94e4fff4d68a831	0
TXT	vio.com	riot-domain- verification=ab04408787e55584088f2deecf85c18c8aa5a58985e6c4d6ce3a92f2cbbd	0
SOA	vio.com	ns-1389.awsdns-45.org awsdns-hostmaster.amazon.com 1	86400
CAA	vio.com	0 digicert.com	0
CAA	vio.com	0 letsencrypt.org	0
CAA	vio.com	0 amazon.com	0

WHOIS REGISTRATION

Registrar	Amazon Registrar, Inc.
Registrant Org	Identity Protection Service
Registrant Country	GB
Domain Age	10227 days
Created	1998-03-18T05:00:00Z
Updated	2022-12-02T16:00:54Z
Expires	2031-03-17T04:00:00Z
Nameservers	ns-220.awsdns-27.com ns-842.awsdns-41.net ns-1898.awsdns-45.co.uk ns-1389.awsdns-45.org

TECHNOLOGY STACK

TECHNOLOGY	CATEGORY	CONFIDENCE	EVIDENCE
Next.js	Framework	high	Header: x-powered-by: Next.js
Google Analytics	Analytics	medium	HTML pattern: gtag\

AI SECURITY ANALYSIS

gpt-4.1-nano · two-pass analysis

INTELLIGENCE KNOWLEDGE CHECK

UNKNOWN

Unknown — suspicious pattern

Unknown domain

Vio.com is not recognized as a major brand, government, or reputable service based on training data. The domain's generic name and lack of prominent association suggest it is obscure or potentially used for less transparent purposes. No specific threat activity is publicly documented for this domain, but its obscurity warrants caution.

SCAN EVIDENCE VERDICT

25 /100 **MEDIUM RISK**

The domain vio.com is unfamiliar and lacks recognition as a reputable entity, aligning with prior intelligence indicating suspicion. The real-time scan shows a valid SSL certificate, a mature domain registration, and no known threat flags from blocklists, which suggests benign intent. However, the domain's obscurity, missing security headers, and hosting on a CDN with a relatively new SSL configuration raise caution. Overall, the evidence confirms some red flags consistent with an unknown, potentially less transparent site, but no active malicious indicators are present.

1. Monitor the domain for any emerging threat activity or user reports.
2. Avoid sharing sensitive information or integrating this domain into critical systems without further validation.
3. Conduct additional reconnaissance, such as content analysis or behavioral monitoring, if used in a security-sensitive context.
4. Keep security controls updated and consider implementing additional verification before engagement.

