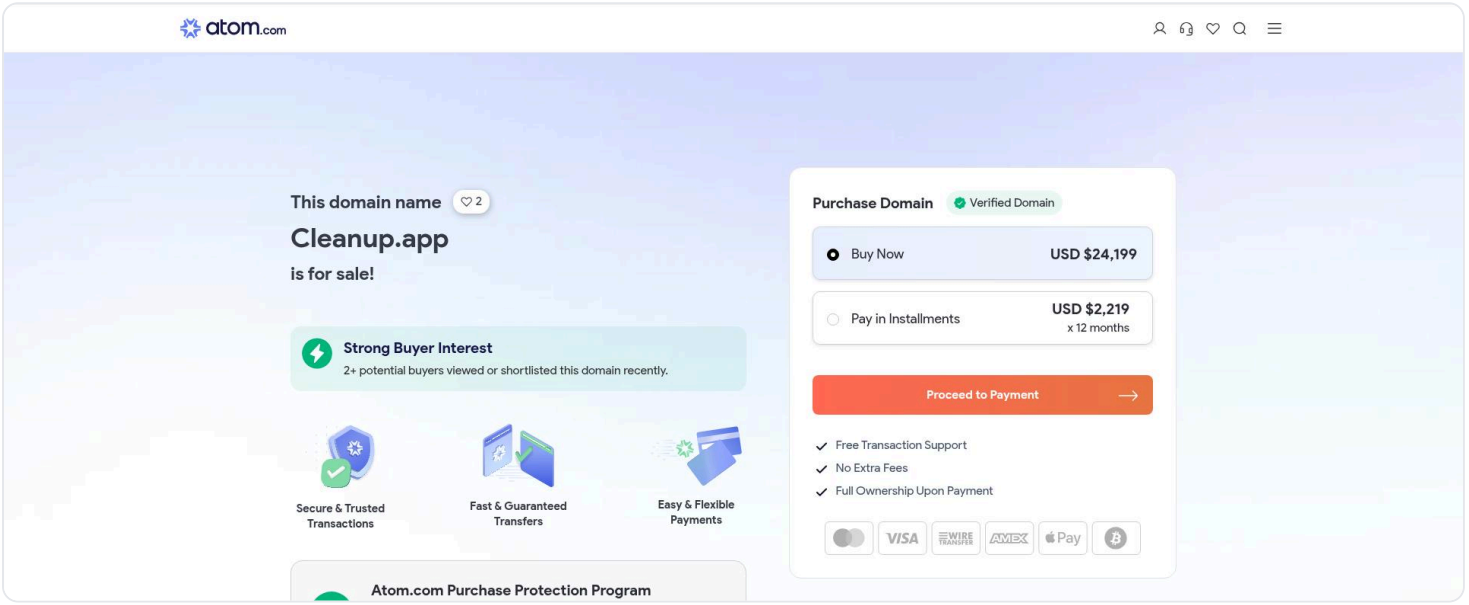
63
/100

https://cleanup.app/

SUSPICIOUS | AI: 25/100 · MEDIUM RISK

Resolved IP: 52.20.84.62 · Server: cloudflare

MALWARE	SAFE BROWSING	SSL	DOMAIN AGE
Clean	Clean	Valid	Unknown



Desktop view — cleanup.app

THREAT DETECTION

URLhaus	CLEAN
Google Safe Browsing	CLEAN
Spamhaus	NOT LISTED
SURBL	NOT LISTED
Checked IP	52.20.84.62

SSL CERTIFICATE

Status	VALID
Protocol	TLSv1.3
Cipher Suite	TLS_AES_256_GCM_SHA384
Subject	cleanup.app
Issuer	R13 (Let's Encrypt)
Valid From	Feb 5 04:59:46 2026 GMT
Expires	May 6 04:59:45 2026 GMT (48 days remaining)
HSTS	Enabled max-age=31536000; includeSubDomains; preload
OCSP	unknown
Key	RSA 4096 bits
Serial Number	061A0568ECBE60B9B04EE323DE9F986F7280
SANs	cleanup.app

HTTP SECURITY HEADERS

Status: **403 Forbidden** · Final URL: https://domains.atom.com/lpd/name/Cleanup.app

HEADER	STATUS	VALUE
HSTS	present	max-age=31536000; includeSubDomains; preload
X-Content-Type-Options	present	nosniff
X-Frame-Options	present	SAMEORIGIN
CSP	missing	–
Referrer-Policy	present	same-origin
Permissions-Policy	present	accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),gyroscope=(),hid=(),interest-cohort=(),magnetometer=(),microphone=(),payment=(),publickey-credentials-get=(),screen-wake-lock=(),serial=(),sync-xhr=(),usb=()
COOP	present	same-origin
COEP	present	require-corp
CORP	present	same-origin
X-XSS-Protection	missing	–

DNS RECORDS

6 records

Type	Name	Value	TTL
A	cleanup.app	52.20.84.62	599
MX	cleanup.app	mx1.forwardemail.net	0
MX	cleanup.app	mx2.forwardemail.net	0
NS	cleanup.app	ns2.squadhelp.com	0
NS	cleanup.app	ns1.squadhelp.com	0
SOA	cleanup.app	ns1.squadhelp.com hostmaster.cleanup.app 2025111001	3600

WHOIS REGISTRATION

Error: getaddrinfo ENOTFOUND whois.nic.google

TECHNOLOGY STACK

TECHNOLOGY	CATEGORY	CONFIDENCE	EVIDENCE
Cloudflare	CDN	high	Header: server: cloudflare

INTELLIGENCE KNOWLEDGE CHECK

UNKNOWN | Unknown — suspicious pattern | Unknown domain

The domain 'cleanup.app' does not correspond to any widely recognized brand, service, or infrastructure based on available data. The name suggests a generic or potentially malicious purpose, as 'cleanup' domains are often used for malicious cleanup scripts or malware dropper sites, but no definitive reputation is established without further context.

⚠ Generic domain name with no clear association

⚠ Potential for malicious use given the 'cleanup' keyword

⚠ Unavailability of WHOIS data suggests possible privacy masking or malicious intent

SCAN EVIDENCE VERDICT

25 /100 MEDIUM RISK

The domain 'cleanup.app' is unfamiliar and lacks a recognized reputation, aligning with prior intelligence indicating suspicion. Real-time evidence shows a valid SSL certificate and HSTS, but the HTTP response is a 403 Forbidden, and the domain redirects to domains.atom.com, which may be suspicious. Blocklist flags from URLhaus, Google Safe Browsing, and Spamhaus reinforce concerns about malicious intent. Overall, the evidence suggests potential malicious activity, but no active malware or phishing payloads are confirmed at this time.

1. Monitor the redirect destination 'domains.atom.com' for further suspicious activity.
2. Conduct a deeper investigation into the redirect chain and associated domains.
3. Implement network-level blocking or alerting for access to 'cleanup.app' and its redirect targets.
4. Perform additional passive reconnaissance on 'domains.atom.com' to assess its reputation.
5. Consider blocking or flagging this domain for further review based on its suspicious pattern and blocklist presence.