

DomainTools for Recorded Future

Enabling Rapid Alert Triage and Response

DomainTools Iris Investigate API in the Recorded Future Domain Intel Card

Domain names factor into almost every variant of cyberattacks, and yet analysts must frequently consult multiple disparate resources to build a complete risk assessment. The DomainTools Iris Investigate API delivers a comprehensive domain profile in the Recorded Future Domain Intel Card, enabling rapid alert triage and response. With immediate, in-context access to the unparalleled DomainTools Iris dataset, analysts will gain domain data in a carefully designed, expandable manner allowing information groups be easily navigated.

Domain Risk Assessment

Risk factors including domain age and registration status appear at the very top of Iris results to enable rapid threat assessments, including the Domain Risk Score. Domain Risk Score predicts how likely a domain is to be malicious, often before it is weaponized. This can close the window of vulnerability between the time a malicious domain is registered, and when it is observed and reported causing harm. The Domain Risk Score algorithms analyze a domain's association to known-bad infrastructure, as well as intrinsic properties of the domain that closely resemble those of known phishing, malware, and spam domains. Data shown on the intel card includes the classifiers and evidence behind the score to better inform analyst actions.

Additional sections appear on-demand below the risk factors, offering details including:

- Domain registration details
- IP location and ASN for web host, name server and mail server
- SSL certificate details, including common name and certificate hash
- Website tracking codes & response profile

DomainTools Iris

Analysts can also continue their domain name research directly in the DomainTools Iris platform with a link that preserves their context and starts an Iris Investigation with the domain they were researching in Recorded Future.



diwaliboom.tk - Domain

0 References to This Entity

Create an alert for diwaliboom.tk

Show recent cyber events involving diwaliboom.tk in Table

0 at risk

No Suspicious Content
Risk Score 0
No Risk Rules Triggered

Analytics

Website Response Code

IP Country Code

IP Address 166.62.28.79
Country Code us
Alexa Rank NO RANK
Overall Risk Score 98
Proximity Risk Score 56
Threat Profile Score 98
Threat profile category Malware because age, infrastructure, domain name, registration

Registration

Domain Status Active

Hosting

IP

IP Address 166.62.28.79
country_code us
ISP GoDaddy.com LLC
ASNNumber AS26496

Name Server

Domain freenom.com
Host ns01.freenom.com

Domain freenom.com
Host ns02.freenom.com

Domain freenom.com
Host ns03.freenom.com

Domain freenom.com
Host ns04.freenom.com

Mail Server

SSL Info

Identity

Registrant name Dot TK administrator
Additional Whois Email abuse@freenom.com
Email Domain freenom.com

Technical Contact

Billing Contact

Admin Contact

Registrant Contact

Country nl
Fax 31205315721
Organization BV Dot TK
Phone 31205315725
Postal Code P.O. Box 11774
Street 1001 GT Amsterdam
Email abuse@freenom.com,copyright@freenom.com

DomainTools Iris Open Iris Investigation Platform