Ministry of Electronics & Information Technology, Government of India

EN HI BN MR BH

Ministry of Electronics & Information Technology Government of India

Vasudev Kutumbukum

Nomoskar! Welcome to URL ANALYZER.

About

This tool performs quality multi-layer security analysis of domains/URLs. It features an advanced engine with 5+ layers of cyber intelligence checkers:

- WHOIS Record checks
- DNS lookup, mail & text record analysis
- VirusTotal reputation & threat verdict
- Phishing feeds: OpenPhish, URLhaus, PhishTank (real-time)
- Shodan: host vulnerabilities, open ports, geolocation & tags
- Certificate Transparency subdomain checks

Feature Highlights:

- Global, cross-intelligence verdicts ("Safe", "Malicious", etc)
- Downloadable, sharing-ready threat intelligence reports
- All results rendered in a clear, professional format

Analyze

Final Flag:

Safe

STIX 2.1 Key Patterns (Command Line Style):

```
==================================================
Key STIX Patterns:
```

```
  [domain-name:value = 'paytm.com']
  [ipv4-addr:value = '172.65.64.50']
  [ipv4-addr:value = '172.65.64.51']
=======================================================
```

STIX Bundle JSON


```
{
  "type": "bundle",
  "id": "bundle--1b738353-0bc4-47fd-abbd-9fb175f2c9ec",
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--b4eb014e-652f-487e-92f8-3e256543ad03",
      "created": "2025-07-31T22:19:54Z",
      "modified": "2025-07-31T22:19:54Z",
      "name": "Domain indicator: paytm.com",
      "pattern": "[domain-name:value = 'paytm.com']",
      "pattern_type": "stix",
      "valid_from": "2025-07-31T22:19:54Z",
      "labels": [
        "malicious-activity"
      ]
    },
    {
      "type": "indicator",
      "id": "indicator--4c648f52-a9ec-4e86-a0c9-d41d5655eeb6",
      "created": "2025-07-31T22:19:54Z",
      "modified": "2025-07-31T22:19:54Z",
      "name": "A address indicator: 172.65.64.50",
      "pattern": "[ipv4-addr:value = '172.65.64.50']",
      "pattern_type": "stix",
      "valid_from": "2025-07-31T22:19:54Z",
      "labels": [
        "malicious-activity"
      ]
    },
    {
      "type": "indicator",
      "id": "indicator--801782d0-50a7-441b-a76c-88f7196166ad",
      "created": "2025-07-31T22:19:54Z",
      "modified": "2025-07-31T22:19:54Z",
      "name": "A address indicator: 172.65.64.51",
      "pattern": "[ipv4-addr:value = '172.65.64.51']",
      "pattern_type": "stix",
      "valid_from": "2025-07-31T22:19:54Z",
      "labels": [
```

```
        "malicious-activity"
      ]
    }
  ]
}
```


WHOIS Information


```
{
  "Creation Date": "23 Jun 2003, 16:29:01, 23 Jun 2003, 11:29:01",
  "Domain Name": "PAYTM.COM",
  "Emails": "abuse@godaddy.com",
  "Expiration Date": "23 Jun 2034, 16:29:01, 23 Jun 2034, 11:29:01",
  "Name Servers": [
    "NS-1112.AWSDNS-11.ORG",
    "NS-1858.AWSDNS-40.CO.UK",
    "NS-249.AWSDNS-31.COM",
    "NS-998.AWSDNS-60.NET"
  ],
  "Registrar": "GoDaddy.com, LLC"
}
```


DNS Records


```
{
  "A": [
    "172.65.64.50",
    "172.65.64.51"
  ],
  "MX": [
    "10 aspmx.l.google.com.",
    "20 alt1.aspmx.l.google.com.",
    "20 alt2.aspmx.l.google.com.",
    "30 aspmx2.googlemail.com.",
    "30 aspmx3.googlemail.com.",
    "30 aspmx4.googlemail.com.",
    "30 aspmx5.googlemail.com."
  ],
  "TXT": [
    "\"14c34xr771wn93wtdyq9kx1t7j2y1ydb\"",
    "\"5ajcnlk.ng.impervadns.net\"",
    "\"MS=10282021\"",
    "\"MS=6341152B9423543860BFE82B9CBE44FB96BDFB19\"",
    "\"MS=ms10282021\"",
    "\"OSSRH-82568\"",
    "\"amazonses:7XabL68hzjmAMz9xh+xv5zq9p67Z/tGQQl8M4KYcHiM=\"",
    "\"amazonses:LWXYzNDz97HfT2/QevyERAj570gnCy9h5ba1SIdHdfA=\"",
```

```
    "\"amazonses:UBMnTGuTG1ddAGNSF+//kk0Ay+bG78S+2sVSolFSOlg=\"",
    "\"amazonses:f2cgo/64/ZR3Wc3M9u8yW+JqF/C6AamF3tP6gjqSzWw=\"",
    "\"amazonses:htyWxncjzmnINnrUYG1SIhJOjIDg3XQehwCvBqav3Uo=\"",
    "\"amazonses:nEOm4A5cBWbInNrqT7VT/JNqwdNxSGddWDrMrGh1lOw=\"",
    "\"apple-domain-verification=Lb2QXBpJpDMp72II\"",
    "\"asv=a6ff2b03eec006950453331350d45f6c\"",
    "\"cursor-domain-verification-7fs8ee=rEZ116QCrFd84UcWz19goUcf5\"",
    "\"d90rdsg118rspmlddjwmhq1xkh2jkw1f\"",
    "\"globalsign-domain-verification=7A10D5AFD979C51C98BCA00B251102F3\"",
    "\"google-site-verification=h8wm7P17qMYkSfARepjour4urvRE7ql07w2fHZgJIDg
    "\"google-site-verification=pPwlV980KnyiBTpL11QH-KNFR8NbPqfNsj404iEMMJg
    "\"google-site-verification=y_IZiW0IuexfXK1qw51Gfoqrn0cZOv9glKe8TGhoDqY
    "\"k8992rr9s318454k3kklt800h3jffckm\"",
    "\"m5gh704hlkqtdys2blf83twdl2r0pwcv\"",
    "\"nqh074ffxh6cg354v5qgtv438vbr1fmr\"",
    "\"tfxc9ygpq5k65807s5bj9lrm5zkjx99p\"",
    "\"v=spf1 ip4:13.127.134.11 ip4:54.240.85.29 ip4:54.240.85.30 include:ar
    "\"vAjntCVONTm6xd6/Zjdla9f2PZXIhdob1LuOKms4rbQ=\"",
    "\"wiz-domain-verification=f6d7b4796a53850158dcd7b59c561bba5e2feb91b0cb
    "\"xd5bmqslydc2qghxq87f5jkc4dvlqs74\"",
    "\"zncxhjkw1p4h6rmgbnl85p7678l1s0lb\""
  ]
}
```


Subdomains (Certificate Transparency Logs)

No subdomains found

Shodan (Host, Geolocation, Vulnerabilities)


```
{
  "Shodan Error": "Access denied (403 Forbidden)"
}
```


VirusTotal


```
{
  "IPs": [
    "172.65.64.50",
    "172.65.64.51"
  ],
  "Last_Check": 1753998330,
  "Reputation": 0,
  "Stats": {
    "harmless": 65,
    "malicious": 0,
    "suspicious": 0,
    "timeout": 0,
    "undetected": 29
```

```
  }
}
```


Phishing Feeds

- OpenPhish: No
- URLhaus: No
- PhishTank: No

Email Verification Records

- DMARC: None
- DKIM: None
- SPF: None

Download Result (JSON) Download as PDF