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 = 'microsoft.com']
  [ipv4-addr:value = '13.107.246.68']
  [ipv6-addr:value = '2603:1030:b:3::152']
  [ipv6-addr:value = '2603:1030:20e:3::23c']
  [ipv6-addr:value = '2603:1030:c02:8::14']
  [ipv6-addr:value = '2603:1020:201:10::10f']
  [ipv6-addr:value = '2603:1010:3:3::5b']
=====================================================
```

STIX Bundle JSON


```
{
  "type": "bundle",
  "id": "bundle--8e39dc2e-be03-4fbf-b6a4-fbbe79e31994",
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--ff650356-b24b-41a5-a3e1-7a10740e6e9a",
      "created": "2025-07-31T23:03:45Z",
      "modified": "2025-07-31T23:03:45Z",
      "name": "Domain indicator: microsoft.com",
      "pattern": "[domain-name:value = 'microsoft.com']",
      "pattern_type": "stix",
      "valid_from": "2025-07-31T23:03:45Z",
      "labels": [
        "malicious-activity"
      ]
    },
    {
      "type": "indicator",
      "id": "indicator--028c2cfd-8506-4d8b-9d0c-fa981b58cd53",
      "created": "2025-07-31T23:03:45Z",
      "modified": "2025-07-31T23:03:45Z",
      "name": "A address indicator: 13.107.246.68",
      "pattern": "[ipv4-addr:value = '13.107.246.68']",
      "pattern_type": "stix",
      "valid_from": "2025-07-31T23:03:45Z",
      "labels": [
        "malicious-activity"
      ]
    },
    {
      "type": "indicator",
      "id": "indicator--7a3ad97c-8b6a-44b1-b7ce-f9697c8ac0a3",
      "created": "2025-07-31T23:03:45Z",
      "modified": "2025-07-31T23:03:45Z",
      "name": "AAAA address indicator: 2603:1030:b:3::152",
```

```
    "pattern": "[ipv6-addr:value = '2603:1030:b:3::152']",
    "pattern_type": "stix",
    "valid_from": "2025-07-31T23:03:45Z",
    "labels": [
      "malicious-activity"
    ]
  },
  {
    "type": "indicator",
    "id": "indicator--aa2f30c4-b44a-4b28-b1b1-073facf64dbd",
    "created": "2025-07-31T23:03:45Z",
    "modified": "2025-07-31T23:03:45Z",
    "name": "AAAA address indicator: 2603:1030:20e:3::23c",
    "pattern": "[ipv6-addr:value = '2603:1030:20e:3::23c']",
    "pattern_type": "stix",
    "valid_from": "2025-07-31T23:03:45Z",
    "labels": [
      "malicious-activity"
    ]
  },
  {
    "type": "indicator",
    "id": "indicator--eff24e0b-3541-4141-931a-cae7c09c3d9d",
    "created": "2025-07-31T23:03:45Z",
    "modified": "2025-07-31T23:03:45Z",
    "name": "AAAA address indicator: 2603:1030:c02:8::14",
    "pattern": "[ipv6-addr:value = '2603:1030:c02:8::14']",
    "pattern_type": "stix",
    "valid_from": "2025-07-31T23:03:45Z",
    "labels": [
      "malicious-activity"
    ]
  },
  {
    "type": "indicator",
    "id": "indicator--caa3c515-313a-4200-b120-116a0ba40705",
    "created": "2025-07-31T23:03:45Z",
    "modified": "2025-07-31T23:03:45Z",
    "name": "AAAA address indicator: 2603:1020:201:10::10f",
    "pattern": "[ipv6-addr:value = '2603:1020:201:10::10f']",
    "pattern_type": "stix",
    "valid_from": "2025-07-31T23:03:45Z",
    "labels": [
      "malicious-activity"
    ]
  },
```

```
    {
      "type": "indicator",
      "id": "indicator--347b50ad-00a2-401e-9a7f-6a3546a2b718",
      "created": "2025-07-31T23:03:45Z",
      "modified": "2025-07-31T23:03:45Z",
      "name": "AAAA address indicator: 2603:1010:3:3::5b",
      "pattern": "[ipv6-addr:value = '2603:1010:3:3::5b']",
      "pattern_type": "stix",
      "valid_from": "2025-07-31T23:03:45Z",
      "labels": [
        "malicious-activity"
      ]
```


WHOIS Information


```
{
  "Creation Date": "02 May 1991, 04:00:00, 02 May 1991, 04:00:00",
  "Domain Name": "MICROSOFT.COM",
  "Emails": [
    "abusecomplaints@markmonitor.com",
    "admin@domains.microsoft",
    "msnhst@microsoft.com",
    "whoisrequest@markmonitor.com"
  ],
  "Expiration Date": "03 May 2026, 04:00:00, 03 May 2026, 00:00:00",
  "Name Servers": [
    "NS1-39.AZURE-DNS.COM",
    "NS2-39.AZURE-DNS.NET",
    "NS3-39.AZURE-DNS.ORG",
    "NS4-39.AZURE-DNS.INFO"
  ],
  "Registrar": "MarkMonitor, Inc."
}
```


DNS Records


```
{
  "A": [
    "13.107.246.68"
  ],
  "AAAA": [
    "2603:1030:b:3::152",
    "2603:1030:20e:3::23c",
    "2603:1030:c02:8::14",
    "2603:1020:201:10::10f",
    "2603:1010:3:3::5b"
  ],
  "MX": [
```

```
    "10 microsoft-com.mail.protection.outlook.com."
  ],
  "TXT": [
    "\"d365mktkey=3uc1cf82cpv750lzk70v9bvf2\"",
    "\"facebook-domain-verification=fwzwhbbzwmg5fzgotc2go51olc3566\"",
    "\"google-site-verification=pjPOauSPcrfXOZS9jnPPa5axowcHGCDAl1_86dCqFpk
    "\"fg2t0gov9424p2tdcuo94goe9j\"",
    "\"t7sebee51jrj7vm932k531hipa\"",
    "\"google-site-verification=M--CVfn_YwsV-2FGbCp_HFaEj23BmT0cTF4l8hXgpvM
    "\"google-site-verification=GfDnTUdATPsK1230J0mXbfsYw-3A9BVMVaKSd4DcKgI
    "\"d365mktkey=SxDf1EZxLvMwx6eEZUxzjFFgHoapF8DvtWEUjwq7ZTwx\"",
    "\"hubspot-developer-verification=OTQ5NGIwYWEtODNmZi00YWE1LTkyNmQtNDhjMD
    "\"d365mktkey=QDa792dLCZhvaAOOCe2Hz6WTzmTssOp1snABhxWibhMx\"",
    "\"d365mktkey=6358r1b7e13hox60tl1uagv14\"",
    "\"google-site-verification=uFg3wr5PWsK8lV029RoXXBBUW0_E6qf1WEWVHhetkOY
    "\"docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840\"",
    "\"d365mktkey=j2qHWq9BHdaa3ZXZH8x64daJZxEWsFa0dxDeilxDoYYx\"",
    "\"v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com incl
    "\"atlassian-domain-verification=xvoaqRfxSg3PnlVnR4xCSOlKyw1Aln0MMxRiKXr
    "\"workplace-domain-verification=lK0QDLk73xymCYMKUXNpfKAT8TY5Mx\"",
    "\"google-site-verification=uhh5_jbxpcQgnb-A7gDIjlrr5Ef34lA2t2_BAveYpnk
    "\"MS=ms79629062\"",
    "\"d365mktkey=3l6dste9txazu0Qd2zu4135PUB4E35txLxyzJxjkPbsx\"",
    "\"d365mktkey=wbU64GRacxVEQxwcLSQnx0zisXLYzgUbfvsufIqO9ZUx\"",
    "\"linear-domain-verification=iuq6saifcnbe\"",
    "\"d365mktkey=ZGFU0tlXPekPusNHPo5QQQWpVf0gic0xpuKroNy3NQEx\"",
    "\"d365mktkey=JlXV17lfZjyvWxNje1qiP390ACSKzTxo5mGqZ3V2BmYx\"",
    "\"google-site-verification=mEAmcTy1e8jIB9W6ENPk2GDg9hjuNytQQRGlK0hPm0c
    "\"d365mktkey=PNcDqkW71x8VOUhcE96aGM4l5PYX1gnlRl6ieXUl5eMx\"",
    "\"d365mktkey=Fu49WtSTeClkHtK7S14227RIVpGwwGrzEsO6RVs1I2Ax\"",
    "\"ms-domain-verification=25524f4b-1476-489c-a086-30f4c5016ecc\"",
    "\"ms-domain-verification=1c4e4677-e58f-4117-8d61-e5b2810388c2\"",
    "\"mixpanel-domain-verify=5803bc4c-5bb6-4ce1-8076-753800097373\"",
    "\"sitecore-domain-verification=1d46cb5467624e33a408d14324874088\"",
    "\"ms-domain-verification=478640ad-6524-43d5-86c4-a914804b9e93\"",
    "\"ms-domain-verification=561512fc-b4ba-4ac7-a946-e464c8f49f1b\"",
    "\"_zx2p8gpzv720db2aqmozy4jhwk2nl43\"",
    "\"airtable-verification=79a09e4a8013ff5737798ffb4ea88eee\"",
    "\"1password-site-verification=35ZTURTFFFDC5BW7GFQKRJ77QM\""
  ]
}
```


Subdomains (Certificate Transparency Logs)

No subdomains found

Shodan (Host, Geolocation, Vulnerabilities)


```
{
  "City": "N/A",
  "Country": "United States",
  "IP": "13.107.246.68",
  "Latitude": "N/A",
  "Longitude": "N/A",
  "Open Ports": "80, 443",
  "Organization": "Microsoft Corporation",
  "Region": "N/A",
  "Shodan Tags": "cloud",
  "Vulns": "None"
}
```


VirusTotal


```
{
  "IPs": [
    "2603:1030:20e:3::23c",
    "2603:1030:b:3::152",
    "2603:1030:c02:8::14",
    "2603:1010:3:3::5b",
    "2603:1020:201:10::10f",
    "13.107.253.38"
  ],
  "Last_Check": 1753971833,
  "Reputation": 38,
  "Stats": {
    "harmless": 66,
    "malicious": 0,
    "suspicious": 0,
    "timeout": 0,
    "undetected": 28
  }
}
```


Phishing Feeds

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

Email Verification Records

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

Download Result (JSON) Download as PDF