

The Best SOC Analyst Tools

A Curated Collection for Cybersecurity Investigations & Malware Analysis

This document outlines essential tools every SOC (Security Operations Center) analyst should be familiar with. Categorized by functionality, it includes free and widely-used tools for investigation, reputation checking, online sandboxing, and more.

Table of Contents

1. Investigation Tools

- Process Hacker
- BrowsingHistoryView
- FullEventLogView

2. Reputation Checking

- VirusTotal
- AbuseIPDB
- Cisco Talos

3. Online Sandbox Analysis

- AnyRun
- Hybrid-Analysis
- urlscan.io

4. Other Utilities

- MXToolBox
- Koodous
- python-oletools

Investigation Tools

◆ Process Hacker

Category: Investigation

A powerful system monitoring tool. Helps detect suspicious processes and behaviors in real time.

 <https://processhacker.sourceforge.io/>

◆ BrowsingHistoryView

Category: Investigation

Aggregates browser history data from multiple browsers into a unified table for quick forensic analysis.

 https://www.nirsoft.net/utils/browsing_history_view.html

◆ FullEventLogView

Category: Investigation

Displays all system event logs in a simplified tabular format, reducing time spent during incident response.

 https://www.nirsoft.net/utils/full_event_log_view.html

By : <https://blog.lalatendu.info/>

Checking Reputation

♦ VirusTotal

Category: Checking Reputation

Search IPs, hashes, domains, and get relationship graphs. Excellent for file/IP threat validation.

 <https://www.virustotal.com/>

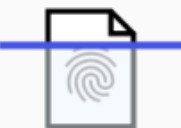


Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

FILE

URL

SEARCH



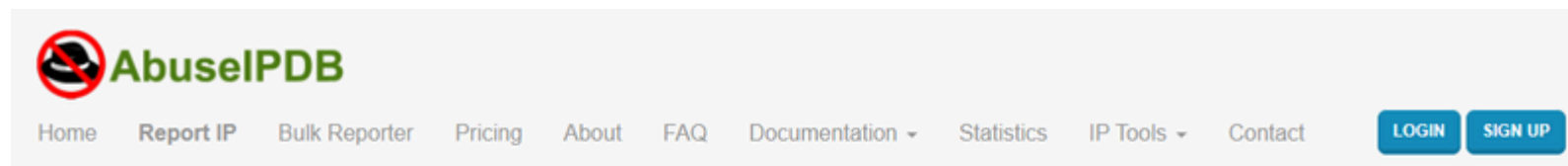
Choose file

♦ AbuseIPDB

Category: Checking Reputation

Check whether an IP has been reported for malicious activity. Ideal for investigating firewall logs.

 <https://www.abuseipdb.com/>



AbuseIPDB » 218.204.70.179

Check an IP Address, Domain Name, or Subnet
e.g. 91.93.224.197, microsoft.com, or 5.188.10.0/24


91.93.224.197

CHECK

218.204.70.179 was found in our database!

This IP was reported **2,734** times. Confidence of Abuse is **100%**: ?

100%

ISP	China Mobile Communications Corporation
Usage Type	Unknown
Domain Name	chinamobileltd.com
Country	 China
City	Jiujiang, Jiangxi

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

REPORT 218.204.70.179

WHOIS 218.204.70.179

AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the [statistics](#). We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider [chipping in!](#)

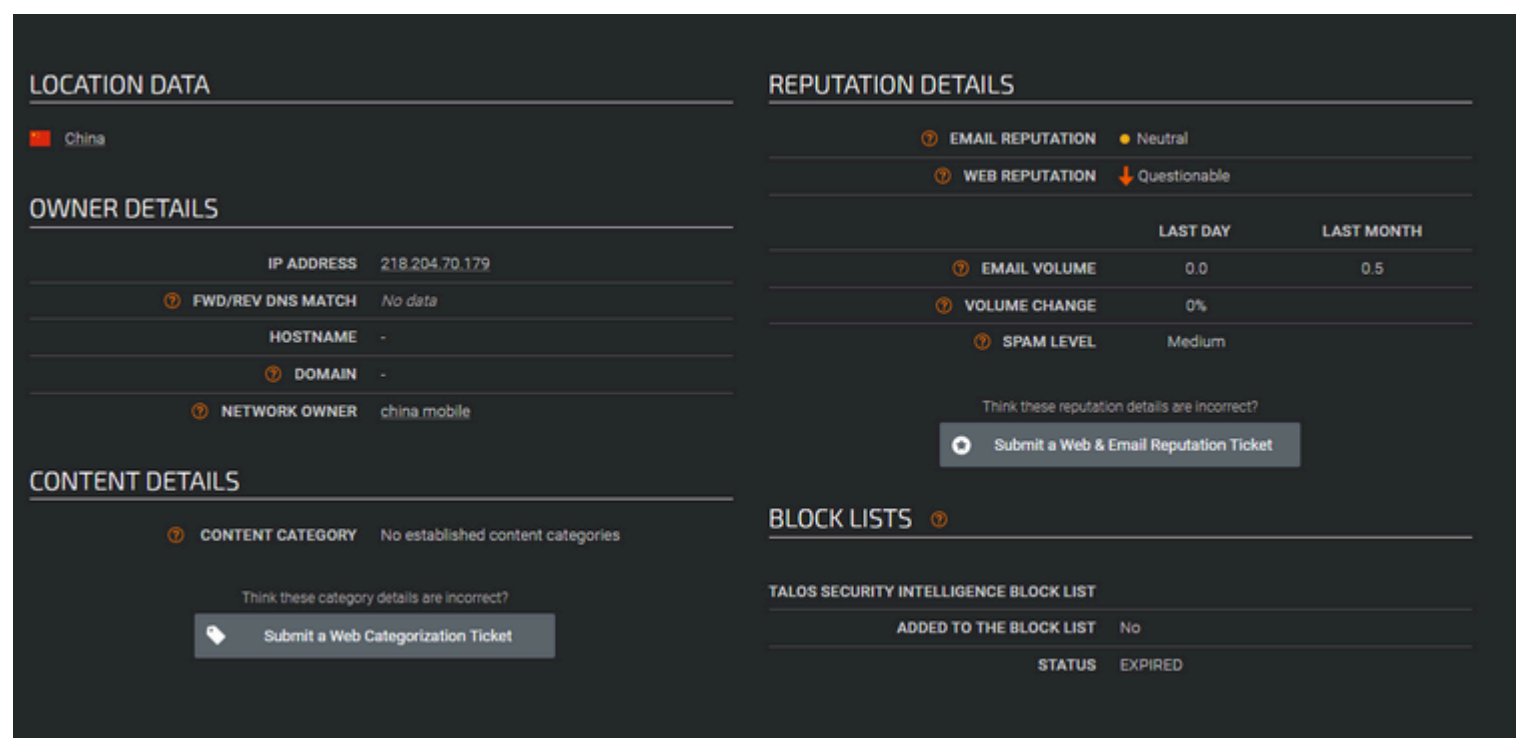
AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the [statistics](#). We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider [chipping in!](#)

◆ Cisco Talos

Category: Checking Reputation

Perform lookups for IPs, domains, and network owners with up-to-date threat intelligence.

 <https://talosintelligence.com/>



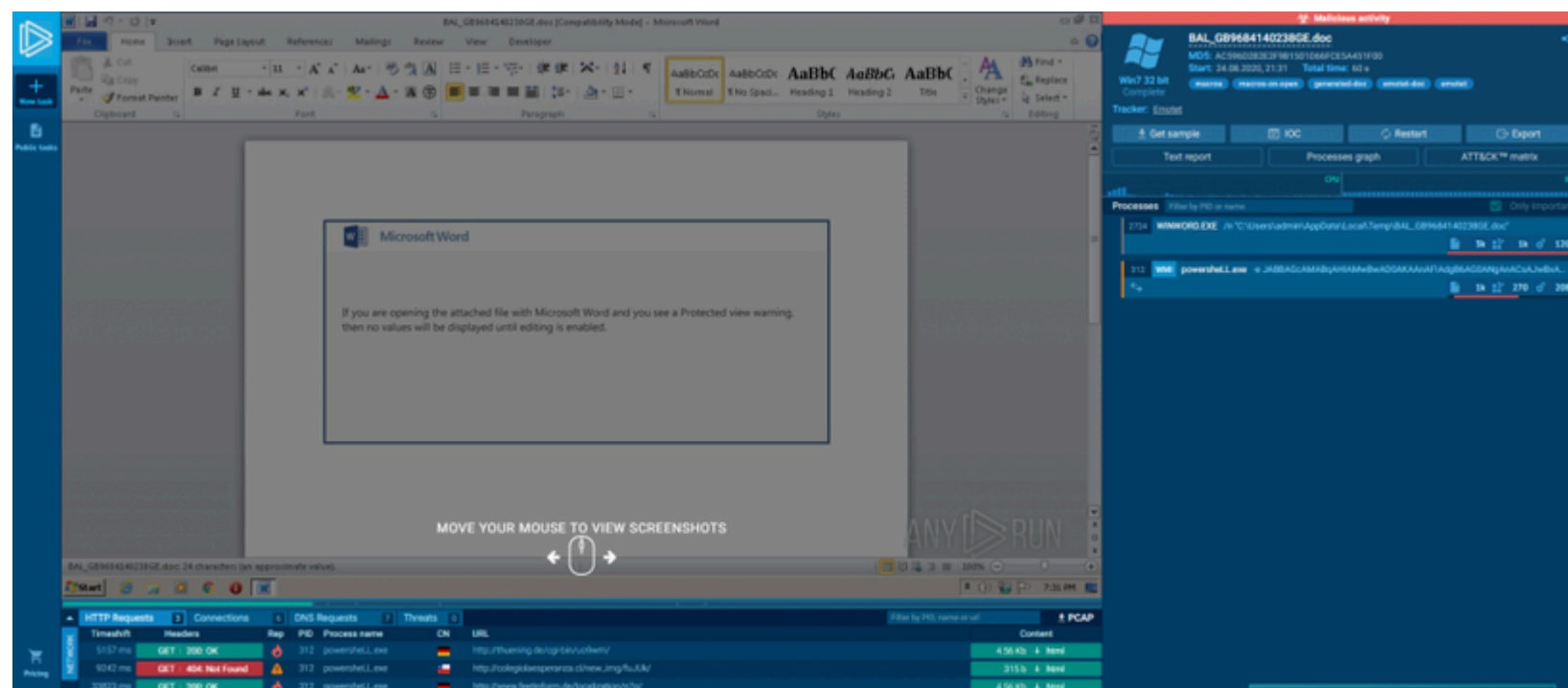
Online Sandbox Analysis

◆ **AnyRun**

Category: Online Sandbox

An interactive malware sandbox that reveals C2 (Command and Control) infrastructure and malware intent. Free tier available.

<https://any.run/>




◆ Hybrid-Analysis

Category: Online Sandbox

Generates detailed malware reports using Falcon Sandbox technology. Great for dynamic malware assessment.


<https://www.hybrid-analysis.com/>

SandboxQuick ScansFile CollectionsResourcesRequest InfoMore



File/URLFile CollectionReport SearchYARA SearchString Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.



or

Analyze

Maximum upload size is 100 MB.
Powered by CrowdStrike Falcon® Sandbox.
Interested in a free trial?

Releases & Updates

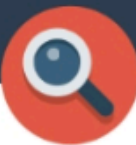
Introducing Community Score on Hybrid Analysis
October 24, 2024

Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis
October 24, 2024

See More!

© 2025 Hybrid Analysis — Hybrid Analysis Terms and Conditions of Use — Hybrid Analysis Privacy Notice — Site Notice — Your Privacy Choices — Contact Us

Category: Online Sandbox
Specialized in scanning and analyzing URLs. Excellent for phishing and redirection investigations.
<https://urlscan.io/>



urlscan.io

[Home](#)[Search](#)[Live](#)[API](#)[Blog](#)[Docs](#)[Pricing](#)[Login](#)

Sponsored by
SecurityTrails
A Recorded Future Company

urlscan.io

A sandbox for the web



[Public Scan](#)[Options](#)




Recent scans



🔄 Updates every 10s - Last update: 21:42:55

URL	Age		Size		IPs		
domains.atom.com/lpd/name/www.essence.fun	11 seconds		539 KB	47	8	3	
www.unlimitedfileservice.com/	12 seconds		1 MB	77	12	2	
www.oversluiten.nl/overwaarde-actie-1?site=1428	13 seconds		3 MB	148	19	4	
preferences.atlassian.com/main/?hid=b73fa3d58d0815000baf921e6e4e195b	14 seconds		886 KB	42	10	2	
www.digitalintro.in/	15 seconds		20 MB	58	4	4	
seguro.capo-darte.site/aceso/entrar	15 seconds		2 MB	17	5	2	
bet365.unikuemoney.com/	17 seconds		501 KB	87	2	2	
www.ap.show/	18 seconds		86 KB	20	8	6	
app.nabla.com/	18 seconds		3 MB	20	7	2	
ipasokangpanalo100.finance.blog/	19 seconds		296 KB	36	7	2	

Thanks to our corporate sponsors







Copyright © 2025, urlscan GmbH
Version: 2025-05-13T11:10

Follow @urlscanio

741 Scans Running51 Scans Queued

683928 Public (24h)370120 Unlisted (24h)1364010 Private (24h)

Page generated on 2025-05-14 16:12:10

[Status Page](#)[Terms of Service](#)[Privacy Policy](#)[Impressum / Legal](#)

[About Us](#)[Security](#)[Sitemap](#)


Other Tools

♦ MXToolBox

Category: Other


Useful in phishing investigations. Helps compare and validate SMTP headers and sender information.

 <https://mxtoolbox.com/>



PricingToolsDelivery CenterMonitoringProductsBlogSupportLogin

SuperToolMX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS LookupAnalyze HeadersAll Tools

 MX Lookup

Domain Name

MX LookupSolve Email Delivery Problems

ABOUT MX LOOKUP

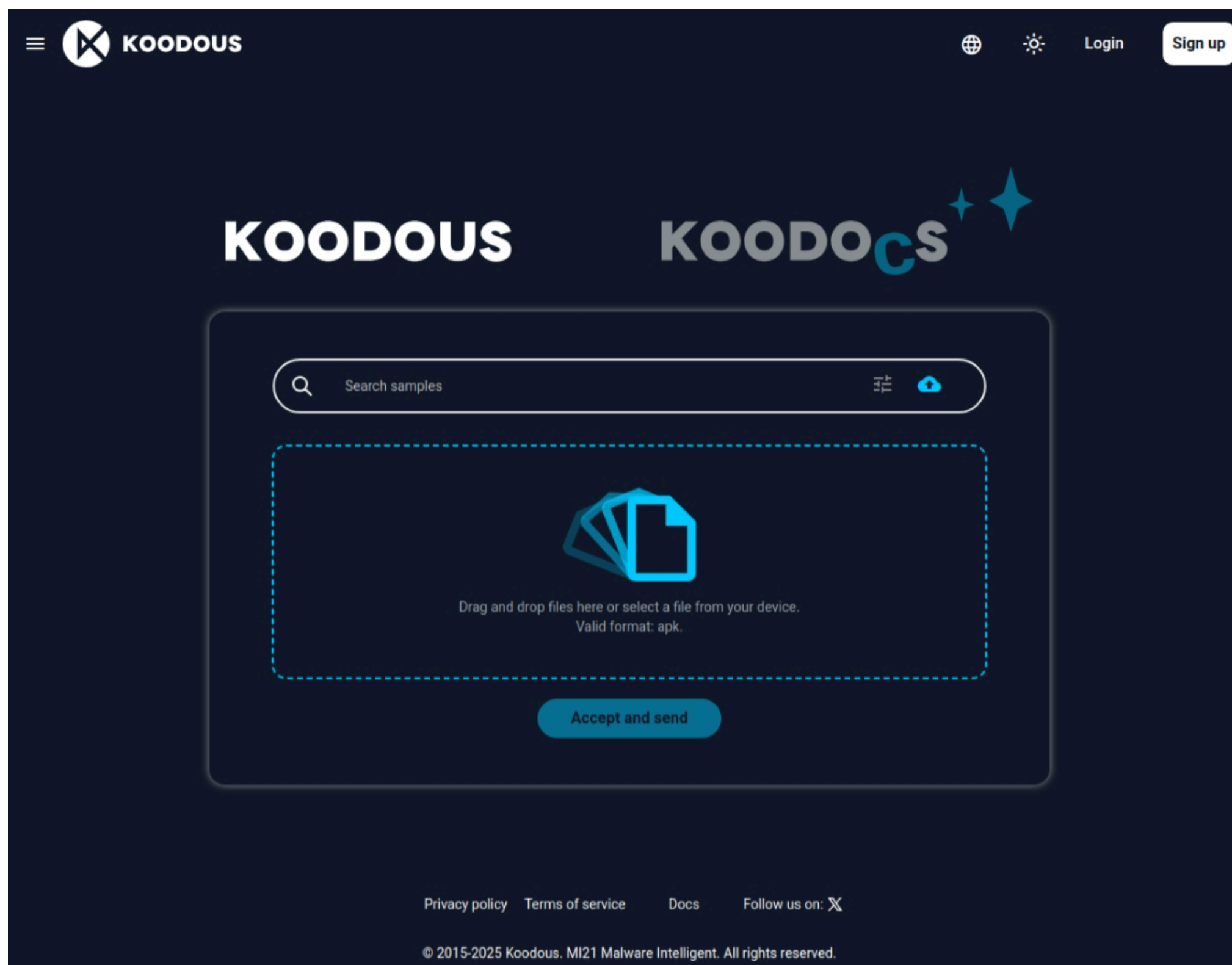
This test will list MX records for a domain in priority order. The MX lookup is done directly against the domain's authoritative name server, so changes to MX Records should show up instantly. You can click [Diagnostics](#) , which will connect to the mail server, verify reverse DNS records, perform a simple Open Relay check and measure response time performance. You may also check each MX record (IP Address) against 105 DNS based [blacklists](#) . (Commonly called RBLs, DNSBLs)

♦ **Koodous**

Category: Other

Provides malware intelligence focused on APK files. Good for analyzing Android threats.

<https://koodous.com/>



♦ python-oletools

Category: Other

A Python framework for analyzing OLE2-based Microsoft files (e.g., Word, Excel, Outlook). Useful for macro and document malware.

<https://github.com/decalage2/oletools>

```
$ oledir 41a84ee951ec7efa36dc16c70aaaf6b8e6d1bce8bd9002d0ab5236197eb3b32a.bin
oledir 0.02 - http://decalage.info/python/oletools
OLE directory entries in file 41a84ee951ec7efa36dc16c70aaaf6b8e6d1bce8bd9002d0ab5236197eb3b32a.bin:
-----+-----+-----+-----+-----+-----+-----+-----+-----+
id |Status|Type  |Name                |Left |Right|Child|1st Sect|Size
-----+-----+-----+-----+-----+-----+-----+-----+-----+
0  |<Used>|Root  |Root Entry         |-    |-    |3     |2A      |2496
1  |unused|Empty |                   |-    |-    |-     |0       |0
2  |<Used>|Stream|WordDocument       |5    |-    |-     |0       |4096
3  |<Used>|Stream|\x05SummaryInformation|2    |4    |-     |16      |4096
4  |<Used>|Stream|\x05DocumentSummaryInf|-    |-    |-     |1E      |4096
   |      |      |ormation           |
5  |<Used>|Stream|1Table             |-    |13   |-     |8       |7094
6  |unused|Empty |                   |-    |-    |-     |0       |0
7  |unused|Empty |                   |-    |-    |-     |0       |0
8  |unused|Empty |                   |-    |-    |-     |0       |0
9  |unused|Empty |                   |-    |-    |-     |0       |0
10 |unused|Empty |                   |-    |-    |-     |0       |0
11 |unused|Empty |                   |-    |-    |-     |0       |0
12 |unused|Empty |                   |-    |-    |-     |0       |0
13 |<Used>|Stream|\x01CompObj      |-    |-    |-     |25      |114
14 |unused|Empty |                   |-    |-    |-     |0       |0
15 |unused|Empty |                   |-    |-    |-     |0       |0
$
$ oledir 6780af202bf7534fd7fcfc37aa57e5a998e188ca7d65e22c0ea658c73fad36a2.bin
oledir 0.02 - http://decalage.info/python/oletools
OLE directory entries in file 6780af202bf7534fd7fcfc37aa57e5a998e188ca7d65e22c0ea658c73fad36a2.bin:
-----+-----+-----+-----+-----+-----+-----+-----+-----+
id |Status|Type  |Name                |Left |Right|Child|1st Sect|Size
-----+-----+-----+-----+-----+-----+-----+-----+-----+
0  |<Used>|Root  |Root Entry         |-    |-    |3     |2A      |2496
1  |<Used>|Stream|1Table             |-    |-    |-     |8       |7094
2  |<Used>|Stream|WordDocument       |5    |-    |-     |0       |4096
3  |<Used>|Stream|\x05SummaryInformation|2    |4    |-     |16      |4096
4  |<Used>|Stream|\x05DocumentSummaryInf|-    |-    |-     |1E      |4096
   |      |      |ormation           |
5  |<Used>|Storage|Macros             |1    |13   |12    |0       |0
6  |<Used>|Storage|VBA                |-    |-    |7     |0       |0
7  |<Used>|Stream|ThisDocument       |8    |9    |-     |0       |1214
8  |<Used>|Stream|Module1            |10   |-    |-     |32      |42488
9  |<Used>|Stream|_VBA_PROJECT       |-    |-    |-     |88      |10014
10 |<Used>|Stream|dir                |-    |-    |-     |13      |571
11 |<Used>|Stream|PROJECTwm         |-    |-    |-     |1C      |65
12 |<Used>|Stream|PROJECT          |6    |11   |-     |1E      |419
13 |<Used>|Stream|\x01CompObj|-    |-    |-     |25      |114
14 |unused|Empty |                   |-    |-    |-     |0       |0
15 |unused|Empty |                   |-    |-    |-     |0       |0
```

- All tools listed are **free** or offer **freemium tiers**.
- URLs are included for direct access.
- Categorization has been verified five times against the original content to ensure completeness and accuracy.