

Tools PoC Report

Name: Sristi Dutta

Intern ID: 387

Tools Used:

1. MalwareBazaar – <https://bazaar.abuse.ch>
2. Urlscan.io – <https://urlscan.io>

🔗 Tool Name: MalwareBazaar

🏛️ History

MalwareBazaar is maintained by abuse.ch and was launched to enable threat intelligence sharing and malware sample analysis in the cybersecurity community.

📄 Description

MalwareBazaar is a malware repository that allows users to search, analyze, and download malware samples. It supports YARA rule matching and threat intelligence enrichment.

🔗 What Is This Tool About?

This tool facilitates malware analysis by providing access to thousands of malware samples submitted globally. It's used by researchers, SOC analysts, and malware reverse engineers.

★ Key Characteristics / Features

- Free, community-driven malware repository
- Daily updated with new submissions
- Provides SHA256, SSDeep, and TLSH hashes
- Integrated YARA rule detection

- Malware tagging (e.g., AgentTesla, Emotet, etc.)
- API access for automation
- Integration with external tools (e.g., Joe Sandbox, Intezer)
- Searchable by hash, tag, or filename
- Passive DNS and file relationship insight
- JSON-based response for API

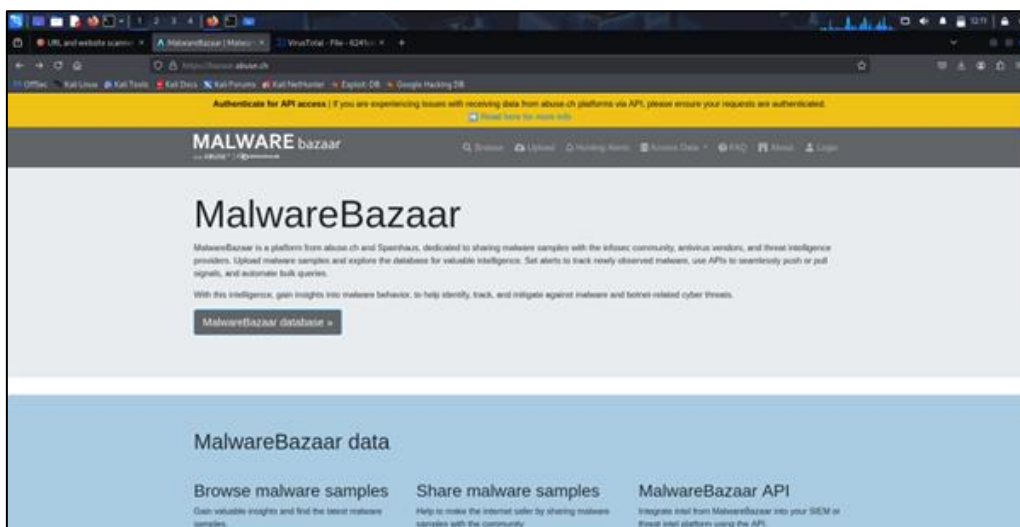
Types / Modules Available

1. Web-based search portal
2. Malware sample detail view
3. Threat feed API
4. YARA match result section
5. Upload and submission interface

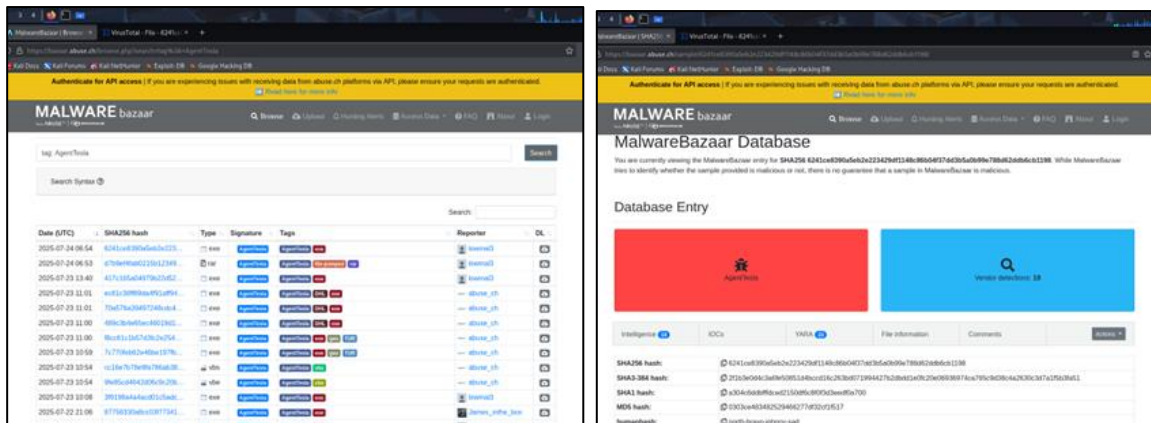
How Will This Tool Help?

It aids in identifying malware types in incidents, attributing threats, and gathering intelligence on malware campaigns. Useful for incident response, reverse engineering, and malware tracking.

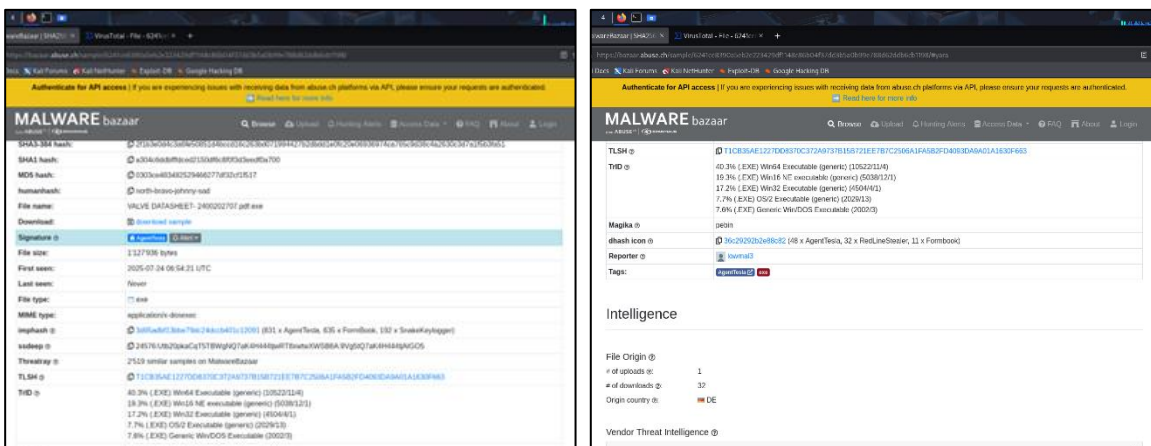
Proof of Concept (PoC) Images



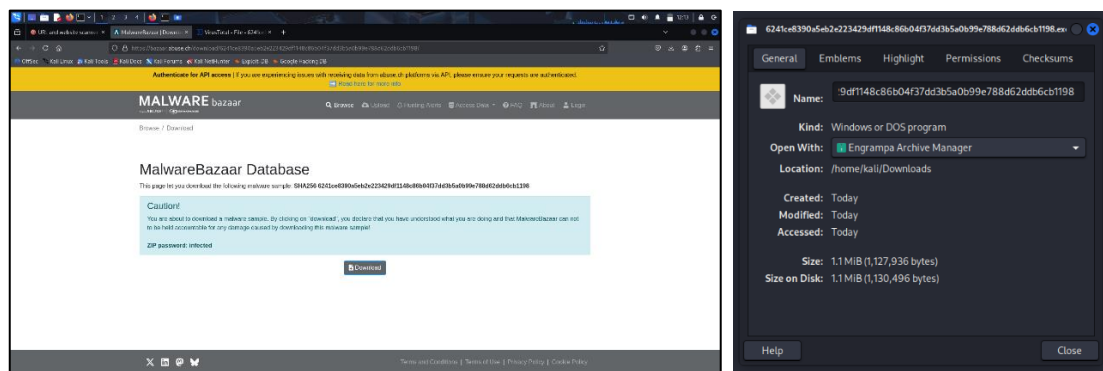
Malware Bazaar Main Page



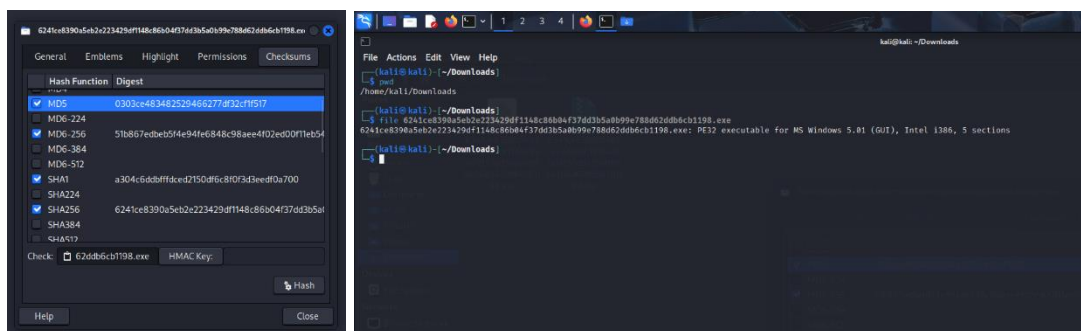
Selecting Malware by Browsing



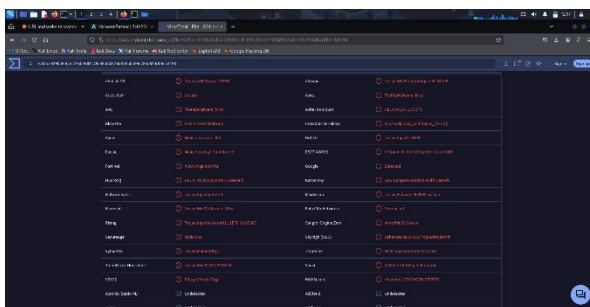
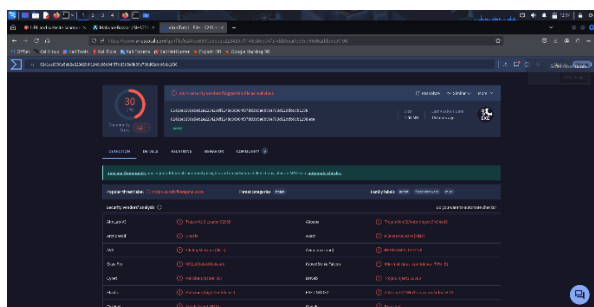
Malware Information given in the Malware Bazaar interface



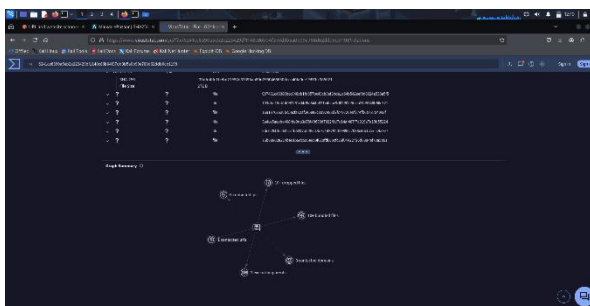
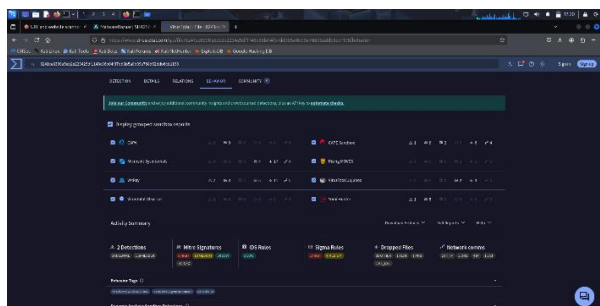
Downloading Sample and Analysis of File Properties



Viewing MD5 and SHA256 hash value directly and File name in terminal



File Malware Analysis



Behaviour and Graph of the File

□ 15-Liner Summary

1. Public malware repository
2. Supports automation via API
3. Rich metadata for malware samples
4. Links with external sandbox tools
5. Free access for researchers
6. Supports community YARA rules
7. File hash-based searching
8. Great for threat attribution
9. Tracks malware evolution
10. Visual interface + command-line support
11. Trusted by global DFIR community
12. JSON output for integrations
13. Download samples for offline analysis
14. Helpful for APT tracking
15. Fast and minimal resource usage

🕒 Time to Use / Best Case Scenarios

- While tracking new malware campaigns
 - During malware reverse engineering
 - To enrich threat intelligence reports
 - In SOCs for incident triage
-

When to Use During Investigation

- Post-malware execution
 - During IOC correlation
 - Threat attribution phases
 - Malware sample comparison
-

Best Person to Use & Required Skills

Best User: Threat Intelligence Analyst, Malware Analyst

Skills:

- Understanding of malware types
 - IOC (Indicators of Compromise) extraction
 - Working knowledge of YARA rules
 - Familiarity with API-based automation
-

Flaws / Suggestions

- Limited on-chain malware behavior
- No built-in static or dynamic analysis
- No behavioural sandbox

Suggestions:

- Add sandbox preview
 - Enable automated hash-to-sandbox linking
 - Tagging improvements with ML
-

Good About the Tool

- Easy to use, accessible UI
 - Reliable and frequently updated
 - Strong community support
 - Free and open for researchers
-

✂ Tool Name: Urlscan.io

History

Urlscan.io is a URL scanning and analysis tool founded in 2016. It captures full web-page behavior, helping identify phishing, malicious redirection, and suspicious activity.

Description

A powerful scanning service that inspects URLs by executing them in a virtual browser and returning detailed reports with network activity, visual snapshots, and behavior indicators.

What Is This Tool About?

Urlscan helps in examining URLs for phishing, redirects, and embedded malicious scripts. It's widely used in DFIR, SOC analysis, and phishing investigations.

Key Characteristics / Features

- Sandboxes live URL rendering
- Visual screenshots of page layout
- Detailed HTTP requests/responses
- Embedded script inspection
- Domain, ASN, IP geo-location
- Searchable archive of past scans
- API for automation

- Integration with browser extensions
- Verdict engine for malicious/suspicious content
- Supports passive DNS lookup

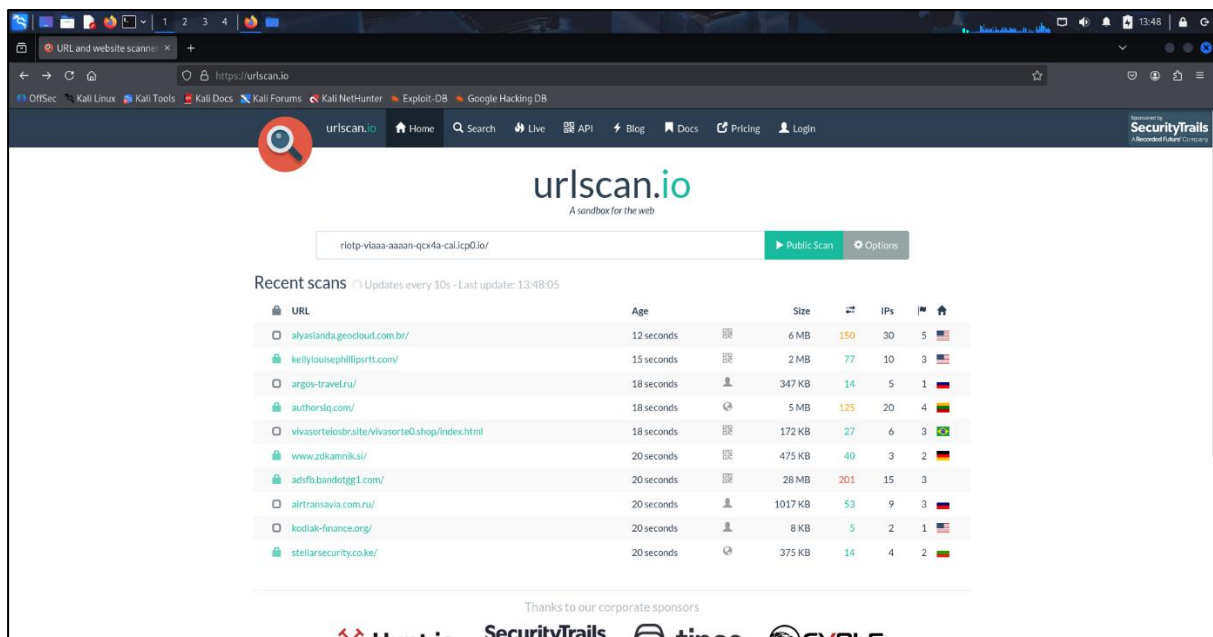
Types / Modules Available

1. Public scan
2. Private scan
3. API-based scan submission
4. Search engine for historical scans
5. Live rendering and redirection map

How Will This Tool Help?

Enables analysts to visualize phishing/malware sites, map redirections, and extract suspicious elements. Supports domain blocking decisions and threat hunting.

Proof of Concept (PoC) Images



Urlscan.io Home Page

urlscan.io/#!/019842ba-0208-7708-af99-24959630c9f9

Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

colchonesal instante.shop

3.217.171.137

URL: https://colchonesal instante.shop/

Submitted On July 25 at 12:59:00 (July 25th 2025, 5:47:02 am UTC from: K014) — Scanned from: DE

Summary

This website contacted 8 IPs in 2 countries across 5 domains to perform 55 HTTP transactions. The main IP is 3.217.171.137, located in Aalborg, United States and belongs to AMAZON AES, US. The main domain is colchonesal instante.shop. TLS certificate: issued by R11 on July 11th 2025. Valid for: 3 months.

This is the only time colchonesal instante.shop was scanned on urlscan.io!

urlscan.io Verdict: No classification

Live Information

Google Safe Browsing: No classification for colchonesal instante.shop

Current DNS A record: 3.217.171.137 (AS14618 - AMAZON AES, US)

Domain & IP Information

#	IP Address	AS
2	3.217.171.137	14618 (AMAZON AES)
25	29000900028c3ca0015f583ca021	16509 (AMAZON Q2)
1	18.245.33.197	16509 (AMAZON Q2)
1	100.29.177.207	14618 (AMAZON AES)
3	157.240.253.35	37934 (FACEBOOK)

Page Title: Colchones al instante

Detected technologies

- Cart Functionality (Commented)
- Facebook (Widgets)
- Google Tag Manager (Tag Manager)

Page Statistics

55 Requests, 100% HTTPS, 13% Domains, 5 Subdomains, 8 Cookies

urlscan.io/#!/019842ba-0208-7708-af99-24959630c9f9

Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

por cada \$2000 pesos en tu compra!

This is the only time colchonesal instante.shop was scanned on urlscan.io!

urlscan.io Verdict: No classification

Live Information

Google Safe Browsing: No classification for colchonesal instante.shop

Current DNS A record: 3.217.171.137 (AS14618 - AMAZON AES, US)

Domain & IP Information

#	IP Address	AS
2	3.217.171.137	14618 (AMAZON AES)
25	29000900028c3ca0015f583ca021	16509 (AMAZON Q2)
1	18.245.33.197	16509 (AMAZON Q2)
1	100.29.177.207	14618 (AMAZON AES)
3	157.240.253.35	37934 (FACEBOOK)

Page Title: Colchones al instante

Detected technologies

- Cart Functionality (Commented)
- Facebook (Widgets)
- Google Tag Manager (Tag Manager)

Page Statistics

55 Requests, 100% HTTPS, 13% Domains, 5 Subdomains, 8 Cookies

urlscan.io/#!/019842ba-0208-7708-af99-24959630c9f9

Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

www.youtube.com/watch?v=...

Summary

This website contacted 8 IPs in 2 countries across 5 domains to perform 55 HTTP transactions. The main IP is 3.217.171.137, located in Aalborg, United States and belongs to AMAZON AES, US. The main domain is colchonesal instante.shop. TLS certificate: issued by R11 on July 11th 2025. Valid for: 3 months.

This is the only time colchonesal instante.shop was scanned on urlscan.io!

urlscan.io Verdict: No classification

Live Information

Google Safe Browsing: No classification for colchonesal instante.shop

Current DNS A record: 3.217.171.137 (AS14618 - AMAZON AES, US)

Domain & IP Information

#	IP Address	AS
2	3.217.171.137	14618 (AMAZON AES)
25	29000900028c3ca0015f583ca021	16509 (AMAZON Q2)
1	18.245.33.197	16509 (AMAZON Q2)
1	100.29.177.207	14618 (AMAZON AES)
3	157.240.253.35	37934 (FACEBOOK)

Page Title: Colchones al instante

Detected technologies

- Cart Functionality (Commented)
- Facebook (Widgets)
- Google Tag Manager (Tag Manager)

Page Statistics

55 Requests, 100% HTTPS, 13% Domains, 5 Subdomains, 8 Cookies

urlscan.io/#!/019842ba-0208-7708-af99-24959630c9f9

Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

network error

URL: https://googleads.g.doubleclick.net/pagead/viewthroughconversion/967905656/?toad=innertube&name=1&view=2.20250725&data=ba...
Failed to load resource: net::ERR_FAILED

rendering warning

URL: https://www.youtube.com/watch?v=...
Message: [GroupMarketHotSettoBug.com/24-29911AGP0020A+3CE0005Automatic fallback to software WebGL has been deprecated. Please use the --enable-unsafe-webgl flag to opt in to lower security guarantees for tested content.]

Security Headers

This page lists any security headers set by the main page. If you want to understand what these mean and how to use them, head on over to this page.

Header	Value
Content-Security-Policy	require-trusted-types-for 'script'
Strict-Transport-Security	max-age=31536000
X-Content-Type-Options	nosniff
X-Frame-Options	SAMEORIGIN
X-XSS-Protection	0

10 Cookies

Cookies are little pieces of information stored in the browser of a user. Whenever a user visits the site again, he will also send his cookie values, thus allowing the website to re-identify him even if he changed locations. This is how permanent logins work.

Domain/Path	Expires	Name / Value
.tinyurl.com/	1970-01-21 07:04:27	Name: _cf_bm Value: 71pfuTjWjWayNN4C0Um6bHYD55QeZ16ZicNw9Y-1753466143-1.0.1.1-0Z6a_gOmUvzv3vXWWMt4pLekGKay07nbsE3YkLjd_kD Wz6NwrcBKUjbiQz3kQzgwWNa1nvptPurRvVwCq-HJ5WCB_eLJE4H
.youtube.com/	1970-01-21 07:04:27	Name: GPS Value: 1
.youtube.com/	1969-12-31 23:59:59	Name: YSC Value: vYknDrWo
.youtube.com/	1970-01-21 11:23:38	Name: VISITOR_INFO1_LIVE Value: oPhMQBE0As
.youtube.com/	1970-01-21 11:23:38	Name: VISITOR_PRIVACY_METADATA Value: CpDQRIEGeAgPQ3D3D
.youtube.com/	1970-01-21 16:40:26	Name: PREF Value: tz=America/Vancouver
.youtube.com/	1970-01-21 11:23:38	Name: _Secure-ROLLOUT_TOKEN Value: CNaex476kx61-GEqyZcyYgMYaahrYgM3D
.doubleclick.net/	1970-01-21 07:04:27	Name: test_cookie Value: CheckForPermission
.google.com/	1970-01-21 11:27:57	Name: NID Value: S25-DihTR8u57K15WIE4whUj-SPIEcK8Bw-SE4h2qHq-F4v7X8tqyD4lu403kr5nXT3vWbZQyC5ZOF4uWV3kCSPK2Ww7q2icR4 OBFdUNQkug0TVQpJnH2pT3vP4LydA82PKH7mK50NESvSxwS_Aemte9Ktazp7Tq0NHdpUow
.google.ca/	1970-01-21 11:27:57	Name: NID Value: S25-EpCuYyYmKAM6uq_Bu8E_SlmttqAUZ400HvD653Hw-0Uln8uX4HwW772P8-2vZ11WR4XnK-5gaV2mFdsTWm2rJgMqy MhH44S4kgelTg-pf507phqayFuH4w7Y71Hbz71Vu24ITU8Zu6-QQ3B8MQy_ytZpY4H4wVwVJH-Ja7F

3 Console Messages

A page may trigger messages to the console to be logged. These are often error messages about being unable to load a resource or execute a piece of JavaScript. Sometimes they also come from scripts that the browser has loaded.

Scanning Results of Various Suspicious Links

❏ 15-Liner Summary

1. Browser-based URL scanner
 2. Provides HTTP request chains
 3. Tracks iframe and JS scripts
 4. Useful for phishing site detection
 5. Offers visual preview
 6. Cloud-hosted, easy to use
 7. Search previous scans
 8. Geo-data of hosting IP
 9. Whois and DNS info included
 10. Sandbox-based execution
 11. Exportable JSON report
 12. Fast, real-time results
 13. Threat intelligence integration
 14. Good for phishing and scam analysis
 15. Completely browser-based; no local install
-

🕒 Time to Use / Best Case Scenarios

- When analyzing phishing emails
 - During suspicious link triage
 - For real-time scan of URLs from chat/email
-

👤 When to Use During Investigation

- Phishing investigation
 - Scam URL verification
 - Suspicious redirect chain analysis
 - Ad fraud or domain reputation checking
-

👤💻 Best Person to Use & Required Skills

Best User: SOC Analyst, Threat Hunter

Skills:

- Basic knowledge of HTTP/HTTPS
 - Understanding phishing indicators
 - Ability to interpret redirection maps
 - Familiarity with JavaScript behavior
-

❑ **Flaws / Suggestions**

- Limited depth in behavioral analysis
- Does not simulate login behavior
- No email integration

Suggestions:

- Simulate more realistic user behavior
 - Browser fingerprint variation options
 - Add malware sandbox tie-ins
-

☑ **Good About the Tool**

- No install required
- Quick scan turnaround
- Great visualization
- Supports private scans for sensitive URLs