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

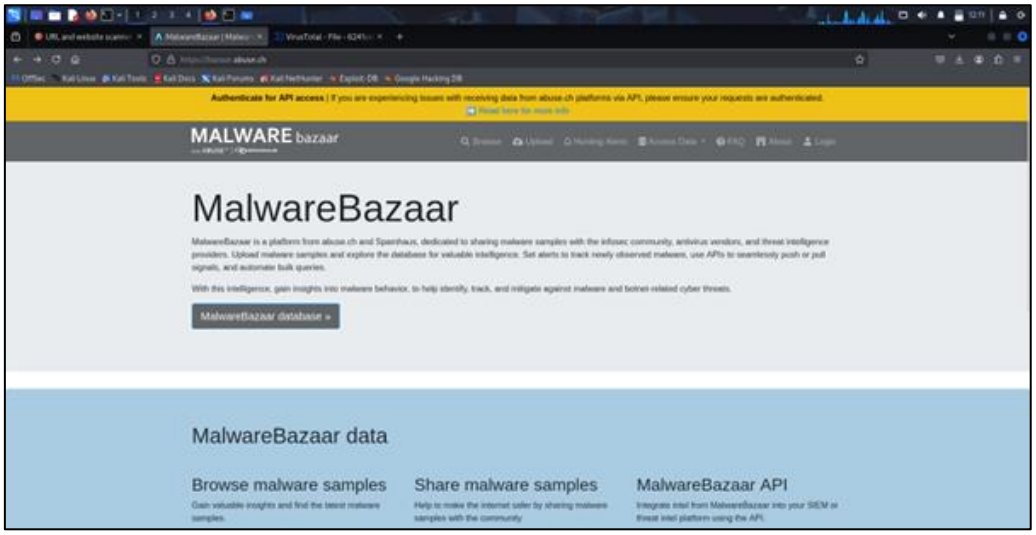
🔗 Types / Modules Available

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

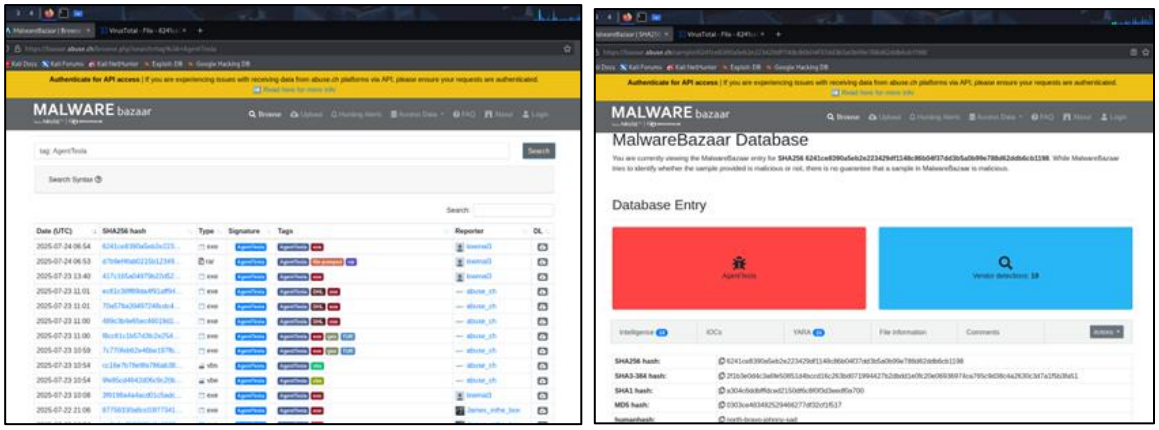
🎯 How Will This Tool Help?

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.

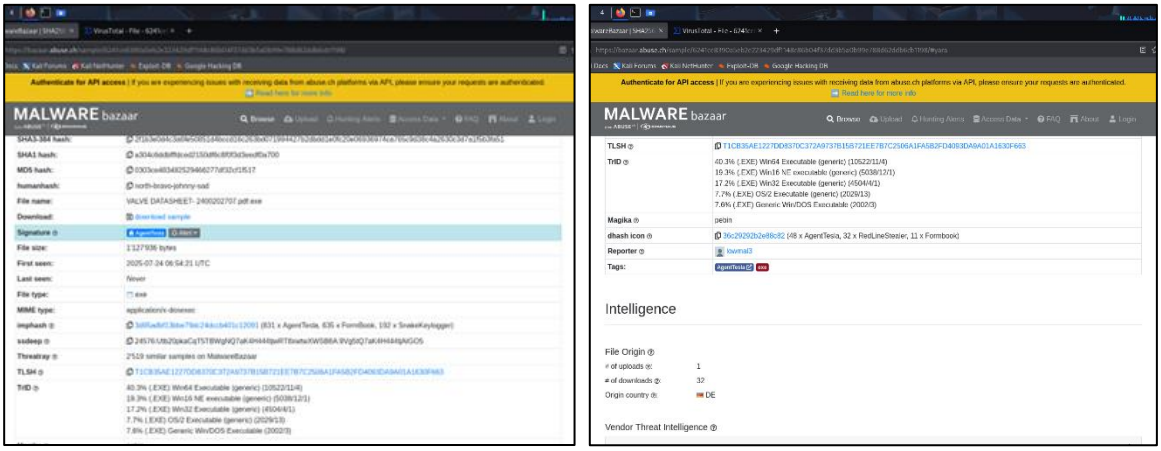
🖼 Proof of Concept (PoC) Images



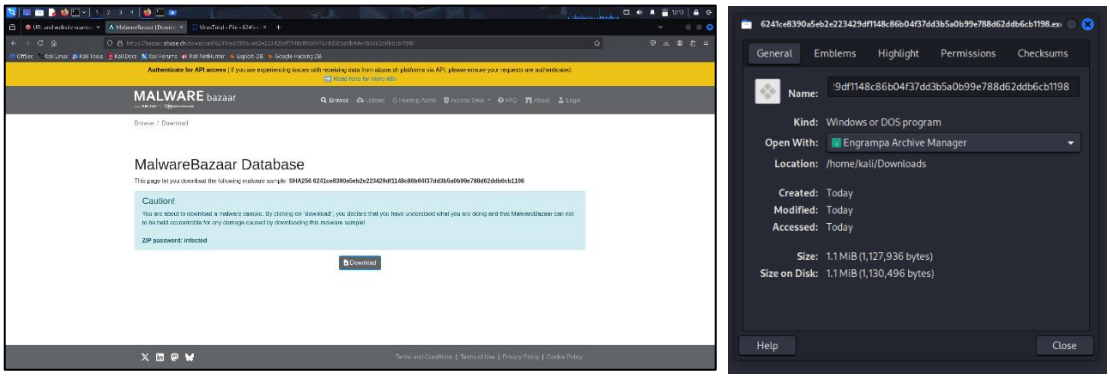
Malware Bazaar Main Page



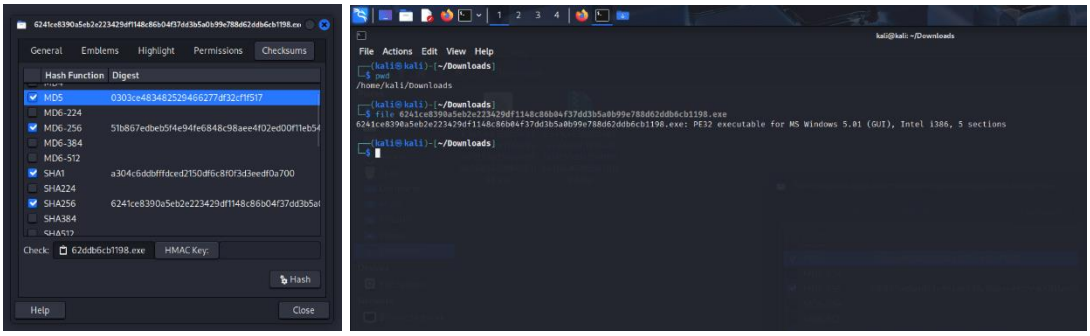
Selecting Malware by Browsing



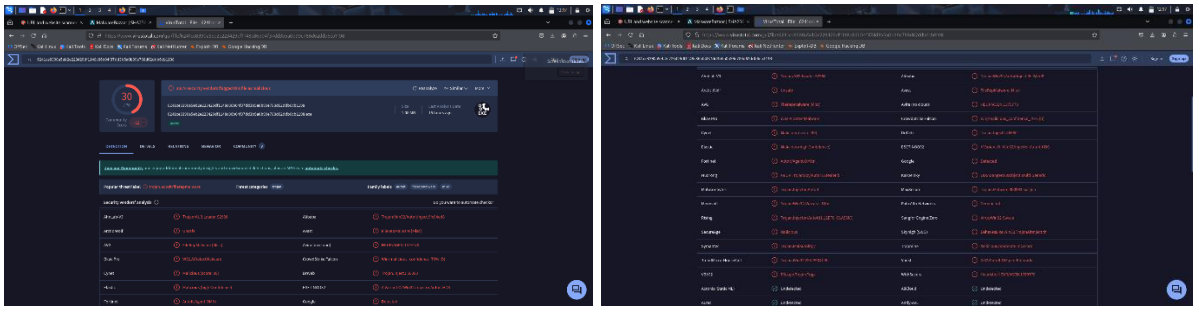
Malware Information given in the Malware Bazaar interface



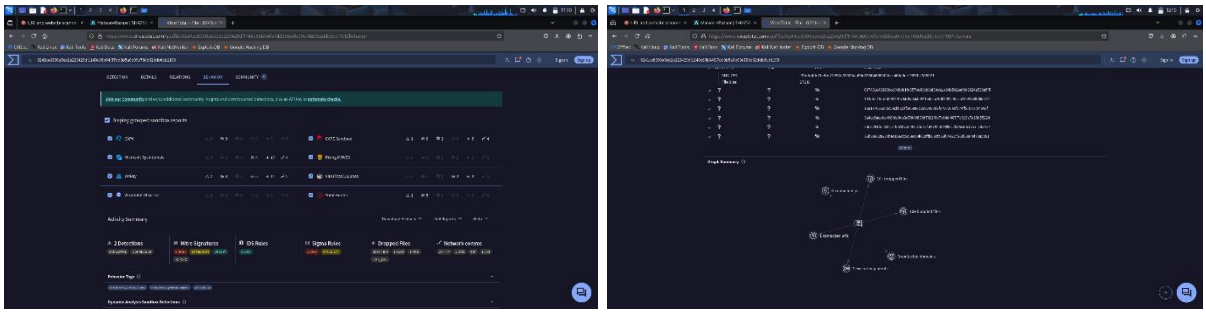
Downloading Sample and Analysis of File Properties



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

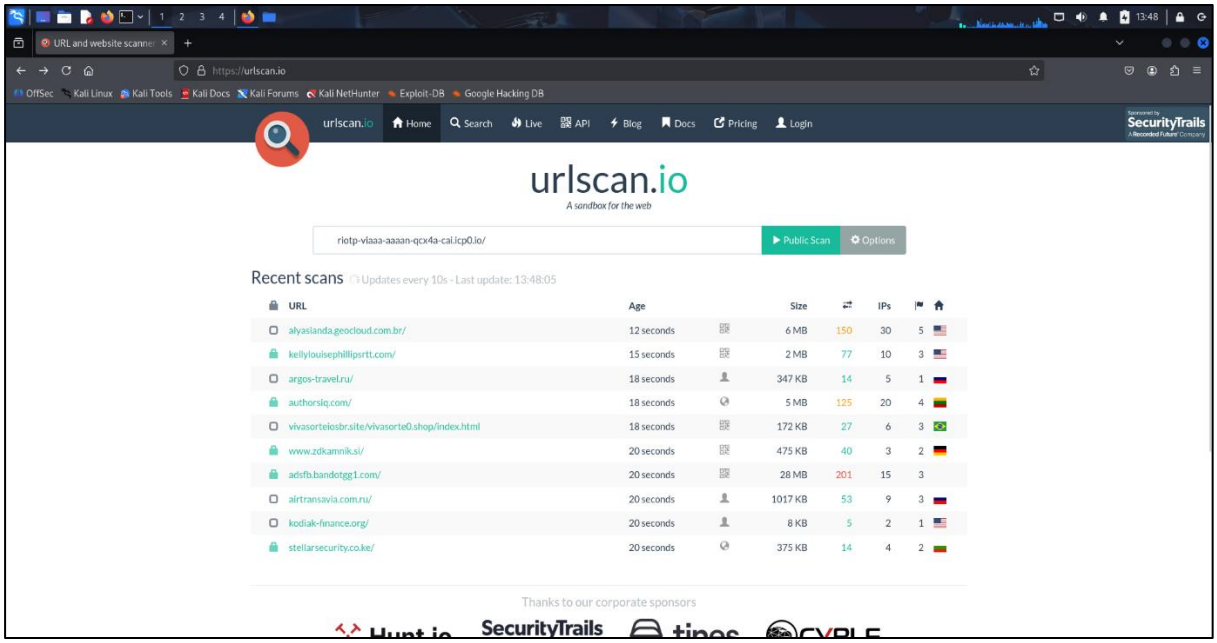
🔧 Types / Modules Available

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

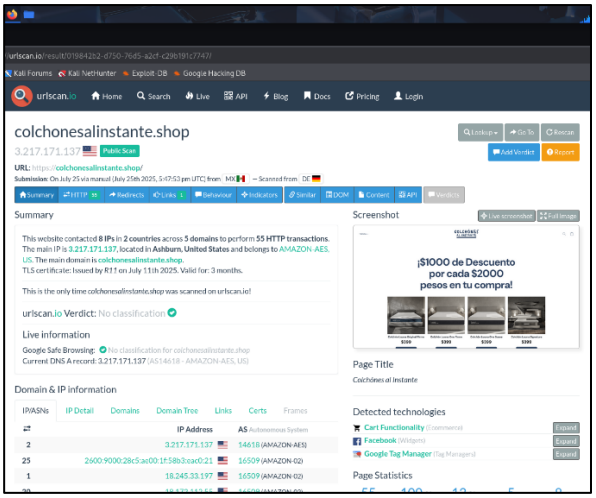
🎯 How Will This Tool Help?

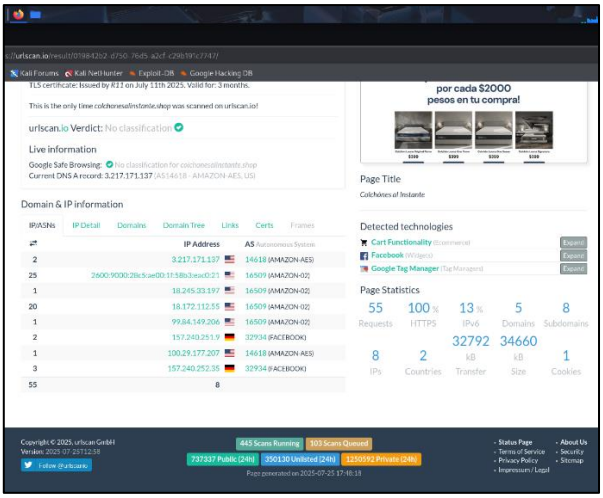
Enables analysts to visualize phishing/malware sites, map redirections, and extract suspicious elements. Supports domain blocking decisions and threat hunting.

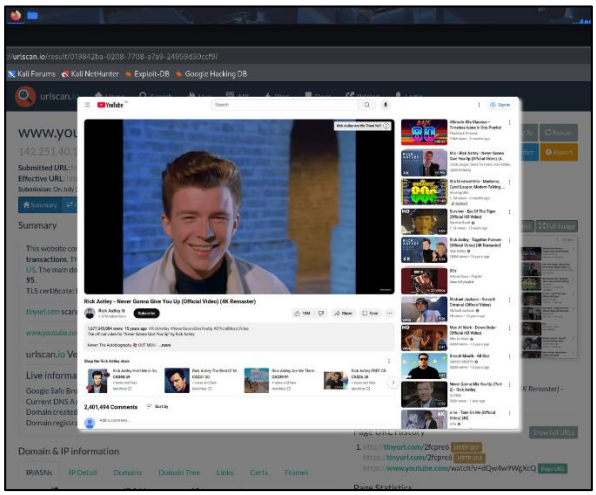
🖼 Proof of Concept (PoC) Images

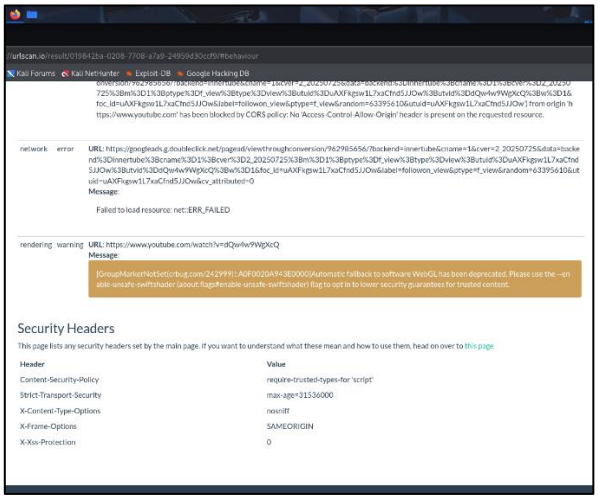


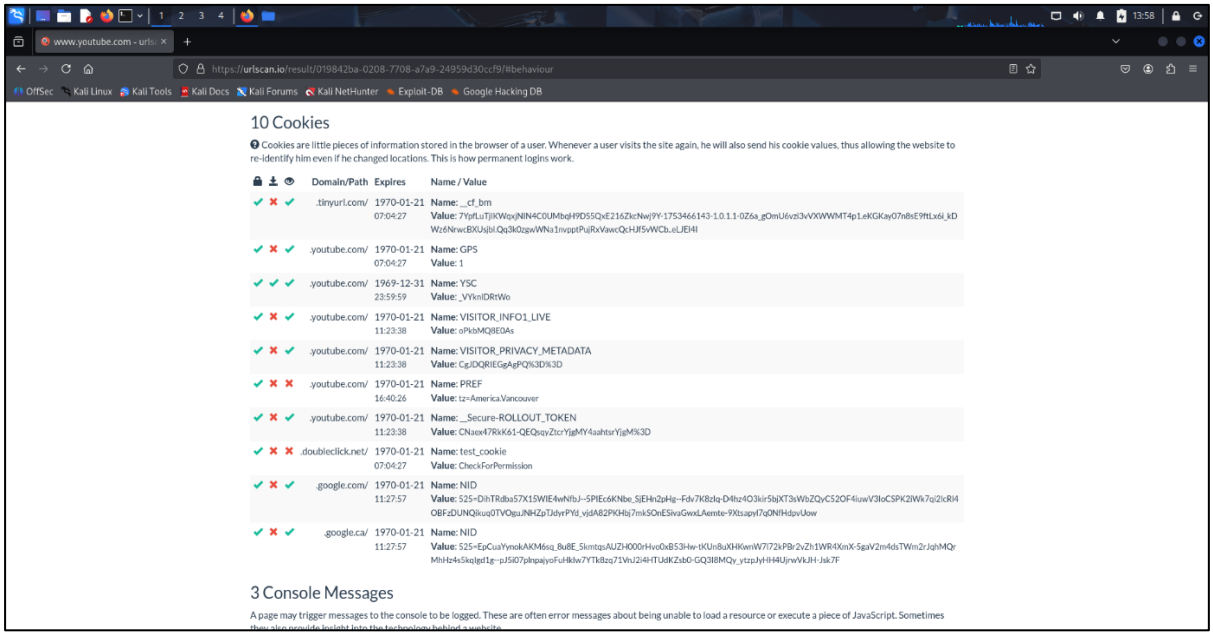
Urlscan.io Home Page











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