Proof of Concept (POC)

Tool name: 2lingual Search (click here)

History:

2lingual.com was created as an experimental bilingual search tool. It's not a big company product like Google or Bing, but rather a personal project developed by a web developer named Michael S. to help users search in two languages at the same time.

Description:

2lingual Search is a **bilingual search engine** that allows you to search in **two languages side-by-side** at the same time. It's mainly used by cybersecurity researchers, translators, students, and international users who want to explore content in multiple languages — especially when the original data or discussion is happening in a non-English language like Chinese or Russian.

Why use this tool?

🔍 1. Search in Two Languages at Once

You can search the same keyword in two languages (e.g., English and Chinese) side-by-side.

- No need to translate or search twice.
- Saves time and effort.

🌐 2. Access Foreign Language Information

Sometimes useful or original info is only available in another language.

Example:

- Cybersecurity topics (like malware) might be discussed first in Chinese or Russian forums.
- With 2lingual, you can find those non-English sources.

🔒 3. Useful for Cybersecurity Research

- Cybercriminals often post tools or guides in non-English forums.
- You can track threats, tool names, or code posted in Chinese, Russian, etc.
- This helps you find early warnings or rare information not found in English.

💬 4. Great for Translators and Researchers

If you're comparing how a topic is covered in different countries or trying to learn a new language:

- You can see how the same keyword gives different results in both languages.
- Helps with translation accuracy and learning.

🧠 5. Language Learning Support

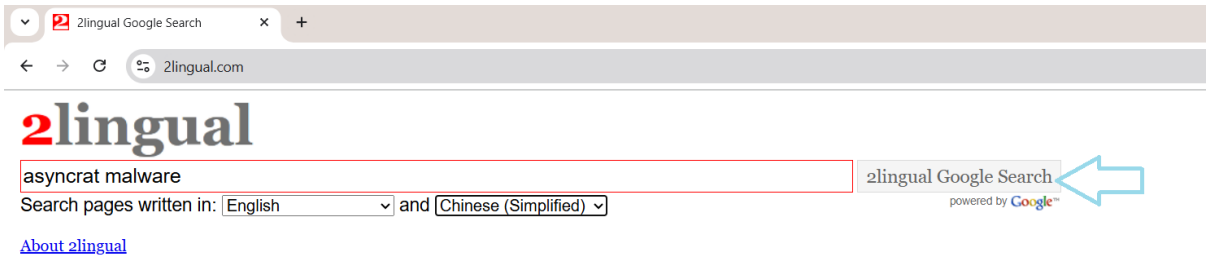
Students can:

- Search the same word in two languages.
- Understand usage, meaning, and sentence examples from both sides.

Key Characteristics/Features:

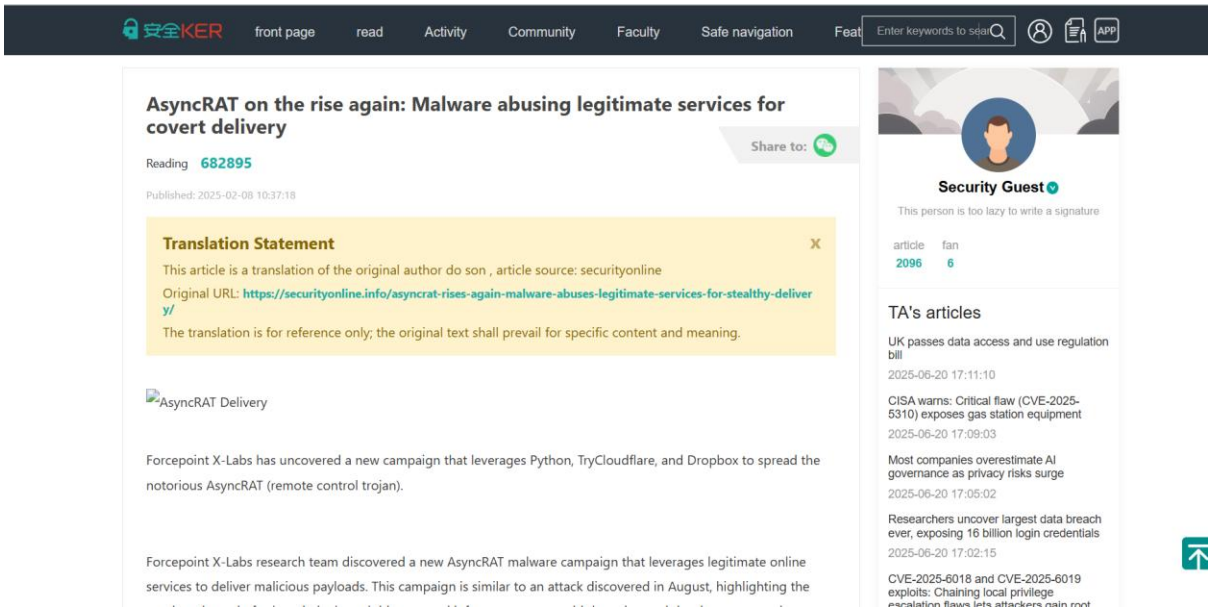
- Dual-language search
- Google-powered
- Split-screen layout
- Helps in understanding foreign content
- Supports multiple search types
- No login required
- Useful for research

Images:



This image is split into two screens:

- left side shows English search result
- Right side shows Chinese search result



Time to Use / Best Case Scenarios:

Use **2lingual search** when:

- You need to **search for the same keyword in two languages**.
- You are doing **cybersecurity research** on malware that might be spreading in **non-English regions** (e.g., China, Russia).
- You are a **translator, researcher, or student** comparing how different cultures/languages discuss the same topic.
- You are trying to **track the original source** of a topic (news, malware, idea) shared in a foreign language.

🔍 When to Use During Investigation:

Use it in early stages of cybersecurity or threat investigation:

- While collecting **open-source intelligence (OSINT)**
- While checking if malware/tool/attack is discussed in **non-English forums**
- When identifying if a tool like **AsyncRAT** or **RedLine Stealer** is active in foreign regions
- To **find leaked tools or conversations** about vulnerabilities

👤 Best Person to Use This Tool & Required Skills:

Role	Skills Required
Cybersecurity analyst	Basic search techniques, understanding threat terms
OSINT researcher	Ability to recognize relevant results in both languages
Translator	Language skills, knowledge of cultural context

- **No advanced tech skills required – easy-to-use tool.**

Suggestions to Improve the Tool:

- ✓ Add built-in translation (side-by-side translation of results).
- ✓ Let users save or export results for future use.
- ✓ Add AI keyword suggestions in both languages.
- ✓ Improve support for more search engines (like Bing or Yandex).
- ✓ Mobile-friendly design or app version.

There is not really an alternative for this site that have exact feature/characteristics. if improvised properly it can transform into something more unique and useful.

Tool name: Abuse.ch (click here)

History:

Abuse.ch started as a community-driven cybersecurity project to track and share information about malware, botnets, and other cyber threats. It is maintained by researchers and volunteers who collect and publish Indicators of Compromise (IOCs) like malicious URLs, IPs, domains, and file hashes to help defenders block attacks.

Description:

Abuse.ch provides multiple free online services and feeds that help cybersecurity professionals detect, block, and analyze malware infections. It focuses on tracking active threats worldwide by sharing up-to-date blacklists of malicious domains, URLs, and malware samples.

Why Use This Tool?

🔍 1. Real-Time Threat Intelligence

- Access continuously updated lists of malware distribution URLs, botnet command-and-control servers, and phishing domains.
- Enables fast blocking and detection to protect networks.

🛡️ 2. Malware Sample Repository

- Download malware samples safely for research and analysis.
- Supports reverse engineering and threat hunting.

🌐 3. Global Coverage

- Tracks threats from all over the world, especially malware active in non-English speaking regions.
- Helps detect new variants before they spread widely.

⚙️ 4. Integration Friendly

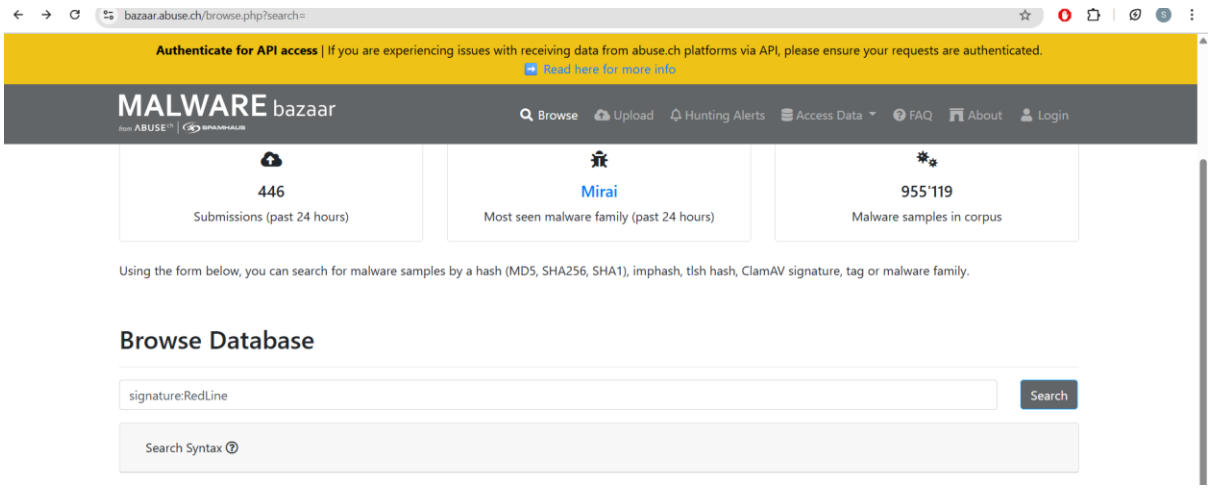
- Feeds available in CSV, JSON, and MISP formats for automated ingestion into security tools and SIEM systems.

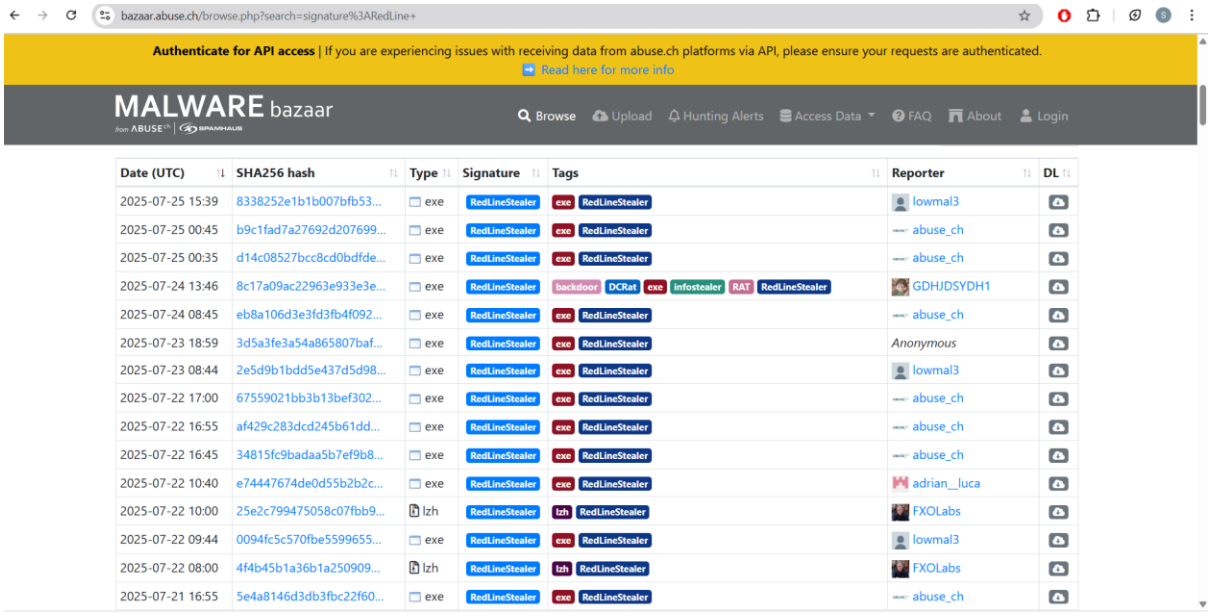
Key Features

- Multiple project portals like URLhaus, MalwareBazaar, ThreatFox, and Feodo Tracker
- Provides IPs, URLs, hashes, domains related to active malware and botnets
- Free, no login required
- API access for automation
- Community-driven and regularly updated

Images:

Malware Bazaar





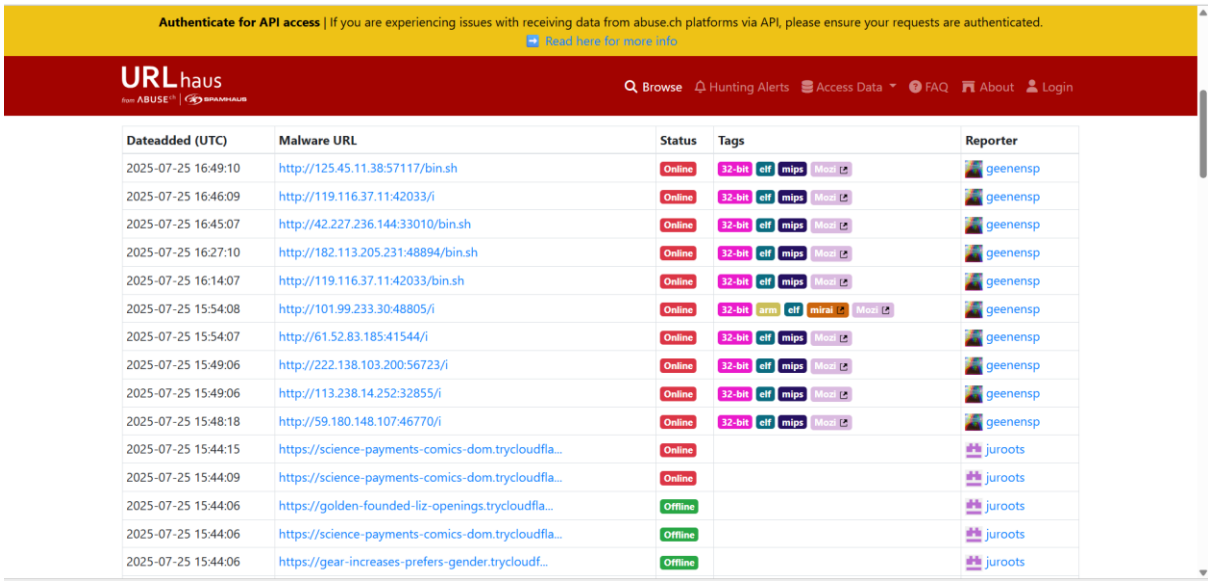
e.g.:

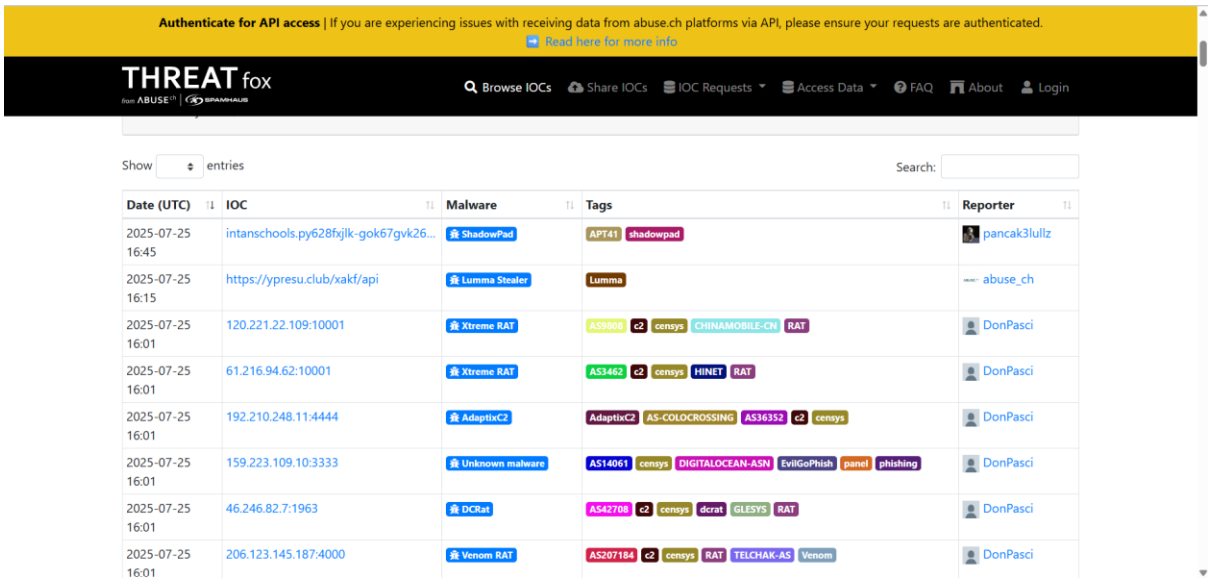
b9c1fad7a27692d207699f147b1f2a98b6469cf63f66208ac0c1a4f9560135d1

Although this specific sample has no analyst comment on VirusTotal, multiple engines detect it as RedLineStealer. Its type and tags indicate it's an info-stealing executable file

How to create hash?

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\3520 i5 16GB> cd Downloads
PS C:\Users\3520 i5 16GB\Downloads> Get-FileHash DevOps_for_Digital_Leaders.pdf -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          E21A7D32A3F22192E3B3CF9FB80CAC5FC003FDC6A6D1AC0A4E3F628DBF16A69D       C:\Users\3520 i5 16GB\Downloa...


PS C:\Users\3520 i5 16GB\Downloads>
```





Time to Use / Best Case Scenarios

Use Abuse.ch when:

- You need current lists of malicious URLs or malware hashes to protect a network
- Performing malware research or reverse engineering
- Investigating botnet activity or phishing campaigns
- Collecting threat intelligence for SOC or CERT operations
- Tracking malware spread in non-English speaking countries

Best Person to Use This Tool & Required Skills:

Role	Skills Required
Cybersecurity Analyst	Basic knowledge of malware, threat detection
Malware Researcher	Reverse engineering, malware analysis
SOC Team Member	Incident detection, using IOCs and feeds
OSINT Researcher	Analyzing open-source cyber threat data

Suggestions to Improve the Tool

- ✓ Add a user-friendly dashboard for visualization of threat data
- ✓ Implement built-in alerts for new malicious URLs or hashes
- ✓ Enhance API with more query options and data filtering
- ✓ Add more language support for global threat reports
- ✓ Develop mobile-friendly app or notification system

Author: Shreya Bishwas Pandey

Intern id:120

What this PoC intends to achieve:

This Proof of Concept demonstrates how the 2lingual Search Tool and Abuse.ch resources can be used together to improve cybersecurity threat intelligence. It aims to show how combining multilingual search capabilities with updated malware data helps cybersecurity professionals identify, track, and analyze new and emerging cyber threats more effectively.