

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

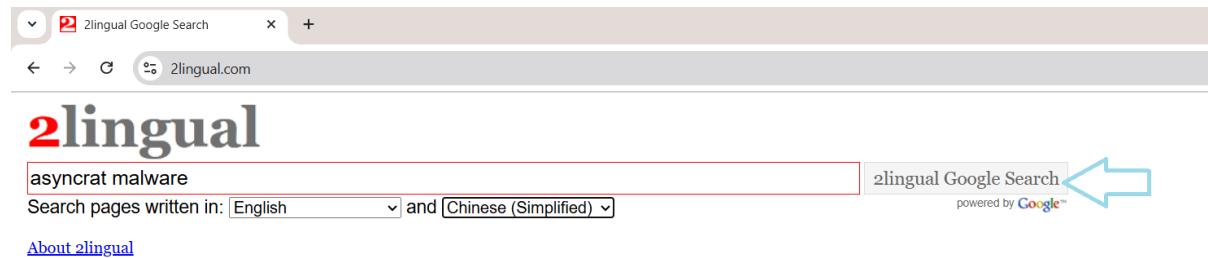
Students can:

- 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:



asyncrat malware - 2lingual Google Search

2lingual.com/2lingual-google-search?qt=1&q=asyncrat+malware&btn=2lingual+Google+Search&lr1=lang_en&lr2=lang_zh-CN

2lingual

asyncrat malware

Search pages written in: English and Chinese (Simplified)

2lingual Google Search

powered by Google™

English results for asyncrat malware

AsyncRAT (Malware Family)

malpedia.caad.fkie.fraunhofer.de

AsyncRAT is a Remote Access Tool (RAT) designed to remotely monitor and control other computers through a secure encrypted connection.

AsyncRAT Reloaded: Using Python and TryCloudflare for Malware ...

www.forcepoint.com

 31 Jan 2025 ... AsyncRAT is remote access trojan (RAT) that exploits the await pattern for efficient, asynchronous communication.

Unmasking AsyncRAT New Infection Chain | McAfee Blog

www.mcafee.com

 3 Nov 2023 ... AsyncRAT, short for "Asynchronous Remote Access Trojan," is a sophisticated piece of malware designed to compromise the security of computer ...

Trojan:MSIL/AsyncRAT

www.microsoft.com

Learn how to protect your PC from virus and malware attacks by researching and reviewing malware descriptions.

Hunt of the Month: Detecting AsyncRAT Malware Over HTTPS ...

corelight.com

 20 Mar 2024 ... We can detect AsyncRAT infections where the C2 server used a default SSL certificate despite the rest of the C2 data encrypted over HTTPS.

From DarkGate to AsyncRAT: Malware Detected and Shared As ...

I Init

Simplified Chinese results for asyncrat 恶意软件 - [Translated asyncrat malware from English to Simplified Chinese] - Turn off automatic query translation

Cracked Software or Cyber Trap? The Rising Danger of AsyncRAT ...

www.mcafee.com

 19 Sept 2024 ... Putting it in Dnspy, we can see an unobfuscated Asyncrat client payload named AsyncClient. ... Fake Android Money Transfer App Targeting Bengali- ...

Victims risk AsyncRAT infection after being redirected to fake ...

www.malwarebytes.com

 2 Jun 2025 ... We found that cybercriminals are preparing for the impending holiday season with a redirect campaign leading to AsyncRAT.

工信部：关于防范AsyncRAT恶意软件的风险提示- 安全内参| 决策者的 ...

www.secrss.com

 24 Oct 2024 ... AsyncRAT是一款针对Windows系统的远程访问恶意软件，具有隐蔽性强和功能全面等特点。在最新的AsyncRAT恶意软件活动中，攻击者采用多阶段攻击策略，利用 ...

惡意軟體AsyncRAT透過冒牌Booking.com訂房網站散布 iHome

www.ithome.com.tw

 10 Jun 2025 ... 資安業者 Malwarebytes 揭露自5月中旬出現的網釣攻擊活動，駭客設置冒牌的Booking.com訂房網站，並透過電玩網站、社群網站、廣告的惡意連結，來引誘使用者上門 ...

網絡釣魚攻擊冒充Booking.com 以一系列惡意軟件竊取憑證- Source

This image is split into two screens:

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

asyncrat再次崛起：恶意软件滥用合法服务进行秘密交付

阅读量 682895

发布时间：2025-02-08 10:37:18

译文声明

本文是翻译文章，文章原作者 do son，文章来源：securityonline
原文地址：<https://securityonline.info/asyncrat-rises-again-malware-abuses-legitimate-services-for-stealthy-delivery/>
译文仅供参考，具体内容表达以及含义原文为准。

AsyncRAT Delivery

Forcepoint X – Labs 曝光了一场新的攻击活动，该活动利用 Python、TryCloudflare 和 Dropbox 来传播臭名昭著的 AsyncRAT（远控木马）。

Forcepoint X – Labs 研究团队发现了一场新的 AsyncRAT 恶意软件攻击活动，此次活动利用合法的在线服务来传递恶意有效载荷。这场活动与 8 月份发现的一次攻击类似，凸显了网络犯罪分子持续利用可信基础设施来躲避检测并欺骗毫无防备用户的趋势。

分享到： 

安全客

这个人太懒了，签名都懒得写一个

文章 粉丝
2096 6

TA的文章

英国通过数据访问和使用监管法案
2025-06-20 17:11:00

CISA警告：严重缺陷 (CVE-2025-5310)
暴露加油站设备
2025-06-20 17:09:03

大多数公司高估了AI治理，因为隐私风险激增
2025-06-20 17:05:02

研究人员发现了有史以来最大的数据泄密事件，暴露了160亿个登录凭证
2025-06-20 17:02:15

CVE-2025-6018和CVE-2025-6019漏洞利用：链接本地特权升级缺陷让攻击者获得大多数Linux发行版的root访问权限

The screenshot shows a news article titled "AsyncRAT on the rise again: Malware abusing legitimate services for covert delivery". The article was published on 2025-02-08 at 10:37:18. It includes a "Translation Statement" box, a sidebar for "Security Guest", and a "TA's articles" sidebar.

Translation Statement:

This article is a translation of the original author do son , article source: securityonline
Original URL: <https://securityonline.info/asyncreat-rises-again-malware-abuses-legitimate-services-for-stealthy-delivery/>

The translation is for reference only; the original text shall prevail for specific content and meaning.

Security Guest:

This person is too lazy to write a signature

TA's articles:

- UK passes data access and use regulation bill (2025-06-20 17:11:10)
- CISA warns: Critical flaw (CVE-2025-5310) exposes gas station equipment (2025-06-20 17:09:03)
- Most companies overestimate AI governance as privacy risks surge (2025-06-20 17:05:02)
- Researchers uncover largest data breach ever, exposing 16 billion login credentials (2025-06-20 17:02:15)
- CVE-2025-6018 and CVE-2025-6019 exploits: Chaining local privilege escalation flaws lets attackers gain root (2025-06-20 17:00:01)

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:



OUR MISSION

Making the Internet a safer place by providing actionable, community-driven threat intelligence data.

abuse.ch has been effecting change on cybercrime for almost twenty years, owing to global recognition of our identified and tracked cyber threat signals. Supported by a community of 15,000 specialist researchers, abuse.ch's independent intelligence is relied on by security researchers, network operators and law enforcement agencies.

Together with [Spanhaus](#), we provide the largest, independently crowdsourced intelligence of tracked malware and botnets to the industry. We develop and operate specialized platforms, built for IT security experts, to share and access relevant threat intel data.

Malware Bazaar

bazaar.abuse.ch/browse.php?search=

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated.
[Read here for more info](#)

MALWARE bazaar from ABUSE.ch SPAMHAUS

446 Submissions (past 24 hours) **Mirai** Most seen malware family (past 24 hours) **955'119** Malware samples in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

Browse Database

signature:RedLine

Search Syntax [?](#)

bazaar.abuse.ch/browse.php?search=signature%3ARedLine+

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated.
[Read here for more info](#)

MALWARE bazaar from ABUSE.ch SPAMHAUS

SHA256 hash **Type** **Signature** **Tags** **Reporter** **DL**

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-07-25 15:39	8338252e1b1b007fb53...	exe	RedLineStealer	RedLineStealer	lowmal3	
2025-07-25 00:45	b9c1fad7a27692d207699...	exe	RedLineStealer	RedLineStealer	abuse_ch	
2025-07-25 00:35	d14c08527bcc8cd0bdfe...	exe	RedLineStealer	RedLineStealer	abuse_ch	
2025-07-24 13:46	8c17a09ac22963e933e3e...	exe	RedLineStealer	backdoor DCRat exe Infostealer RAT RedLineStealer	GDHJDSDYDH1	
2025-07-24 08:45	eb8a106d3e3fd3fb4f092...	exe	RedLineStealer	RedLineStealer	abuse_ch	
2025-07-23 18:59	3d5a3fe3a54a865807baf...	exe	RedLineStealer	RedLineStealer	Anonymous	
2025-07-23 08:44	2e5d9b1bdd5e437d5d98...	exe	RedLineStealer	RedLineStealer	lowmal3	
2025-07-22 17:00	67559021bb3b13bef302...	exe	RedLineStealer	RedLineStealer	abuse_ch	
2025-07-22 16:55	af429c283cd245b61dd...	exe	RedLineStealer	RedLineStealer	abuse_ch	
2025-07-22 16:45	34815fc9badaa5b7ef9b8...	exe	RedLineStealer	RedLineStealer	abuse_ch	
2025-07-22 10:40	e74447674de0d55b2b2c...	exe	RedLineStealer	RedLineStealer	adrian_luca	
2025-07-22 10:00	25e2c799475058c07bb9...	Izh	RedLineStealer	Izh RedLineStealer	FXOLabs	
2025-07-22 09:44	0094fc5c570fe559655...	exe	RedLineStealer	RedLineStealer	lowmal3	
2025-07-22 08:00	4f4b45b1a36b1a250909...	Izh	RedLineStealer	Izh RedLineStealer	FXOLabs	
2025-07-21 16:55	5e4a8146d3db3fb22f60...	exe	RedLineStealer	RedLineStealer	abuse_ch	

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
-----      -----
SHA256        E21A7D32A3F22192E3B3CF9FB80CAC5FC003FDC6A6D1AC0A4E3F628DBF16A69D          Path
-----      -----
PS C:\Users\3520 i5 16GB\Downloads>
```

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated.
[Read here for more info](#)

URLhaus
from ABUSE.ch | SPAMHAUS

Q Browse **Hunting Alerts** **Access Data** **FAQ** **About** **Login**

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2025-07-25 16:49:10	http://125.45.11.38.57117/bin.sh	Online	32-bit elf mips Mod	geenensp
2025-07-25 16:46:09	http://119.116.37.11:42033/i	Online	32-bit elf mips Mod	geenensp
2025-07-25 16:45:07	http://42.227.236.144:33010/bin.sh	Online	32-bit elf mips Mod	geenensp
2025-07-25 16:27:10	http://182.113.205.231:48894/bin.sh	Online	32-bit elf mips Mod	geenensp
2025-07-25 16:14:07	http://119.116.37.11:42033/bin.sh	Online	32-bit elf mips Mod	geenensp
2025-07-25 15:54:08	http://101.99.233.30:48805/i	Online	32-bit arm elf mirai Mod	geenensp
2025-07-25 15:54:07	http://61.52.83.185.41544/i	Online	32-bit elf mips Mod	geenensp
2025-07-25 15:49:06	http://222.138.103.200:56723/i	Online	32-bit elf mips Mod	geenensp
2025-07-25 15:49:06	http://113.238.14.252:32855/i	Online	32-bit elf mips Mod	geenensp
2025-07-25 15:48:18	http://59.180.148.107:46770/i	Online	32-bit elf mips Mod	geenensp
2025-07-25 15:44:15	https://science-payments-comics-dom.trycloudfla...	Online		juroots
2025-07-25 15:44:09	https://science-payments-comics-dom.trycloudfla...	Online		juroots
2025-07-25 15:44:06	https://golden-founded-liz-openings.trycloudfla...	Offline		juroots
2025-07-25 15:44:06	https://science-payments-comics-dom.trycloudfla...	Offline		juroots
2025-07-25 15:44:06	https://gear-increases-prefers-gender.trycloudf...	Offline		juroots

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated.
[Read here for more info](#)

THREATfox
from ABUSE.ch | SPAMHAUS

Q Browse IOCs **Share IOCs** **IOC Requests** **Access Data** **FAQ** **About** **Login**

Show **entries** Search:

Date (UTC)	IOC	Malware	Tags	Reporter
2025-07-25 16:45	intschools.py628fxjk-gok67gvk26...	ShadowPad	APT41 shadowpad	pancak3luliz
2025-07-25 16:15	https://ypresu.club/xakf/api	Lumma Stealer	Lumma	abuse_ch
2025-07-25 16:01	120.221.22.109:10001	Xtreme RAT	AS9806 c2 censys CHINAMOBILE-CH RAT	DonPasci
2025-07-25 16:01	61.216.94.62:10001	Xtreme RAT	AS3462 c2 censys HINET RAT	DonPasci
2025-07-25 16:01	192.210.248.11:4444	AdaptixC2	AdaptixC2 AS-COLOCROSSING AS36352 c2 censys	DonPasci
2025-07-25 16:01	159.223.109.10:3333	Unknown malware	AS14061 censys DIGITALOCEAN-ASN EvilGoPhish panel phishing	DonPasci
2025-07-25 16:01	46.246.82.7:1963	DCRat	AS42708 c2 censys dcrat GLESYS RAT	DonPasci
2025-07-25 16:01	206.123.145.187:4000	Venom RAT	AS207184 c2 censys RAT TELCHAK-AS Venom	DonPasci

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.