FINANCIAL FRAUD INVESTIGATION:

Tips & Techniques Booklet

silo

By Authentic8

Table of Contents

Keep your online fraud investigations anonymous and secure, even on the dark web

Silo for Research (Toolbox) is a secure and anonymous web browsing solution that enables users to conduct research, collect evidence and analyze data across the open, deep and dark web. Silo for Research is built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

Financial fraud, crime and AML investigators can accomplish their goals without introducing risk to the organization or revealing intent. All web activity is logged and encrypted so compliance teams can be sure that the tools are being used appropriately.

Full Isolation:
All web code is executed on Silo servers, not end-user devices

Cloud-Based:
Turn-key, cloud-hosted solution that creates a clean instance every time

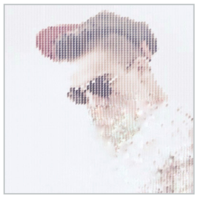
Managed Attribution:
Configure the browser fingerprint and egress location

Access Open, Deep or Dark Web:
One-click access to any destination without tainting your environment

Workflow Enhancements:
Integrated tools for content capture, analysis and storage

Complete Audit Oversight:
Encrypted audit logs of all web activity are captured in one place and easily exported

Contributors



Amir Khashayar Mohammadi designs security systems and creates content as a Cybersecurity Specialist at Authentic8, with a focus on malware analysis, cryptanalysis, web exploitation, and other cyber-attack vectors. A Computer Science and Engineering major, he likes to write blogs, conduct vulnerability research, and work on automation projects.

Daniel Ben-Chitrit is the Sr. Product Manager for Cyber and Open Source Threat Intelligence at Authentic8. He brings almost a decade of experience building cyber security products and performing threat hunting to support threat intelligence collection and analysis across both the Public and Private sector.

Jeff Ennis is the Director of Systems Engineering for Authentic8's Federal team, supporting Civilian, DoD, and IC agencies. He brings 20 years of information technology and cybersecurity experience in both the end user and vendor communities, including HP, VMware, IBM, UUNET, and Lockheed Martin.

Jeff Phillips is the Director of Product Marketing for Authentic8, where he focuses on driving product go-to-market strategy and enabling sales. Prior to Authentic8, Jeff has had a successful history launching products at startups and Fortune 100 companies, including Microsoft.

Matt Ashburn is the national security engagement lead at Authentic8. Previously, Matt served as a CIA officer focusing on cyber issues, including a detail serving on the National Security Council as the Chief Information Security Officer and Special Advisor to the National Security Advisor, leading technical expertise, risk reduction strategies, and policy for national security systems.

Nick Finnberg started his intelligence career as an Army National Guard Intelligence Analyst, dedicating four years to the counterdrug task force and specializing in large-scale money laundering investigations and open source intelligence gathering. At Authentic8, Nick provides training to analysts as they enhance their anonymous online investigation capabilities.

Rishi Kant is the Chief Product Officer for Authentic8, where he leads the product management, product marketing and UX teams. Prior to joining Authentic8, he led multiple products at Tanium and business strategy engagements at McKinsey. Rishi has a PhD in Engineering from Stanford, and BS/MS degrees in EE/CS from UC Berkeley.

silo
By Authentic8

QUICK GUIDE

Research Tools for Financial Crime and Fraud Investigations

The key to financial crime investigations is to "follow the money". To successfully uncover fraud and expose unlawful activity, analysts need access to accurate data, real-time intel, and precision tools tailored to their investigations. Authentic8 financial crime investigators and AML experts compiled a curated collection of resources that every financial crime and fraud analyst should have in their toolbox. We grouped these resources into three categories:

1. DATABASES: Every investigation begins with the facts, the data. Having a list of go-to resources at your fingertips saves time.
2. TOOLS: Data is great, but analysts need to go deeper, and they need the right tools for the job.
3. INTEL: Whether it's intel on a person of interest or a company, sites in this category can provide you with the latest information.

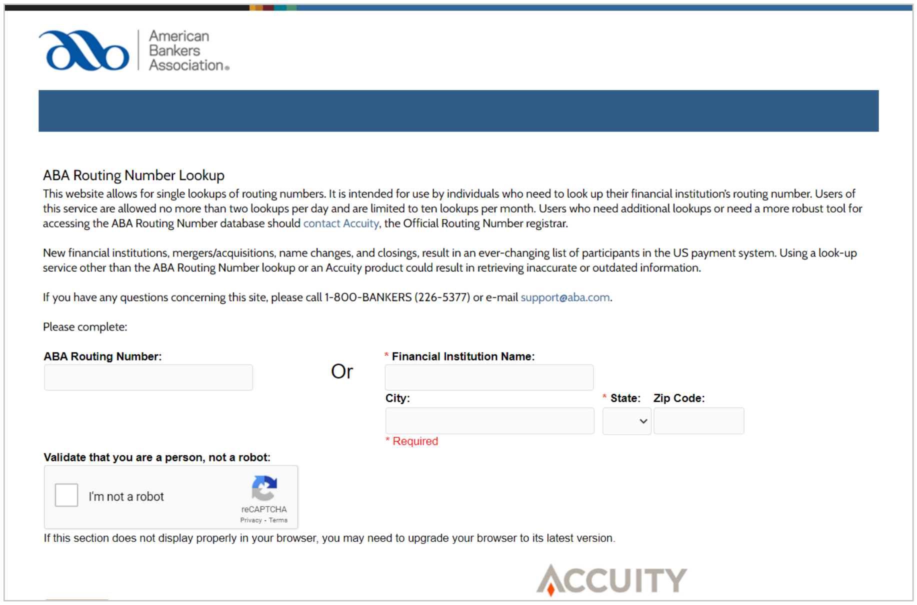
CATEGORY	NAME	LINK
DATABASES	American Banking Association (ABA) Routing Number Lookup	https://routingnumber.aba.com/Default1.aspx
	AML Toolbox	https://start.me/p/rxeRqr/aml-toolbox?embed=1
	BankFind Portal	https://research2.fdic.gov/bankfind/
	BIN Codes	https://www.bincodes.com/bin-checker/
	HS Code Lookup & Finder	https://www.freightos.com/freight-resources/harmonized-system-code-finder-hs-code-lookup/
	IRS Tax Exempt Organization Search	https://apps.irs.gov/app/eos/
	U.S. Securities and Exchange Commission EDGAR Search	https://www.sec.gov/edgar/searchedgar/companysearch.html
TOOLS	dnstwister	https://dnstwister.report/
	Dark.fail	https://dark.fail
	Have i been pwnd	https://haveibeenpwned.com/
	PhishTank	https://phishtank.com
	Social Bearing	https://socialbearing.com/
	Social Searcher	https://www.social-searcher.com/

CATEGORY	NAME	LINK
INTEL	Bitcoin Who's Who	https://bitcoinwhoswho.com/
	Foreign Assets Registration Act Quick Search	https://efile.fara.gov/ords/f?p=185:1:0::::P1_DISPLAY
	FTC Scam Alerts	https://www.consumer.ftc.gov/features/scam-alerts
	List-Org	https://www.list-org.com/
	LobbyView	https://www.lobbyview.org/query#!/
	OpenCorporates	https://opencorporates.com/
	Ripoff Report	https://www.ripoffreport.com/
	SWIFT BIC Search	https://www2.swift.com/bsl/
	ThisNumber	https://www.thisnumber.com/
	TweetDeck	https://tweetdeck.twitter.com/

DATABASES

American Banking Association (ABA) Routing Number Lookup

https://routingnumber.aba.com/Default1.aspx



ABA Routing Number Lookup

This website allows for single lookups of routing numbers. It is intended for use by individuals who need to look up their financial institution's routing number. Users of this service are allowed no more than two lookups per day and are limited to ten lookups per month. Users who need additional lookups or need a more robust tool for accessing the ABA Routing Number database should contact Accuity, the Official Routing Number registrar.

New financial institutions, mergers/acquisitions, name changes, and closings, result in an ever-changing list of participants in the US payment system. Using a look-up service other than the ABA Routing Number lookup or an Accuity product could result in retrieving inaccurate or outdated information.

If you have any questions concerning this site, please call 1-800-BANKERS (226-5377) or e-mail support@aba.com.

Please complete:

ABA Routing Number:

Or

* Financial Institution Name:

City:

* State:

Zip Code:

* Required

Validate that you are a person, not a robot:

□ I'm not a robot

If this section does not display properly in your browser, you may need to upgrade your browser to its latest version.

What It Is

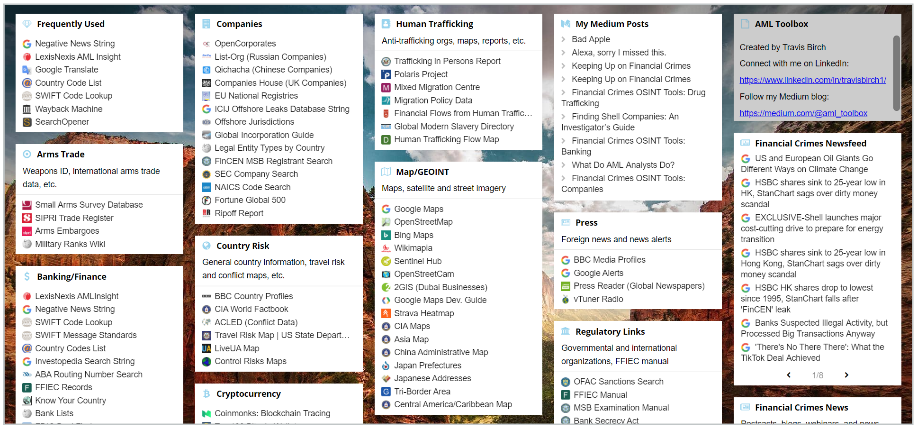
Establishing new financial institutions, mergers/acquisitions, name changes, and closings, result in an ever-changing list of participants in the U.S. payment system. The ABA website allows for accurate lookups of routing numbers.

Use Case

Researchers can use this service to retrieve accurate and up-to-date information on financial institutions.

AML Toolbox

https://start.me/p/rxeRqr/aml-toolbox?embed=1



Frequently Used
- Negative News String
- LexisNexis AML Insight
- Google Translate
- Country Code List
- SWIFT Code Lookup
- Wayback Machine
- SearchOpener

Arms Trade

Weapons ID, international arms trade data, etc.

- Small Arms Survey Database
- SIPRI Trade Register
- Arms Embargoes
- Military Ranks Wiki

Banking/Finance
- LexisNexis AMLInsight
- Negative News String
- SWIFT Code Lookup
- SWIFT Message Standards
- Country Codes List
- Investopedia Search String
- ABA Routing Number Search
- FFIEC Records
- Know Your Country
- Bank Lists

Companies
- OpenCorporates
- List-Org (Russian Companies)
- Qichacha (Chinese Companies)
- Companies House (UK Companies)
- EU National Registries
- ICIJ Offshore Leaks Database String
- Offshore Jurisdictions
- Global Incorporation Guide
- Legal Entity Types by Country
- FinCEN MSB Registrant Search
- SEC Company Search
- NAICS Code Search
- Fortune Global 500
- Ripoff Report

Country Risk

General country information, travel risk and conflict maps, etc.

- BBC Country Profiles
- CIA World Factbook
- ACLED (Conflict Data)
- Travel Risk Map | US State Depart…
- LiveUA Map
- Control Risks Maps

Cryptocurrency
- Coinmonks: Blockchain Tracing

Human Trafficking

Anti-trafficking orgs, maps, reports, etc.

- Trafficking in Persons Report
- Polaris Project
- Mixed Migration Centre
- Migration Policy Data
- Financial Flows from Human Traffic…
- Global Modern Slavery Directory
- Human Trafficking Flow Map

Map/GEOINT

Maps, satellite and street imagery

- Google Maps
- OpenStreetMap
- Bing Maps
- Wikimapia
- Sentinel Hub
- OpenStreetCam
- 2GIS (Dubai Businesses)
- Google Maps Dev. Guide
- Strava Heatmap
- CIA Maps
- Asia Map
- China Administrative Map
- Japan Prefectures
- Japanese Addresses
- Tri-Border Area
- Central America/Caribbean Map

My Medium Posts
- Bad Apple
- Alexa, sorry I missed this.
- Keeping Up on Financial Crimes
- Keeping Up on Financial Crimes
- Financial Crimes OSINT Tools: Drug Trafficking
- Finding Shell Companies: An Investigator's Guide
- Financial Crimes OSINT Tools: Banking
- What Do AML Analysts Do?
- Financial Crimes OSINT Tools: Companies

Press

Foreign news and news alerts

- BBC Media Profiles
- Google Alerts
- Press Reader (Global Newspapers)
- vTuner Radio

Regulatory Links

Governmental and international organizations, FFIEC manual

- OFAC Sanctions Search
- FFIEC Manual
- MSB Examination Manual
- Bank Secrecy Act

AML Toolbox

Created by Travis Birch

Connect with me on LinkedIn:

https://www.linkedin.com/in/travisbirch1/

Follow my Medium blog:

https://medium.com/@aml_toolbox

Financial Crimes Newsfeed
- US and European Oil Giants Go Different Ways on Climate Change
- HSBC shares sink to 25-year low in HK, StanChart sags over dirty money scandal
- EXCLUSIVE-Shell launches major cost-cutting drive to prepare for energy transition
- HSBC shares sink to 25-year low in Hong Kong, StanChart sags over dirty money scandal
- HSBC HK shares drop to lowest since 1995, StanChart falls after 'FinCEN' leak
- Banks Suspected Illegal Activity, but Processed Big Transactions Anyway
- 'There's No There There': What the TikTok Deal Achieved

Financial Crimes News

Podcasts, blogs, webinars, and news

What It Is

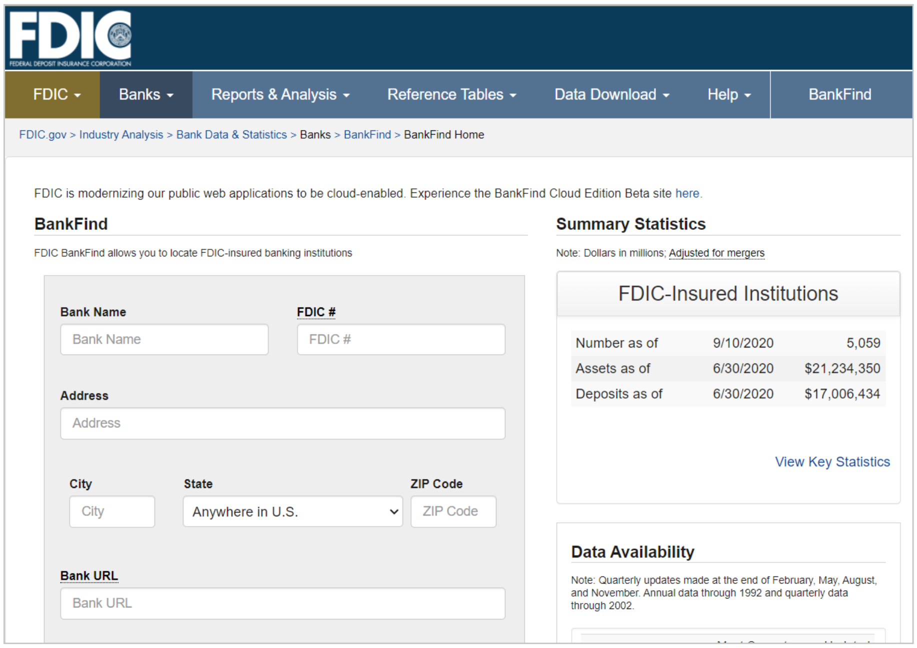
An extensive collection of websites, tools, research papers, regulatory links, datasets, and news sources designed specifically for anti-money laundering investigators and OSINT researchers.

Use Case

When following the money trail, researchers can take advantage of many available resources, along with specialized regulatory, industry and geopolitical information.

BankFind Portal

https://research2.fdic.gov/bankfind/



FDIC.gov > Industry Analysis > Bank Data & Statistics > Banks > BankFind > BankFind Home

FDIC is modernizing our public web applications to be cloud-enabled. Experience the BankFind Cloud Edition Beta site here.

BankFind

FDIC BankFind allows you to locate FDIC-insured banking institutions

Bank Name: Bank Name

FDIC #: FDIC #

Address: Address

City: City

State: Anywhere in U.S.

ZIP Code: ZIP Code

Bank URL: Bank URL

Summary Statistics

Note: Dollars in millions; Adjusted for mergers

FDIC-Insured Institutions

Number as of	9/10/2020	5,059
Assets as of	6/30/2020	$21,234,350
Deposits as of	6/30/2020	$17,006,434

Data Availability

Note: Quarterly updates made at the end of February, May, August, and November. Annual data through 1992 and quarterly data through 2002.

What It Is

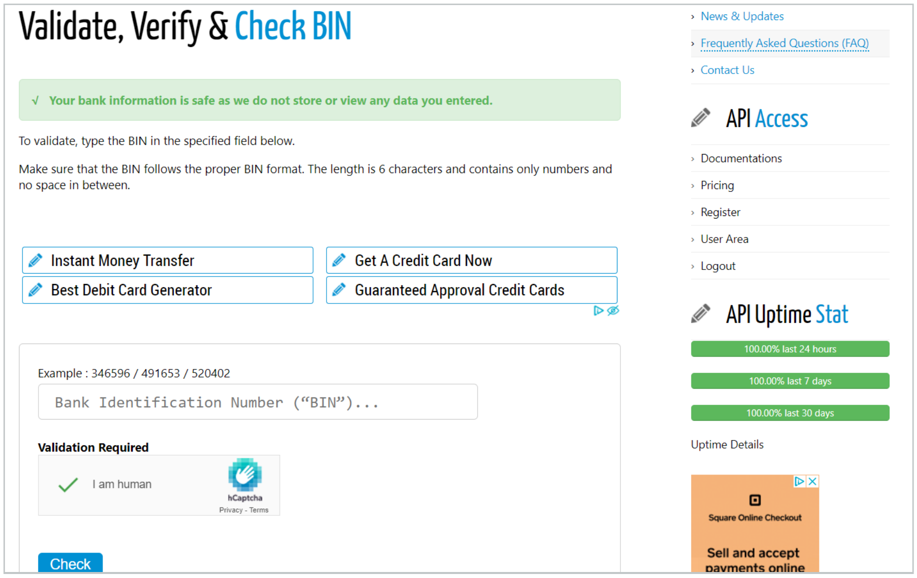
The Federal Deposit Insurance Corporation (FDIC) hosts a BankFind portal to help locate specific information on FDIC-insured banking institutions.

Use Case

Researchers can use advanced search criteria to find a bank or holding company, generate comprehensive financial or demographic reports, and find bank locations or groups of banks.

BIN Codes

https://www.bincodes.com/bin-checker/



Validate, Verify & Check BIN

√ Your bank information is safe as we do not store or view any data you entered.

To validate, type the BIN in the specified field below.

Make sure that the BIN follows the proper BIN format. The length is 6 characters and contains only numbers and no space in between.

Instant Money Transfer | Get A Credit Card Now
Best Debit Card Generator | Guaranteed Approval Credit Cards

Example : 346596 / 491653 / 520402

Bank Identification Number ("BIN")...

Validation Required

I am human

hCaptcha
Privacy - Terms

Check

› News & Updates
› Frequently Asked Questions (FAQ)
› Contact Us

API Access

› Documentations
› Pricing
› Register
› User Area
› Logout

API Uptime Stat

100.00% last 24 hours
100.00% last 7 days
100.00% last 30 days

Uptime Details

Square Online Checkout
Sell and accept payments online

What It Is

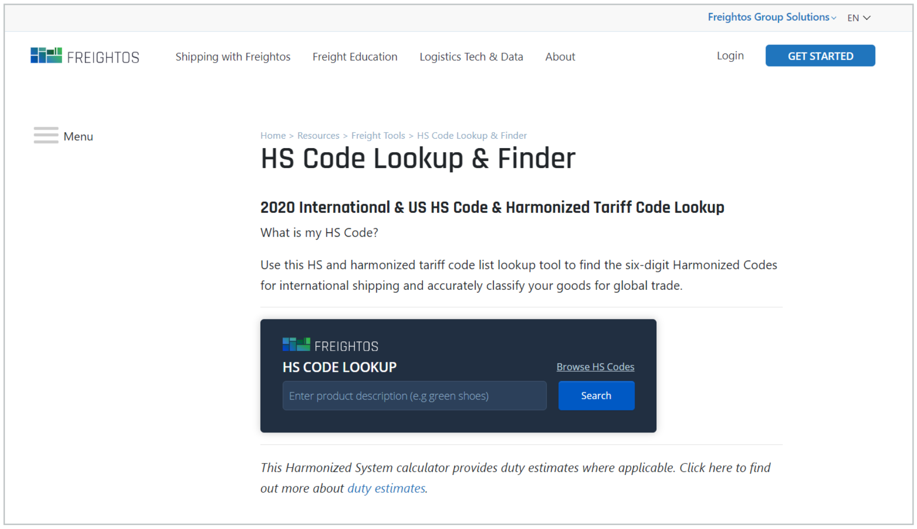
This website provides limited free BIN and credit card validation tools. Bank Identification Number ("BIN") or Issuer Identification Number ("IIN") is the first six digits of a bank card number or payment card number, and is commonly used in credit cards and debit cards, stored-value cards, gift cards, and other similar cards.

Use Case

BIN is beneficial to identify a card brand, issuing institution or bank, country of issuance, card type and category of cards. This information is useful for fraud prevention, especially for online stores.

HS Code Lookup & Finder

https://www.freightos.com/freight-resources/harmonized-system-code-finder-hs-code-lookup/



Home > Resources > Freight Tools > HS Code Lookup & Finder

HS Code Lookup & Finder

2020 International & US HS Code & Harmonized Tariff Code Lookup

What is my HS Code?

Use this HS and harmonized tariff code list lookup tool to find the six-digit Harmonized Codes for international shipping and accurately classify your goods for global trade.

FREIGHTOS
HS CODE LOOKUP
Browse HS Codes
Enter product description (e.g green shoes)
Search

This Harmonized System calculator provides duty estimates where applicable. Click here to find out more about duty estimates.

What It Is

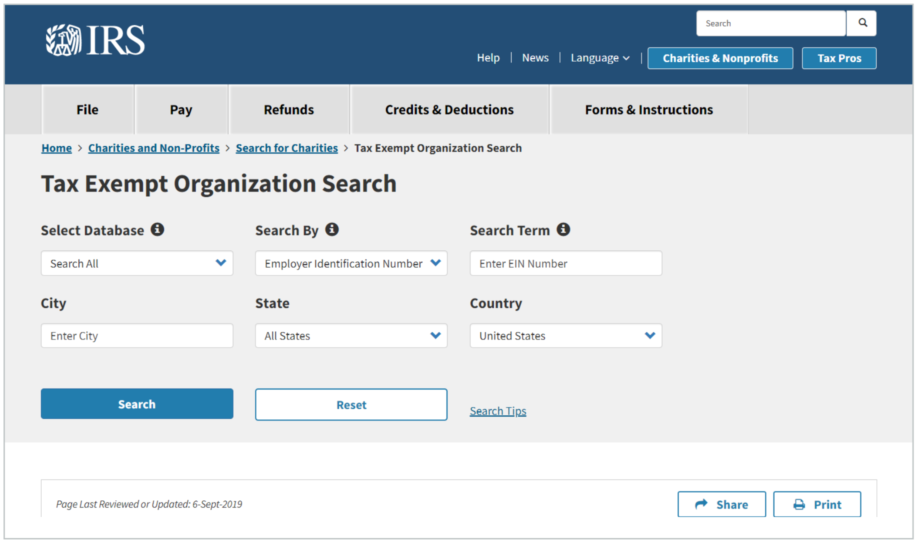
HS Codes, also known as the Harmonized Commodity Description and Coding System, are a standardized international system to classify globally traded products. The system is maintained by the World Customs Organization and is used to ease global trade by creating unified categories to classify different types of goods.

Use Case

Use the HS and harmonized tariff code list lookup tool to find the six-digit Harmonized Codes for international shipping and accurately classify goods for global trade.

IRS Tax Exempt Organization Search

https://apps.irs.gov/app/eos/



Tax Exempt Organization Search

Select Database: Search All

Search By: Employer Identification Number

Search Term: Enter EIN Number

City: Enter City

State: All States

Country: United States

Page Last Reviewed or Updated: 6-Sept-2019

What It Is

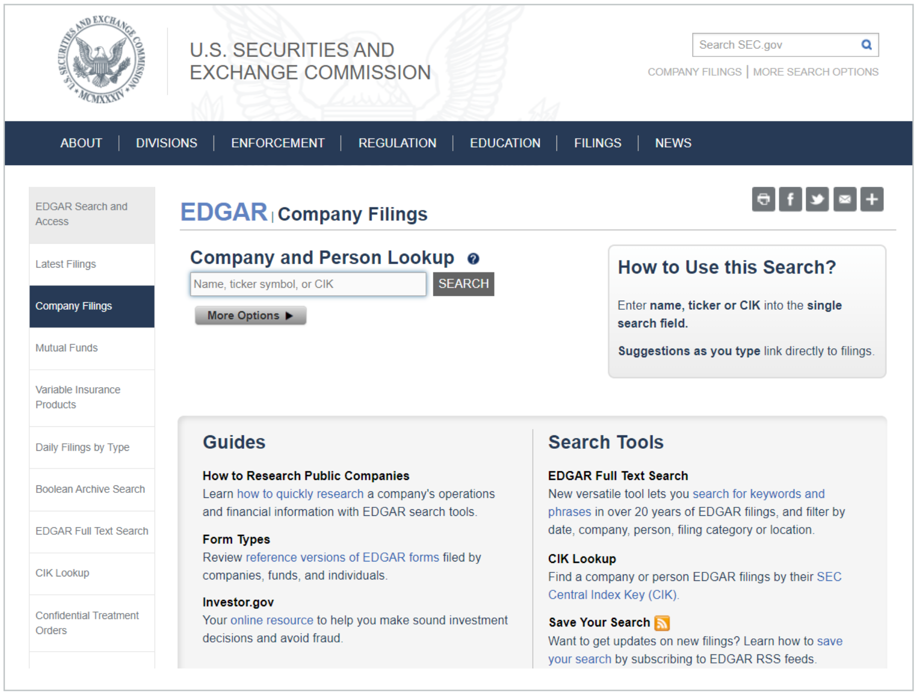
Tax Exempt Organization Search provides access to IRS information about tax-exempt organizations.

Use Case

Locate any tax-exempt organization by name, Employer ID number, category, or location.

U.S. Securities and Exchange Commission EDGAR Search

https://www.sec.gov/edgar/searchedgar/companysearch.html



EDGAR | Company Filings

Company and Person Lookup

Name, ticker symbol, or CIK

How to Use this Search?

Enter **name, ticker or CIK** into the **single search field.**

Suggestions as you type link directly to filings.

Guides

How to Research Public Companies
Learn how to quickly research a company's operations and financial information with EDGAR search tools.

Form Types
Review reference versions of EDGAR forms filed by companies, funds, and individuals.

Investor.gov
Your online resource to help you make sound investment decisions and avoid fraud.

Search Tools

EDGAR Full Text Search
New versatile tool lets you search for keywords and phrases in over 20 years of EDGAR filings, and filter by date, company, person, filing category or location.

CIK Lookup
Find a company or person EDGAR filings by their SEC Central Index Key (CIK).

Save Your Search
Want to get updates on new filings? Learn how to save your search by subscribing to EDGAR RSS feeds.

What It Is

The U.S. Securities and Exchange Commission EDGAR Search allows researchers to search for company filings.

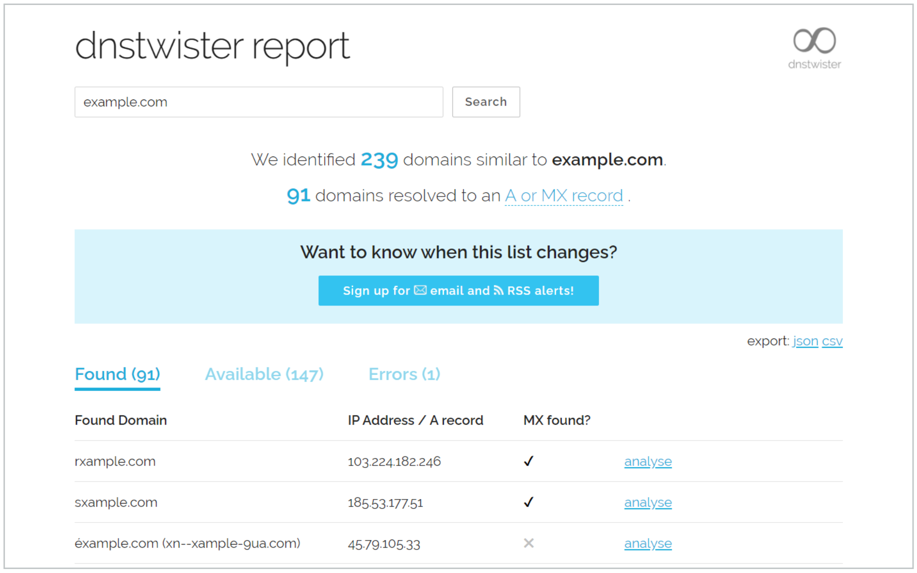
Use Case

Analysts can find specific information on shell companies, including their financial information and operations, using the corporations' SEC filings.

TOOLS

dnstwister

https://dnstwister.report/



dnstwister report

We identified 239 domains similar to **example.com**.

91 domains resolved to an A or MX record .

Want to know when this list changes?

Found Domain	IP Address / A record	MX found?	
rxample.com	103.224.182.246	✓	analyse
sxample.com	185.53.177.51	✓	analyse
éxample.com (xn--xample-gua.com)	45.79.105.33	×	analyse

What It Is

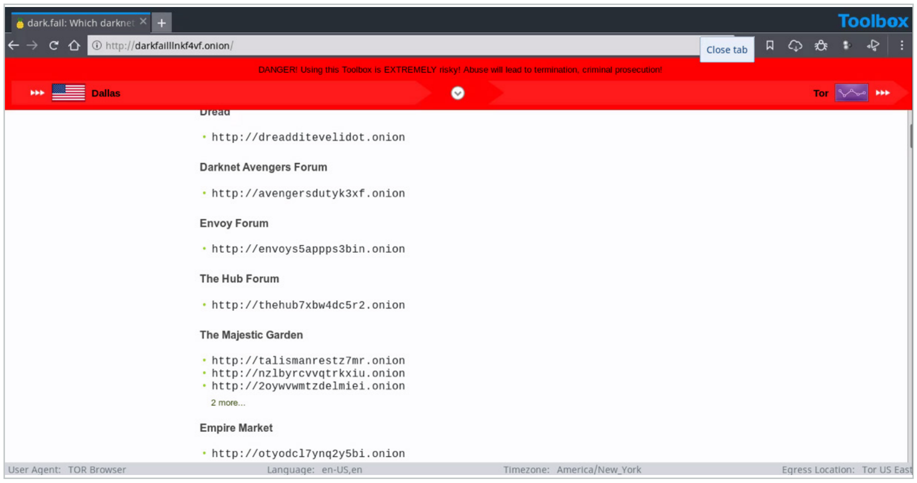
dnstwister generates a list of domain names that are similar to one provided by the user, checking to see if any of them are registered.

Use Case

dnstwister can tell researchers if someone may be using a domain similar to theirs for malicious purposes, such as phishing or trademark infringement.

Dark.fail

https://dark.fail/



DANGER! Using this Toolbox is EXTREMELY risky! Abuse will lead to termination, criminal prosecution!

Dread

- http://dreadditevelidot.onion

Darknet Avengers Forum

- http://avengersdutyk3xf.onion

Envoy Forum

- http://envoys5appps3bin.onion

The Hub Forum

- http://thehub7xbw4dc5r2.onion

The Majestic Garden

- http://talismanrestz7mr.onion
- http://nzlbyrcvvqtrkxiu.onion
- http://2oywvwmtzdelmiei.onion

2 more...

Empire Market

- http://otyodcl7ynq2y5bi.onion

User Agent: TOR Browser Language: en-US,en Timezone: America/New_York Egress Location: Tor US East

What It Is

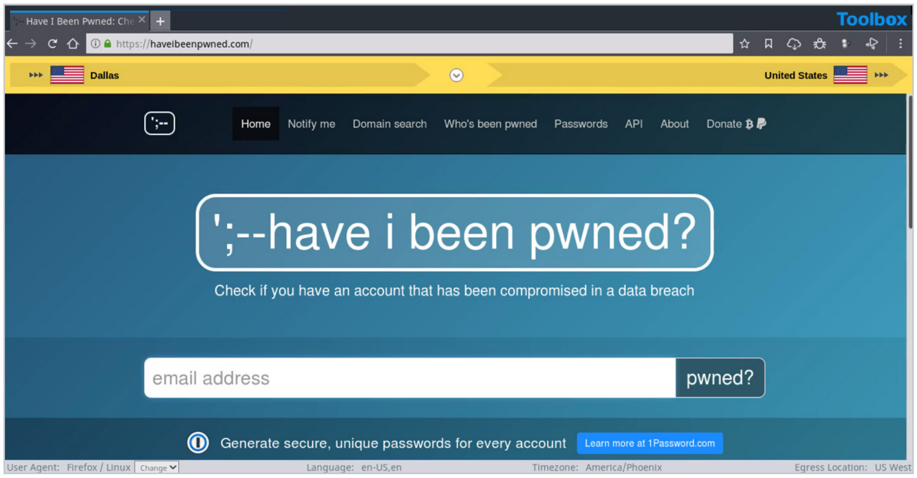
Dark.fail indexes every major darknet site and keeps track of all domains linked to a particular hidden service.

Use Case

Tor admins rely on Dark.fail to disseminate links in the wake of takedowns of sites like DeepDotWeb. Researchers can use Dark.fail when exploring sites that correlate with the hidden service.

Have i been pwnd

https://haveibeenpwned.com/



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Generate secure, unique passwords for every account

User Agent: Firefox / Linux Language: en-US,en Timezone: America/Phoenix Egress Location: US West

What It Is

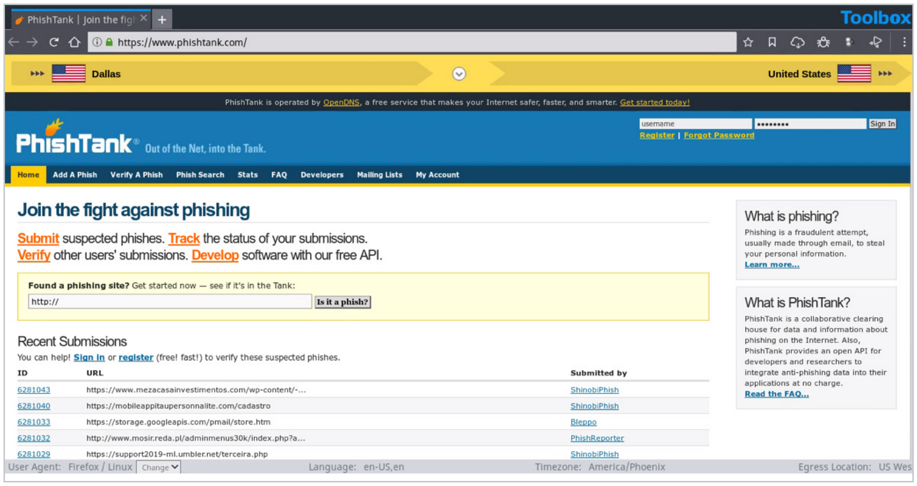
This service exposes the severity of the risks of online attacks, while helping victims of data breaches learn about compromises of their accounts. Users can subscribe to receive breach notifications, and search for pwned accounts and passwords across domains.

Use Case

Users can securely enter email addresses and passwords to find out if they exist across a multitude of exposed data breaches. The site returns a complete list of breaches where specific accounts have been exposed, and identifies what types of data (email addresses, names, passwords, locations, etc.) has been stolen.

PhishTank

https://phishtank.com



PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
6281043	https://www.mezacasainvestimentos.com/wp-content/-...	ShinobiPhish
6281040	https://mobileappitaupersonnalite.com/cadastro	ShinobiPhish
6281033	https://storage.googleapis.com/pmail/store.htm	Bleppo
6281032	http://www.mosir.reda.pl/adminmenus30k/index.php?a...	PhishReporter
6281029	https://support2019-ml.umbler.net/terceira.php	ShinobiPhish

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. Learn more...

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge. Read the FAQ...

User Agent: Firefox / Linux Language: en-US,en Timezone: America/Phoenix Egress Location: US Wes

What It Is

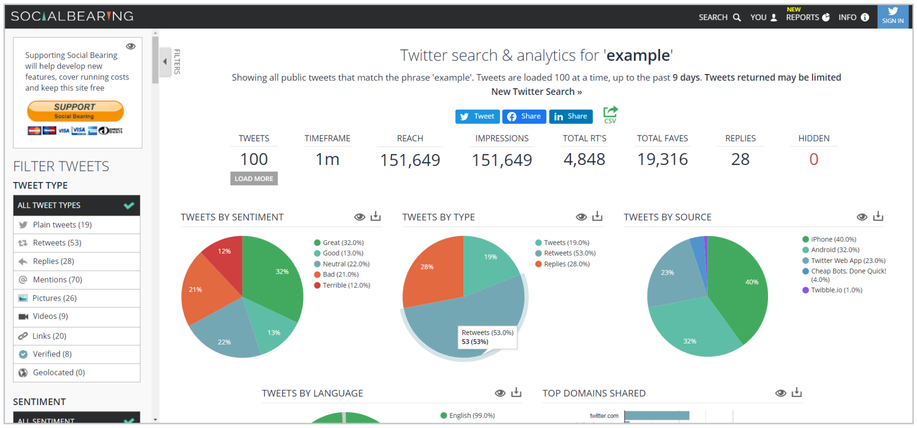
PhishTank is a free community site where anyone can submit, verify, track and share phishing data. PhishTank also provides an open API for developers and researchers to integrate anti-phishing data into their applications.

Use Case

Users submit suspicious URLs via email, and PhishTank identifies, verifies, tracks, confirms, and publishes phishing sites on its web page.

Social Bearing

https://socialbearing.com/



Supporting Social Bearing will help develop new features, cover running costs and keep this site free

FILTER TWEETS

TWEET TYPE

- ALL TWEET TYPES ✓
- Plain tweets (19)
- Retweets (53)
- Replies (28)
- Mentions (70)
- Pictures (26)
- Videos (9)
- Links (20)
- Verified (8)
- Geolocated (0)

Twitter search & analytics for '**example**'

Showing all public tweets that match the phrase 'example'. Tweets are loaded 100 at a time, up to the past **9 days. Tweets returned may be limited**

New Twitter Search »

TWEETS	TIMEFRAME	REACH	IMPRESSIONS	TOTAL RT'S	TOTAL FAVES	REPLIES	HIDDEN
100	1m	151,649	151,649	4,848	19,316	28	0

What It Is

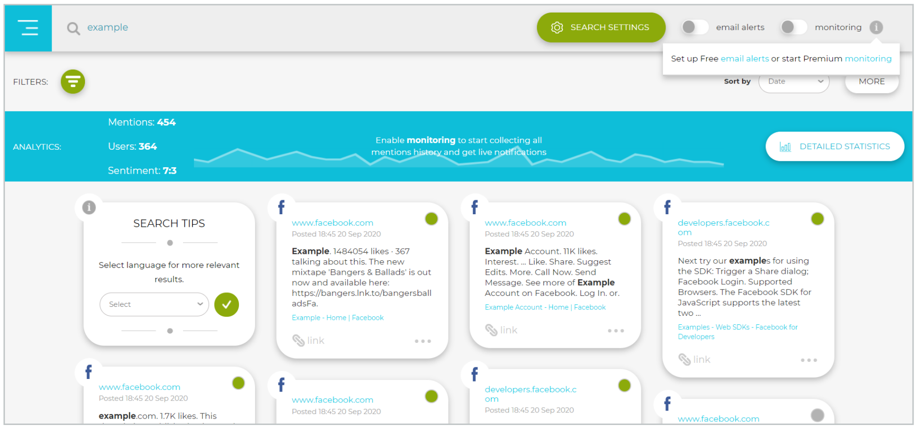
Free Twitter analytics & search for tweets, timelines, and Twitter maps.

Use Case

Allows researchers to find, filter and sort tweets or people by engagement, influence, location, sentiment and more.

Social Searcher

https://www.social-searcher.com/



Set up Free email alerts or start Premium monitoring

Mentions: **454**

Users: **364**

Sentiment: **7:3**

Enable **monitoring** to start collecting all mentions history and get live notifications

Select language for more relevant results.

www.facebook.com
Posted 18:45 20 Sep 2020

Example. 1484054 likes · 367 talking about this. The new mixtape 'Bangers & Ballads' is out now and available here: https://bangers.lnk.to/bangersballadsFa.

Example - Home | Facebook

www.facebook.com
Posted 18:45 20 Sep 2020

Example Account. 11K likes. Interest. ... Like. Share. Suggest Edits. More. Call Now. Send Message. See more of **Example** Account on Facebook. Log In. or.

Example Account - Home | Facebook

developers.facebook.com
Posted 18:45 20 Sep 2020

Next try our **example**s for using the SDK: Trigger a Share dialog; Facebook Login. Supported Browsers. The Facebook SDK for JavaScript supports the latest two ...

Examples - Web SDKs - Facebook for Developers

www.facebook.com
Posted 18:45 20 Sep 2020

example.com. 1.7K likes. This

www.facebook.com
Posted 18:45 20 Sep 2020

developers.facebook.com
Posted 18:45 20 Sep 2020

www.facebook.com

What It Is

A search engine that allows analysts to monitor all public social mentions in social networks and web.

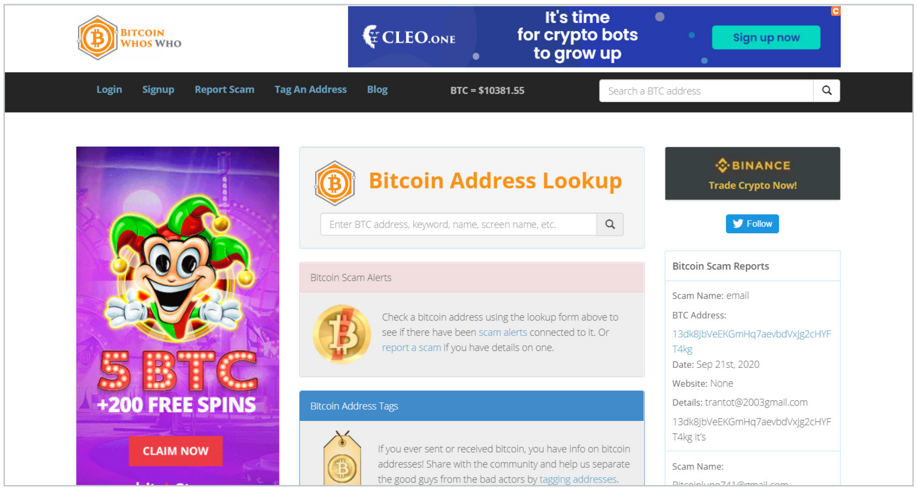
Use Case

Analysts use it to quickly measure and track what people are saying about a particular company, brand, product, or service. Users can get visibility into audience behavior triggers, explore popular hashtags, and identify the most popular users and influencers of a product or service.

INTEL

Bitcoin Who's Who

https://bitcoinwhoswho.com/



Bitcoin Address Lookup

Enter BTC address, keyword, name, screen name, etc.

Bitcoin Scam Alerts

Check a bitcoin address using the lookup form above to see if there have been scam alerts connected to it. Or report a scam if you have details on one.

Bitcoin Address Tags

If you ever sent or received bitcoin, you have info on bitcoin addresses! Share with the community and help us separate the good guys from the bad actors by tagging addresses.

Bitcoin Scam Reports

Scam Name: email

BTC Address: 13dk8JbVeEKGmHq7aevbdVxjg2cHYFT4kg

Date: Sep 21st, 2020

Website: None

Details: trantot@2003gmail.com 13dk8JbVeEKGmHq7aevbdVxjg2cHYFT4kg it's

Scam Name:

What It Is

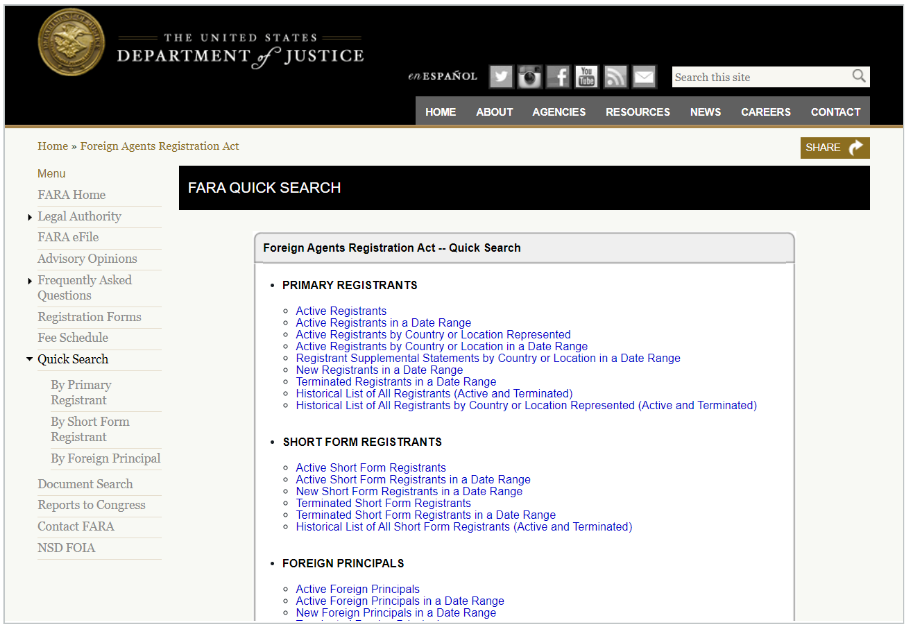
Bitcoin Who's Who profiles the members of the bitcoin ecosystem to help users verify a bitcoin address owner and avoid a bitcoin scam or fraud.

Use Case

With Bitcoin Who's Who, researchers can discover new connections and previously unknown associations on the bitcoin blockchain.

Foreign Assets Registration Act Quick Search

https://efile.fara.gov/ords/f?p=185:1:0::::P1_DISPLAY



FARA QUICK SEARCH

Foreign Agents Registration Act -- Quick Search

- PRIMARY REGISTRANTS
  - Active Registrants
  - Active Registrants in a Date Range
  - Active Registrants by Country or Location Represented
  - Active Registrants by Country or Location in a Date Range
  - Registrant Supplemental Statements by Country or Location in a Date Range
  - New Registrants in a Date Range
  - Terminated Registrants in a Date Range
  - Historical List of All Registrants (Active and Terminated)
  - Historical List of All Registrants by Country or Location Represented (Active and Terminated)
- SHORT FORM REGISTRANTS
  - Active Short Form Registrants
  - Active Short Form Registrants in a Date Range
  - New Short Form Registrants in a Date Range
  - Terminated Short Form Registrants
  - Terminated Short Form Registrants in a Date Range
  - Historical List of All Short Form Registrants (Active and Terminated)
- FOREIGN PRINCIPALS
  - Active Foreign Principals
  - Active Foreign Principals in a Date Range
  - New Foreign Principals in a Date Range

What It Is

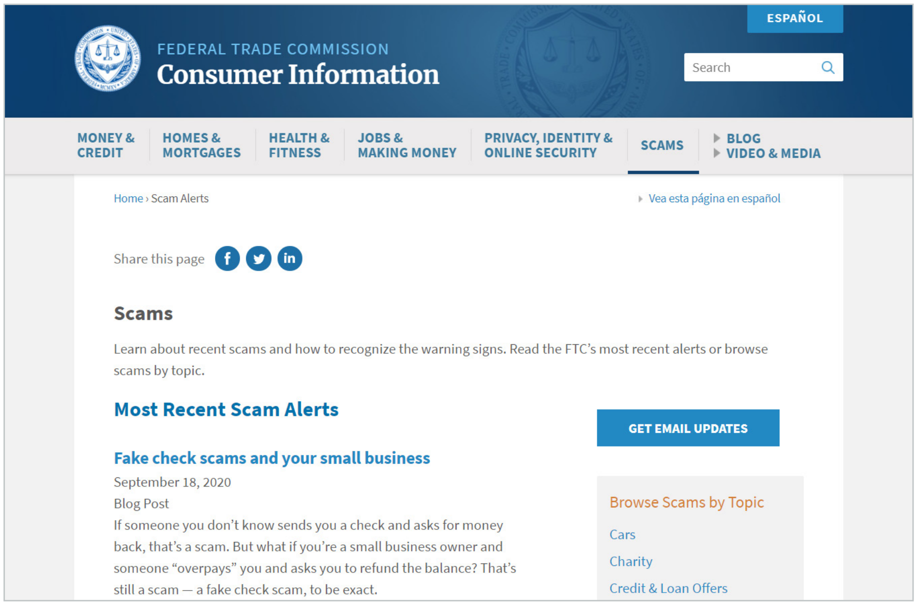
The Foreign Agents Registration Act (FARA) requires certain agents of foreign principals who are engaged in political activities or other activities specified under the statute to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities. The FARA quick search engine provides 21 distinct search portals for enhanced due diligence on primary registrants, short form registrants and foreign principles.

Use Case

Analysts can use FARA to find supplemental documents entailing a company's foreign relations, in the context of their engagement in political or other activities covered by the act.

FTC Scam Alerts

https://www.consumer.ftc.gov/features/scam-alerts



Scams

Learn about recent scams and how to recognize the warning signs. Read the FTC's most recent alerts or browse scams by topic.

Most Recent Scam Alerts

Fake check scams and your small business

September 18, 2020

Blog Post

If someone you don't know sends you a check and asks for money back, that's a scam. But what if you're a small business owner and someone "overpays" you and asks you to refund the balance? That's still a scam — a fake check scam, to be exact.

What It Is

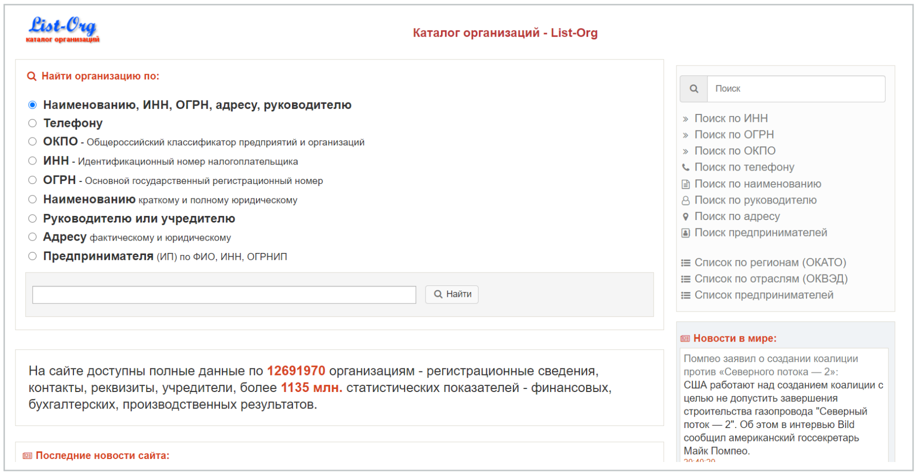
Federal Trade Commission's scam alert feed provides information on the latest scams and how to recognize the warning signs.

Use Case

Researchers can benefit from information on the latest trends in scamming/fraud and tips on how to recognize and avoid them.

List-Org

https://www.list-org.com/



Найти организацию по:

- ● Наименованию, ИНН, ОГРН, адресу, руководителю
- ○ Телефону
- ○ ОКПО - Общероссийский классификатор предприятий и организаций
- ○ ИНН - Идентификационный номер налогоплательщика
- ○ ОГРН - Основной государственный регистрационный номер
- ○ Наименованию краткому и полному юридическому
- ○ Руководителю или учредителю
- ○ Адресу фактическому и юридическому
- ○ Предпринимателя (ИП) по ФИО, ИНН, ОГРНИП

На сайте доступны полные данные по **12691970** организациям - регистрационные сведения, контакты, реквизиты, учредители, более **1135 млн.** статистических показателей - финансовых, бухгалтерских, производственных результатов.

Последние новости сайта:

Новости в мире:

Помпео заявил о создании коалиции против «Северного потока — 2»:
США работают над созданием коалиции с целью не допустить завершения строительства газопровода "Северный поток — 2". Об этом в интервью Bild сообщил американский госсекретарь Майк Помпео.

What It Is

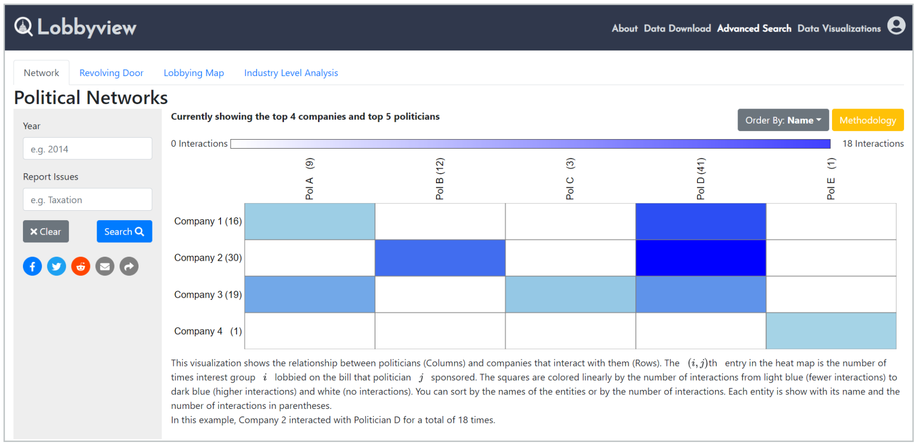
The List-Org site contains complete data on more than 12 million organization, with more than 980 unique financial data points. The site itself and all search results are in Russian, but could be translated using Google's translate function.

Use Case

Researchers can search Russian companies for information on registration, contacts, financials, and founders.

LobbyView

https://www.lobbyview.org/query#!/



Political Networks

Currently showing the top 4 companies and top 5 politicians

This visualization shows the relationship between politicians (Columns) and companies that interact with them (Rows). The (i, j)th entry in the heat map is the number of times interest group i lobbied on the bill that politician j sponsored. The squares are colored linearly by the number of interactions from light blue (fewer interactions) to dark blue (higher interactions) and white (no interactions). You can sort by the names of the entities or by the number of interactions. Each entity is show with its name and the number of interactions in parentheses.

In this example, Company 2 interacted with Politician D for a total of 18 times.

What It Is

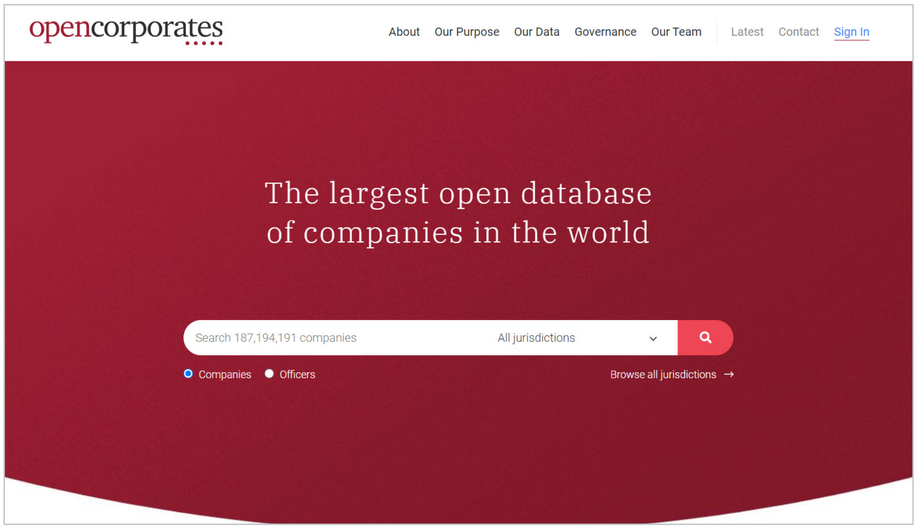
LobbyView is a database for researchers to conduct systematic data analysis on over 1 million lobbying issues and congressional bills.

Use Case

The reports unearth data and hidden connections between interest groups, government agencies, politicians, firms and lobbyists.

OpenCorporates

https://opencorporates.com/



The largest open database of companies in the world

What It Is

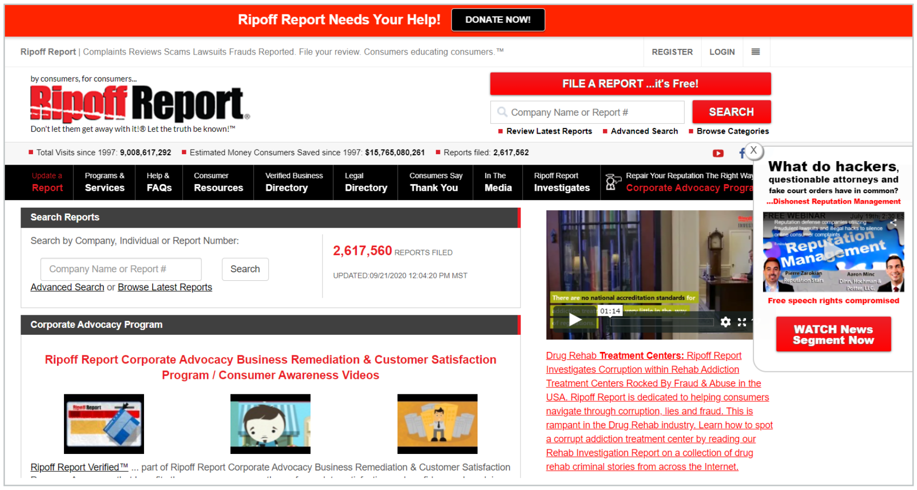
OpenCorporates hosts the largest open database of companies in the world, dedicated to making high-quality, official company data openly available. Data that can be trusted, accessed, and analyzed when and how it's needed.

Use Case

Researchers can analyze data from the complex networks that form banks and financial companies, used for money laundering, organized crime and corruption.

Ripoff Report

https://www.ripoffreport.com/



Ripoff Report Needs Your Help!

Ripoff Report | Complaints Reviews Scams Lawsuits Frauds Reported. File your review. Consumers educating consumers.™

by consumers, for consumers...
Ripoff Report®
Don't let them get away with it!® Let the truth be known!™

Total Visits since 1997: **9,008,617,292** Estimated Money Consumers Saved since 1997: **$15,765,080,261** Reports filed: **2,617,562**

Search by Company, Individual or Report Number:

Advanced Search or Browse Latest Reports

2,617,560 REPORTS FILED

UPDATED:09/21/2020 12:04:20 PM MST

Ripoff Report Corporate Advocacy Business Remediation & Customer Satisfaction Program / Consumer Awareness Videos

Ripoff Report Verified™ ... part of Ripoff Report Corporate Advocacy Business Remediation & Customer Satisfaction

There are no national accreditation standards for

Drug Rehab **Treatment Centers:** Ripoff Report Investigates Corruption within Rehab Addiction Treatment Centers Rocked By Fraud & Abuse in the USA. Ripoff Report is dedicated to helping consumers navigate through corruption, lies and fraud. This is rampant in the Drug Rehab industry. Learn how to spot a corrupt addiction treatment center by reading our Rehab Investigation Report on a collection of drug rehab criminal stories from across the Internet.

What do hackers, questionable attorneys and fake court orders have in common?
...Dishonest Reputation Management

FREE WEBINAR July 19th, 2:30 ES
Reputation defense companies utilizing fraudulent lawsuits and illegal hacks to silence online consumer complaints
Reputation Management
Pierre Zarokian Reputation Stars
Aaron Minc Dinn, Hochman & Potter, LLC

Free speech rights compromised

What It Is

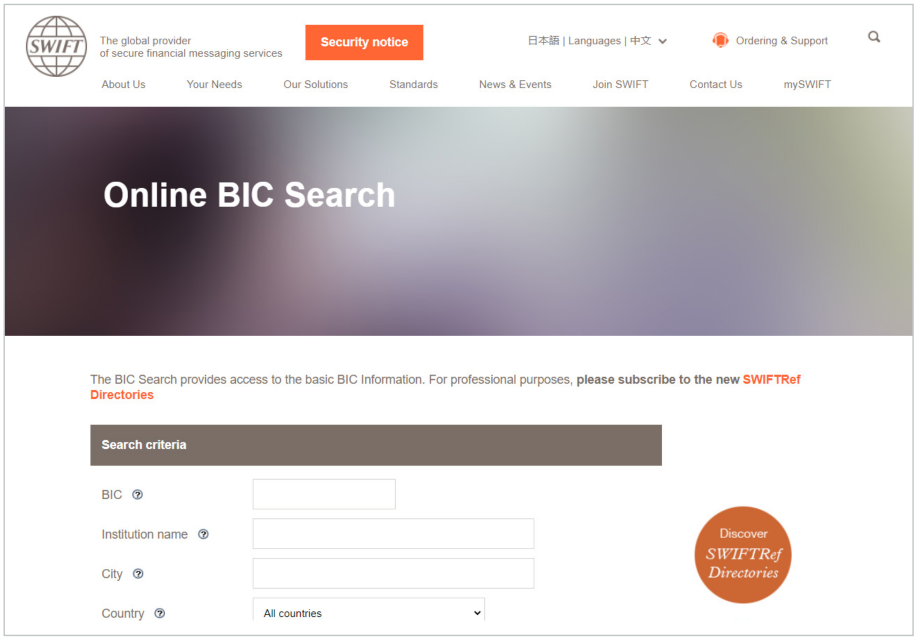
Ripoff Report is a worldwide consumer reporting web site and publication, by consumers, for consumers, to file and document complaints about companies or individuals.

Use Case

Enterprises and consumers are encouraged to search the Ripoff Report before they do business with any company to identify bad business practices, credit theft incidents, fraudulent employment and business opportunities, and individual con artists who scam consumers. Researchers can check the Ripoff Report to find complaints against specific companies and organizations.

SWIFT BIC Search

https://www2.swift.com/bsl/



The global provider of secure financial messaging services

The BIC Search provides access to the basic BIC Information. For professional purposes, **please subscribe to the new SWIFTRef Directories**

What It Is

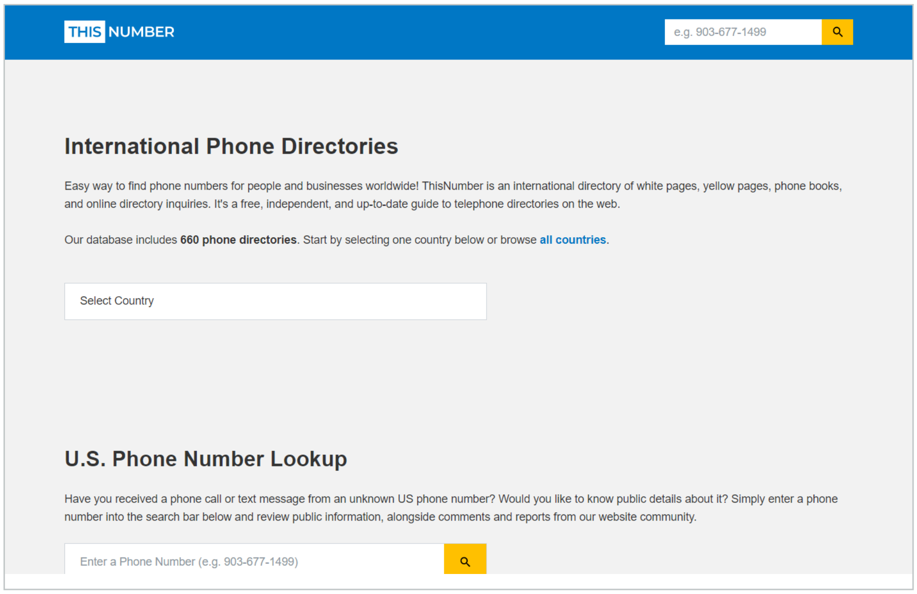
The BIC search portal provides access to basic information hosted within the SWIFT Bank Identifier Information (BIC) database.

Use Case

Researchers can find the information on both financial and non-financial institutions. The BIC is used in financial transactions, client and counterparty databases, compliance documents, and more.

ThisNumber

https://www.thisnumber.com/



International Phone Directories

Easy way to find phone numbers for people and businesses worldwide! ThisNumber is an international directory of white pages, yellow pages, phone books, and online directory inquiries. It's a free, independent, and up-to-date guide to telephone directories on the web.

Our database includes **660 phone directories**. Start by selecting one country below or browse **all countries**.

Select Country

U.S. Phone Number Lookup

Have you received a phone call or text message from an unknown US phone number? Would you like to know public details about it? Simply enter a phone number into the search bar below and review public information, alongside comments and reports from our website community.

Enter a Phone Number (e.g. 903-677-1499)

What It Is

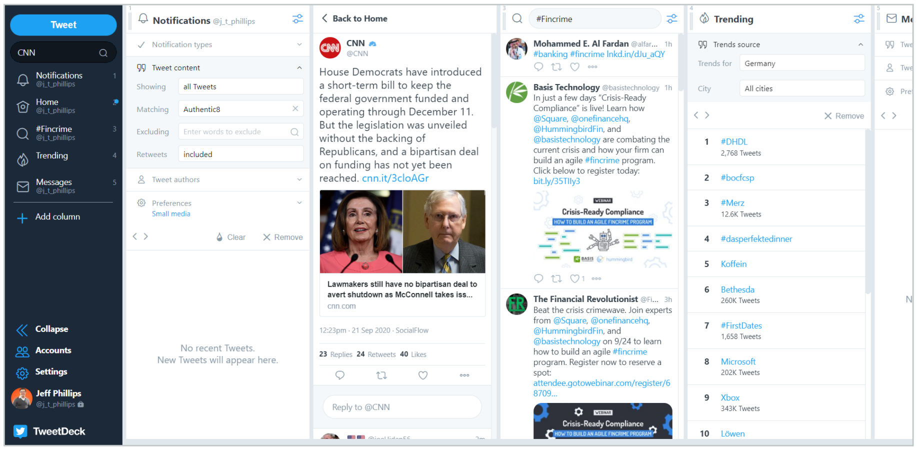
ThisNumber offers an easy way to find phone numbers for people and businesses around the world. The database currently contains 660 phone directories.

Use Case

Analysts can look up public details for any phone number – in the U.S. or internationally – alongside comments from the user community related to activity from this phone number.

TweetDeck

https://tweetdeck.twitter.com/



Showing: all Tweets
Matching: Authentic8
Excluding: Enter words to exclude
Retweets: included

No recent Tweets.
New Tweets will appear here.

CNN @CNN
House Democrats have introduced a short-term bill to keep the federal government funded and operating through December 11. But the legislation was unveiled without the backing of Republicans, and a bipartisan deal on funding has not yet been reached. cnn.it/3cloAGr

Lawmakers still have no bipartisan deal to avert shutdown as McConnell takes iss...
cnn.com

12:23pm · 21 Sep 2020 · SocialFlow
23 Replies 24 Retweets 40 Likes

Mohammed E. Al Fardan @alfar... 1h
#banking #fincrime lnkd.in/dJu_aQY

Basis Technology @basistechnology 1h
In just a few days "Crisis-Ready Compliance" is live! Learn how @Square, @onefinancehq, @HummingbirdFin, and @basistechnology are combating the current crisis and how your firm can build an agile #fincrime program. Click below to register today: bit.ly/35TIly3

WEBINAR Crisis-Ready Compliance HOW TO BUILD AN AGILE FINCRIME PROGRAM

The Financial Revolutionist @Fi... 3h
Beat the crisis crimewave. Join experts from @Square, @onefinancehq, @HummingbirdFin, and @basistechnology on 9/24 to learn how to build an agile #fincrime program. Register now to reserve a spot: attendee.gotowebinar.com/register/68709...

Trends for: Germany
City: All cities

1 #DHDL 2,768 Tweets
2 #bocfcsp
3 #Merz 12.6K Tweets
4 #dasperfektedinner
5 Koffein
6 Bethesda 260K Tweets
7 #FirstDates 1,658 Tweets
8 Microsoft 202K Tweets
9 Xbox 343K Tweets
10 Löwen

What It Is

A powerful Twitter tool for real-time tracking, organizing, and audience engagement.

Use Case

Analysts can set up an organized feed, tailored to the Twitter accounts they want to follow. For example, a feed of accounts that are suspected of being associated with a carding forum.

By Authentic8

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

© Authentic8, Inc. All rights reserved. 01082021

How Pastebin Can Help with Research

In this tutorial, we will show you how researchers can use information they find on Pastebin to locate hackers who are offering leaked data for sale.

What is Pastebin?

Pastebin.com is often compared to a clipboard—it's a place to paste anything, like plaintext documents, logs, source code, etc. for anyone to view. Pastebin is also an infamous repository of stolen databases, PoC exploit code, combo lists, doxing victims, and credit card numbers—all available for sale. Publishing information on Pastebin requires no login, and it's been popularized throughout the hacker community through the use of internet relay chat.

Pastebin does its best to remove sensitive information, but with millions of active pastes, moderating it is an overwhelming task. Pastebin is often the first stop researchers go to when they look for stolen information when leaks surface.

Using Pastebin to Hunt for Stolen Data

Sometimes hackers boast about the data they possess by uploading samples on Pastebin and then offering links to the full dumps. These links point to anywhere from Torrent sites, like The Pirate Bay, to a variety of darknet .onion marketplaces, where stolen data can be purchased.

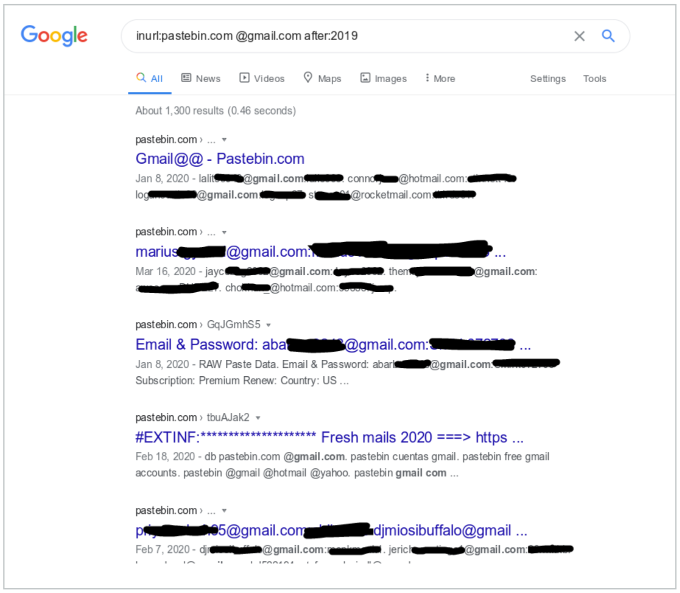
It's crucial that during this hunt, sessions remain unique and untied from normal browsing. This is because of the tracking that occurs on Google (when dorking for pastes) and on external sites (that researchers may be required to visit for full dumps) listed within the paste.

When we use Google to search for pastes from pastebin.com, we use the inurl: Google search parameter to do this. Your search should be formatted as follows:

inurl:pastebin.com <SEARCH PARAM>

When looking for stolen databases, you can start by searching for standard email providers:

- @gmail.com
- @live.com
- @hotmail.com
- @yahoo.com



inurl:pastebin.com @gmail.com after:2019

About 1,300 results (0.46 seconds)

pastebin.com › ...

Gmail@@ - Pastebin.com

Jan 8, 2020 - lalit[redacted]@gmail.com[redacted] conno[redacted]@hotmail.com:[redacted] log[redacted]@gmail.com[redacted] st[redacted]@rocketmail.com[redacted]

pastebin.com › ...

marius[redacted]@gmail.com:[redacted] ...

Mar 16, 2020 - jayc[redacted]@gmail.com:[redacted]. them[redacted]@gmail.com: [redacted]. cho[redacted]@hotmail.com:[redacted].

pastebin.com › GqJGmhS5

Email & Password: aba[redacted]@gmail.com:[redacted] ...

Jan 8, 2020 - RAW Paste Data. Email & Password: abar[redacted]@gmail.com:[redacted] Subscription: Premium Renew: Country: US ...

pastebin.com › tbuAJak2

#EXTINF:******************** Fresh mails 2020 ===> https ...

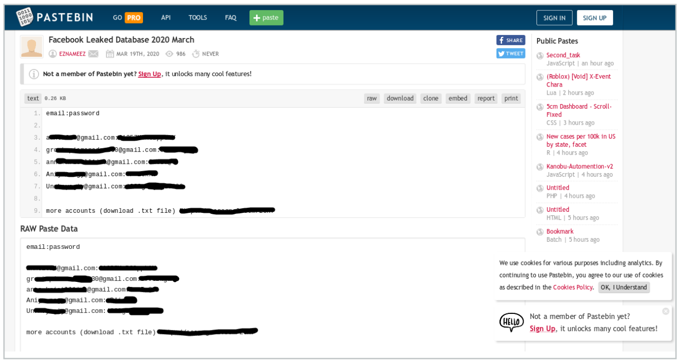
Feb 18, 2020 - db pastebin.com **@gmail.com**. pastebin cuentas gmail. pastebin free gmail accounts. pastebin @gmail @hotmail @yahoo. pastebin **gmail com** ...

pastebin.com › ...

p[redacted]5@gmail.com[redacted]djmiosibuffalo@gmail ...

Feb 7, 2020 - dj[redacted]@gmail.com:[redacted]. jerich[redacted]@gmail.com:[redacted]

Searching for emails helps find resurfaced stolen databases because these data sets contain leaked credentials belonging to these providers (see screenshot). To get the latest results first, we recommend setting the Google dork to sort by date. To do this, we use after: and before: search parameters, followed by the date (ex. after:2018-12-31 or after:2018):



Facebook Leaked Database 2020 March

EZNAMEEZ MAR 19TH, 2020 986 NEVER

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.26 KB raw download clone embed report print

```
email:password

a[redacted]@gmail.com:[redacted]
gr[redacted]0@gmail.com:[redacted]
an[redacted]@gmail.com:[redacted]
Ani[redacted]@gmail.com:[redacted]
Un[redacted]@gmail.com:[redacted]

more accounts (download .txt file) [redacted]
```

RAW Paste Data

```
email:password

[redacted]@gmail.com:[redacted]
gr[redacted]30@gmail.com:[redacted]
ar[redacted]@gmail.com:[redacted]
Ani[redacted]@gmail.com:[redacted]
Un[redacted]@gmail.com:[redacted]

more accounts (download .txt file)[redacted]
```

Public Pastes

Second_task
JavaScript | an hour ago

(Roblox) [Void] X-Event Chara
Lua | 2 hours ago

5cm Dashboard - Scroll-Fixed
CSS | 3 hours ago

New cases per 100k in US by state, facet
R | 4 hours ago

Kanobu-Automention-v2
JavaScript | 4 hours ago

Untitled
PHP | 4 hours ago

Untitled
HTML | 5 hours ago

Bookmark
Batch | 5 hours ago

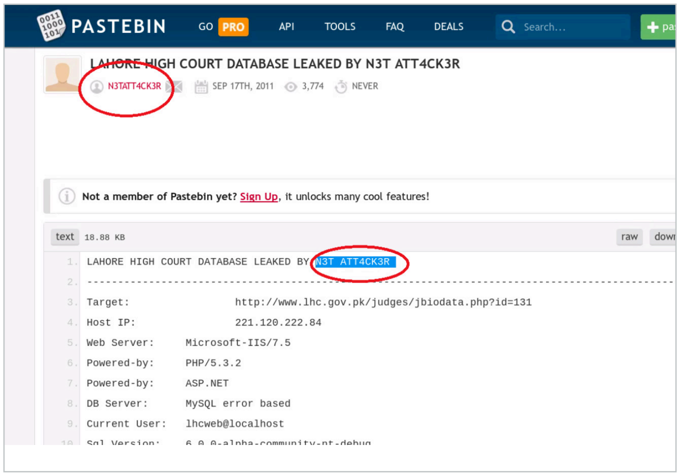
We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy. OK, I Understand

HELLO Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

Simply searching for the term **"database"** will return a number of stolen databases, accompanied by links to full dumps when the data set is too large for Pastebin to host. Alternatively, the link may redirect to an escrow or a marketplace forum, where a transaction must be completed before accessing the full data set.

The URL in our example redirects to rocketr.net, one of many publically available escrow services for trading currency for digital commodities, such as stolen data. Another popular escrow is satoshibox.com.

Searching for Visa, Mastercard, "cc dump," etc., helps find large credit card dumps that link back to carding forums where they are typically sold in bulk for a small price. Similarly, searching "dox" or "doxed" reveals lists of victims that have had their private information posted online. These individuals could easily become victims of financial fraud in the future, especially if the dox contains their social security numbers, credit card details, etc.



LAHORE HIGH COURT DATABASE LEAKED BY N3T ATT4CK3R

N3TATT4CK3R SEP 17TH, 2011 3,774 NEVER

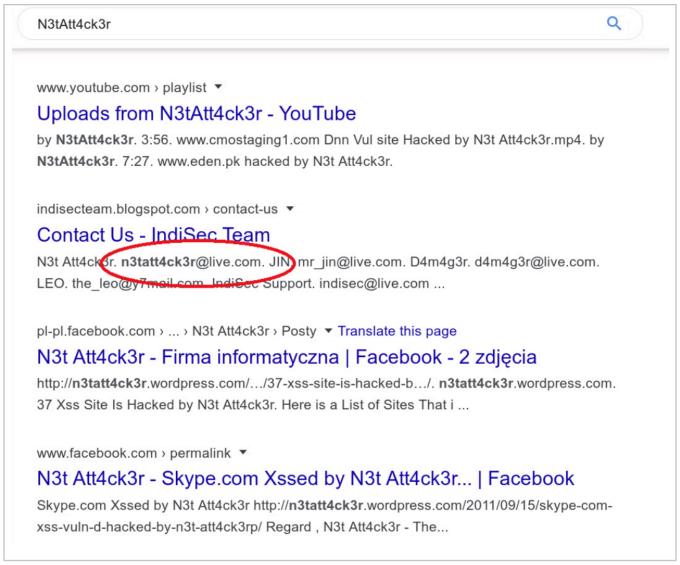
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 18.88 KB raw down

```
LAHORE HIGH COURT DATABASE LEAKED BY N3T ATT4CK3R
---------------------------------------------------------------------
Target:                 http://www.lhc.gov.pk/judges/jbiodata.php?id=131
Host IP:                221.120.222.84
Web Server:     Microsoft-IIS/7.5
Powered-by:     PHP/5.3.2
Powered-by:     ASP.NET
DB Server:      MySQL error based
Current User:   lhcweb@localhost
Sql Version:    6.0.0-alpha-community-nt-debug
```

Using Pastebin to Hunt for the Author of the Stolen Data

So far, we've learned how to find various forms of stolen data on Pastebin, but how can you attribute it to the real identity of a person who has actually leaked the goods? Sometimes (not always), pastes contain attribution in the form of an alias. People who leak information at times like being known as the root cause. Yes, some leakers like attribution, so they can use their reputation to increase sales of stolen data.



N3tAtt4ck3r

www.youtube.com › playlist ▾
Uploads from N3tAtt4ck3r - YouTube
by **N3tAtt4ck3r**. 3:56. www.cmostaging1.com Dnn Vul site Hacked by N3t Att4ck3r.mp4. by **N3tAtt4ck3r**. 7:27. www.eden.pk hacked by N3t Att4ck3r.

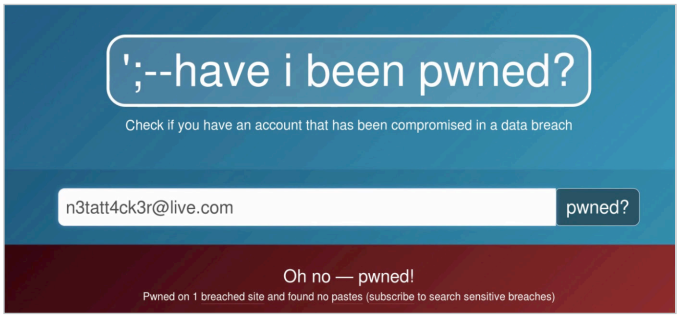
indisecteam.blogspot.com › contact-us ▾
Contact Us - IndiSec Team
N3t Att4ck3r. **n3tatt4ck3r**@live.com. JIN. mr_jin@live.com. D4m4g3r. d4m4g3r@live.com. LEO. the_leo@y7mail.com. IndiSec Support. indisec@live.com ...

pl-pl.facebook.com › ... › N3t Att4ck3r › Posty ▾ Translate this page
N3t Att4ck3r - Firma informatyczna | Facebook - 2 zdjęcia
http://**n3tatt4ck3r**.wordpress.com/.../37-xss-site-is-hacked-b.../. **n3tatt4ck3r**.wordpress.com. 37 Xss Site Is Hacked by N3t Att4ck3r. Here is a List of Sites That i ...

www.facebook.com › permalink ▾
N3t Att4ck3r - Skype.com Xssed by N3t Att4ck3r... | Facebook
Skype.com Xssed by N3t Att4ck3r http://**n3tatt4ck3r**.wordpress.com/2011/09/15/skype-com-xss-vuln-d-hacked-by-n3t-att4ck3rp/ Regard , N3t Att4ck3r - The...

Leakers tend to only release partial dumps of the data breach on sites like Pastebin as a form of advertisement. The more obvious approach is to link directly to a forum or marketplace where the full dump can be purchased or traded for sought-after commodities.

Some attackers consistently use the same aliases, so even a simple Google search will show their nicknames appearing on several different platforms, most likely hoping to generate more leads for their offerings.


';--have i been pwned?

Check if you have an account that has been compromised in a data breach

n3tatt4ck3r@live.com

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

The easiest way to figure out who is hiding behind an alias is to locate their email. Email addresses are used to sign into various sites, and inevitably sites get breached and their users' personal information gets stolen and placed inside a database.

If we want to pursue this investigation even further, we can get our hands on the database in which this user resides, and find other essential artifacts, like their IP addresses, phone numbers, and more.

According to HaveIbeenPwned.com, this particular person has been found in one data breach. In addition to their own password, the database also contains an IP address. A simple search can help determine the general location of the attacker, and law enforcement can go much further in identifying and locating this individual.

This example shows how a researcher can go from a leak posted on Pastebin to unveiling the identity of the perpetrator. A series of simple steps can help investigators get to the bottom of unmasking the hacker who is responsible for the leak, and if warranted, even taking legal action.

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

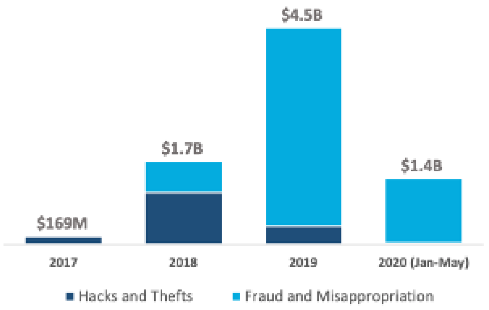
© Authentic8, Inc. All rights reserved. 01082021

Crypto Money Laundering on the Rise

Since Bitcoin's historic rise, the number of users participating in the cryptocurrency ecosystem has reached nearly 69 million. This increase in active cryptocurrency users has also led to a surge of cryptocurrencies being used to launder money. According to the United Nations Office on Drugs and Crime, money laundering costs the global economy between $800 billion and $2 trillion per year — that's two to five percent of the world's gross domestic product.

Money laundering in the era of cryptocurrency is more convenient than traditional laundering schemes, with multiple types of available crypto coins and a good amount of anonymity for traders to hide their true identities. Add the dark web, and you have a murky, constantly changing and decentralized environment that creates many additional challenges for investigators.

Blockchain Fraud Continues to Vastly Exceed Hacks and Thefts in 2020



Source: CipherTrace Cryptocurrency Intelligence

FinCEN Warns of Threats Posed by Virtual Currency Misuse

Criminals continue to exploit virtual currency to support illegal activity, money laundering and other behavior endangering U.S. national security. To help financial institutions, law enforcement and regulators who work with convertible virtual currencies (CVCs), the Financial Crimes Enforcement Network (FinCEN) offers guidance to assist organizations in identifying and reporting suspicious activity. The advisory highlights the risks associated with dark web marketplaces, peer-to-peer (P2P) exchangers, unregistered money services businesses and CVC kiosks. It also gives organizations a set of tools to help identify unregistered financial activity and suspicious virtual currency purchases, transfers and transactions.

The Need for Effective AML Programs

The FinCEN regulatory framework mandates that businesses develop, implement, and maintain an effective anti-money laundering program ("AML program") that is designed to prevent organizations from being used to facilitate money laundering and the financing of terrorist activities.

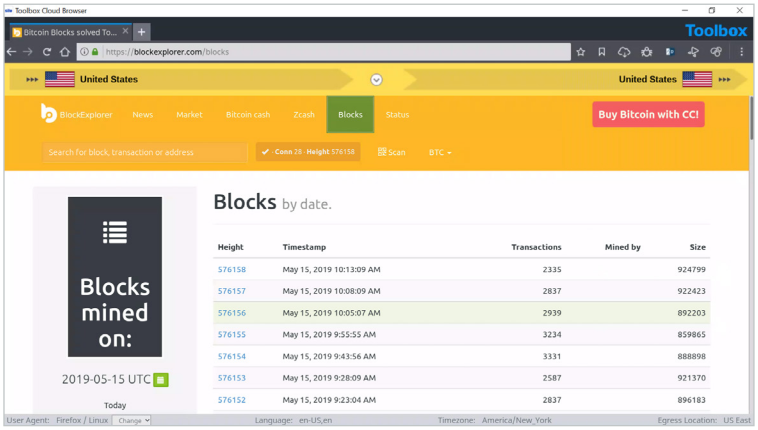
The minimum set of requirements for an AML program include:

- Establishment of policies, procedures, and internal controls designed to assure ongoing compliance (including verifying customer identification, filing reports, creating and retaining records and responding to law enforcement requests
- Designation of individuals responsible to assure day-to-day compliance with the program
- Training for appropriate personnel, including training in the detection of suspicious transactions
- Ongoing independent reviews to monitor and maintain an adequate program

> Without sufficient controls in place, financial institutions cannot reasonably assess and mitigate the potential risks posed by a customer's source of funds, and criminals can exploit the U.S. financial system by engaging in illicit transactions. Individuals engaged in illicit activity will continue to exploit these vulnerabilities as long as the perceived risk of detection is less than that of using traditional financial institutions.

Tracking Cryptocurrencies

How can CVC transactions be tracked? One popular way is using blockchain technology. Blockchain is an open, decentralized ledger that records transactions between two parties in a permanent way without needing third-party authentication. For example, every transaction involving a Bitcoin address is stored forever in the blockchain; however, Bitcoin addresses are pseudonyms, meaning that the identity of the address owner (i.e., who receives bitcoin at that address) is generally unknown.



Blocks by date.

Height	Timestamp	Transactions	Mined by	Size
576158	May 15, 2019 10:13:09 AM	2335		924799
576157	May 15, 2019 10:08:09 AM	2837		922423
576156	May 15, 2019 10:05:07 AM	2939		892203
576155	May 15, 2019 9:55:55 AM	3234		859865
576154	May 15, 2019 9:43:56 AM	3331		888898
576153	May 15, 2019 9:28:09 AM	2587		921370
576152	May 15, 2019 9:23:04 AM	2837		896183

User Agent: Firefox / Linux Language: en-US,en Timezone: America/New_York Egress Location: US East

Bitcoin blockchains from blockexplorer.com

If a user's address is ever linked to their identity, every transaction will be linked to that user. Below are examples of OSINT tools that allow investigators to search by block number, address, block hash, transaction hash or public key to find out more information on bitcoin transactions.

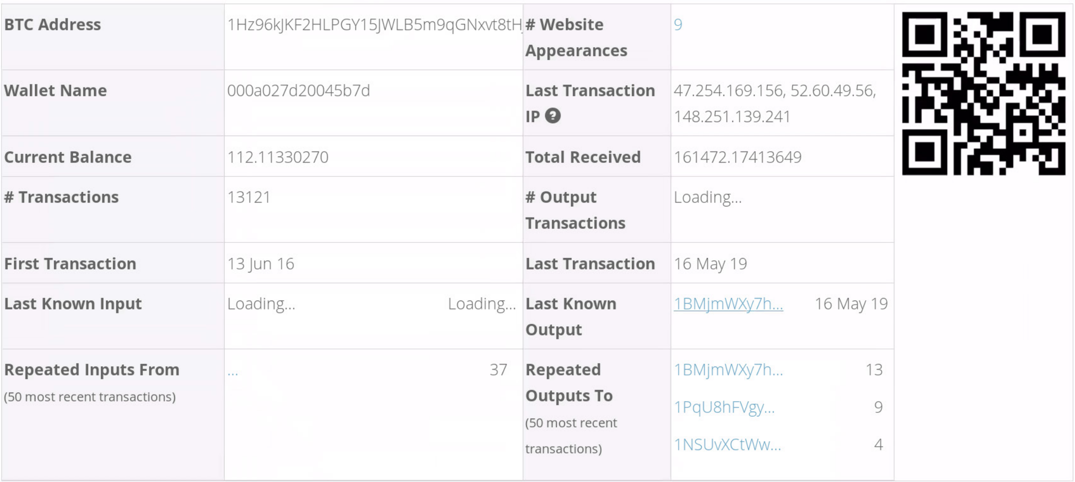
- https://www.blockchain.com/explorer
- https://blockchain.info/
- https://www.chainalysis.com/
- https://bitcoinwhoswho.com/

To prevent tracking on their transactions, money launderers have begun to use a system known as cryptocurrency tumblers. Cryptocurrency tumblers mix potentially identifiable currency with untraceable currency to make it harder to track.

Some addresses can be grouped by their ownership, using behavior patterns and publicly available information from off-chain sources. The challenge for forensic investigators, as usual, is to identify the persons behind the keyboard, which may be accomplished through a mixture of traditional investigative and digital forensic techniques.

Bitcoin Address Reports

Once a Bitcoin address is identified, it can be run through a blockchain tracking tool. Using bitcoinwhoswho.com, investigators can generate a report for bitcoin address 1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tHJ.



BTC Address	1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tH	**# Website Appearances**	9
Wallet Name	000a027d20045b7d	**Last Transaction IP** ?	47.254.169.156, 52.60.49.56, 148.251.139.241
Current Balance	112.11330270	**Total Received**	161472.17413649
# Transactions	13121	**# Output Transactions**	Loading...
First Transaction	13 Jun 16	**Last Transaction**	16 May 19
Last Known Input	Loading... Loading...	**Last Known Output**	1BMjmWXy7h... 16 May 19
Repeated Inputs From (50 most recent transactions)	... 37	**Repeated Outputs To** (50 most recent transactions)	1BMjmWXy7h... 13 1PqU8hFVgy... 9 1NSUvXCtWw... 4

Bitcoin address report from bitcoinwhoswho.com

Probable fields of interest:

- **Current Balance/Total Received:** This data point allows analysts to hypothesize which type of address they're dealing with. Due to the high volume of transactions, this wallet likely belongs to a bitcoin miner.
- **Last Transaction IP:** Analysts can view the last known IP to relay an output transaction involving a selected address. Repeated use of an IP can be used as a unique identifier.
- **Website Appearances:** Provides a view of any site where this exact bitcoin address appeared, which could be of value for identifying reputation/type of transactions.
- **Repeated Inputs From/Repeated Outputs To**: This data point allows analysts to view the 50 most recent Bitcoin addresses involved with incoming and outbound transactions associated with this address. By looking at the transaction history and frequently interacted-with wallets, investigators can engage in network and link analysis to identify patterns and possible relationships between the disparate Bitcoin addresses.

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

© Authentic8, Inc. All rights reserved. 01082021

silo
By Authentic8

TOP CHALLENGES

Financial Crime Investigators

Q2 2020 survey of 500+ financial fraud investigators reveals anti-fraud specialists lack proper tools to conduct critical investigations on the web, putting themselves and their organizations at risk.

INSUFFICIENT TOOLS

Expose Investigators to Potential Threats

80% need to mask their identity on the web for investigations

+

15% also need to access the dark web at least once every month

=

YET **58%** use a local browser on their main corporate PC for investigations

EFFICACY & EFFICIENCY CHALLENGES

Put Investigations & Organizations at Risk

30% are routinely blocked from relevant websites

44% struggle with chain of custody for evidence

66% face challenges in hiding their online identity

CLOUD BROWSER

Enables Secure and Anonymous Investigations

2X fewer people face a challenge in hiding their online identity

Do Financial Crime Investigators Have a Bull’s Eye on their Back?

Rishi Kant

The COVID-19 pandemic seems like a double whammy for financial crime investigators. While online fraud has skyrocketed, teams are still adapting to a remote work environment. A recent survey among Association of Certified Financial Crime Specialists (ACFCS) members asked: Are they appropriately equipped for their mission?

Financial institutions are on high alert as attacks on the industry spiked by 38% in February and March. In March, the Financial Crimes Enforcement Network (FinCEN) alerted institutions to “malicious and fraudulent transactions similar to those that occur in the wake of natural disasters” and warned them of increased scam activity.

Between January and February, the Federal Trade Commission (FTC) reported more than 52,000 cases of fraud that were related to COVID-19 and resulted in $38.6M of fraud loss. All of this puts additional pressure on the industry’s fraud analysts and investigators, while they struggle with the consequences of working from home.

Together with Authentic8, the Association of Certified Financial Crime Specialists (ACFCS) asked members who attended a recent webinar on dark web research if they felt sufficiently equipped to conduct their online investigations.

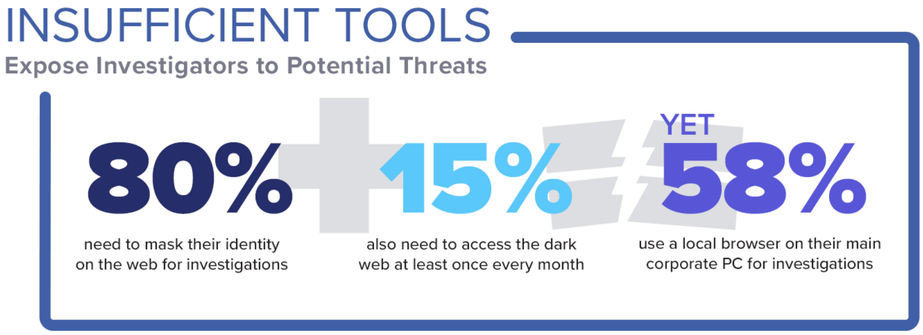
When anonymity is vital, does your browser have your back?

More than 500 cybersecurity leaders, investigators, and analysts responded. The collective answer: “No.”

The results indicate that most surveyed specialists lack the proper equipment to conduct critical investigations on the web securely and efficiently. The culprit is the web browser.

I found it remarkable that the primary tool financial crime specialists rely on for their investigative work on the web is putting their mission and their organizations at risk. There were three main takeaways from the survey:

1. Investigator needs are not met by tools provided
2. Tool-related challenges impede investigations and can put organizations at risk
3. A specific cohort of investigators had much less “pain” than the rest



INSUFFICIENT TOOLS

Expose Investigators to Potential Threats

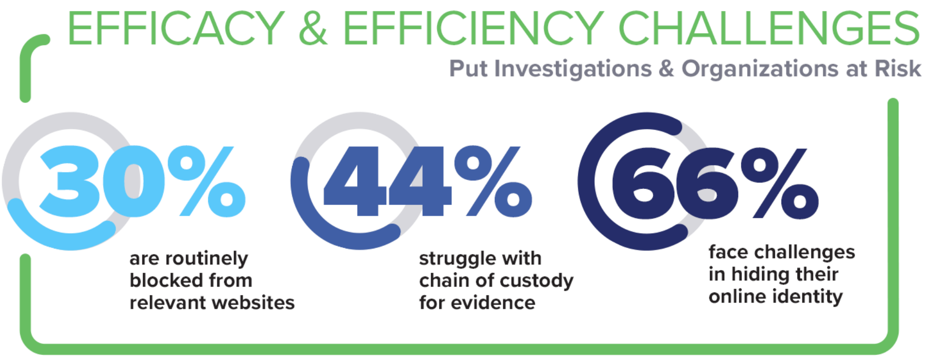
80% need to mask their identity on the web for investigations

15% also need to access the dark web at least once every month

YET 58% use a local browser on their main corporate PC for investigations

1 - Investigator needs are not met by tools provided

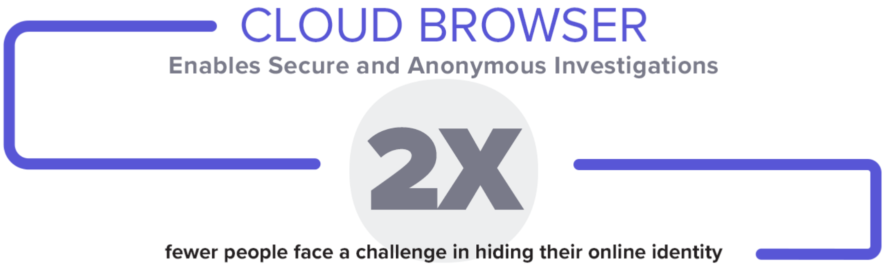
- Need - 80% of those involved with investigative work online stated that they need to hide or misattribute their identity online. Anonymity or managed attribution capabilities are essential for investigators when examining suspicious websites or online forums because revealing their identity—or that of their organization—can compromise their mission and makes them vulnerable to targeted watering hole attacks.
- Need - 15% of those surveyed said they need to access the dark web at least once every month. Many criminal activities happen on the dark web, so investigators frequently need to visit these sites.
- Mismatch - Yet 58% of that same group responded that they conduct investigations without protection, via a local browser on their PC. Local browsers can reveal detailed information about the user, organization, and corporate assets, even with "incognito mode" or VPN / privacy plugins in place, which effectively runs counter to the "hide or misattribute" need for investigators. Additionally, using a local browser to access the dark web can open an organization to scrutiny and reputational risk.



2 - Tool-related issues impede investigations and put organizations at risk

- 66% face a challenge in hiding their online identity. As discussed above, it is critical to hide the investigator's and organization's identity to protect investigations and avoid possible "watering hole" attacks. Unfortunately, a local browser does little to protect one's identity, which can jeopardize investigations, lead to regulatory fines and reputation risk for the organization.
- 44% of those collecting and analyzing evidence face issues in maintaining chain-of-custody. Compliance manager needs are best met by a centrally managed, encrypted, tamper-safe audit logging system - capabilities that are not readily available in a decentralized local browsing environment. As a result, an investigator's hard work may be naught due to technicalities in chain-of-custody management.
- 30% are routinely blocked from accessing sites they need to investigate. Most local browsers are governed by a set of corporate web filters that deny access to websites based on company-wide policy. Unfortunately, many investigators need to visit suspicious sites, which are likely to be blocked. This can result in delays of multiple days that can impact the timely filing of regulatory reports (e.g., Suspicious Activity Reports) and lead to fines on the financial institution.

3 - A specific cohort of investigators had much less "pain" than the rest



CLOUD BROWSER

Enables Secure and Anonymous Investigations

2X

fewer people face a challenge in hiding their online identity

The most remarkable result of the survey was that not everyone claimed to face the above challenges. There was one cohort—those who used a cloud browser solution—who claimed to have much less "pain" than the rest.

The implication: There is a better way of doing things than using a local browser.

What is a "cloud browser"?

A cloud browser is a browser that runs on cloud-hosted servers. It executes all web code in a secure, isolated environment managed by policy, to provide protection and oversight. The end-user device receives a benign display stream, and end-users can interact via regular mouse and keyboard input. A concrete example of this is Silo for Research (Toolbox).

Silo for Research is a cloud browser-based product, built for the needs of investigators. Silo for Research combines web isolation with attribution management for secure, geographically distributed research and analysis.

Silo for Research can be configured to appear on the internet from one of dozens of global exit nodes and spoof different client environments. To the website under examination, the research framework presents itself as a regular browser launched on a local device on a local network.

Websites and social media platforms are presented only with the IP address of Authentic8's server and cannot trace the network back to the end-user. This eliminates the risk of attribution or de-anonymization as the result of the web browser.

Can you measure investigation outcomes?

It is possible, but it is essential to recognize that different stakeholders have different outcomes they care about regarding an investigation. The good news is that a solution like Silo for Research can address the top priorities for multiple stakeholders.

- **Analysts and investigators** can decrease time to insight, even in a WFH environment. Purpose-built tooling can drive Mean-Time-To-Resolution (MTTR) down by up to 50%.
- **IT admins and support teams** can reduce costs and management overhead. Cloud-hosted tooling can reduce expenses by 2x compared to custom-built infrastructure.
- **Compliance and risk officers** can simplify compliance and improve case documentation. Auditable logs enable teams to meet regulatory requirements.

So yes, investigation outcomes can be measured—not only in lower IT costs and MTTR reduction—but also in avoiding regulatory sanctions.

With Silo for Research, your firm will be able to conduct timely and thorough investigations (even when analysts work from home), file SARs quickly, maintain chain-of-custody and promptly produce documentation if compelled by regulators - without pushing IT to the brink.

Final thoughts

Financial crime is on the rise. Pandemic-induced remote work is hampering investigations. Regulatory fines continue to grow in size. Does it make sense to roll the dice when it comes to equipping analysts and investigators with the tools they need?

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

© Authentic8, Inc. All rights reserved. 01082021

silo
By Authentic8

CASE STUDY
FINANCIAL SERVICES

Case Study: Global Top Ten Financial Services Firm

Authentic8 Helps Identify Threats and Fraudsters Online

Banks, insurance companies, and financial service firms today use many different methods to gather intelligence from the open, deep, and dark web. For the financial industry, open source intelligence is a valuable resource to keep businesses up to date on existing, evolving and future threats, past breaches, or hidden caches of compromised, fraud-related data.

Introduction

A top ten financial institution with teams of investigators focused on different challenges, The firm relies on the Authentic8 Silo for Research (Toolbox) solution for their cyber-threat intelligence, financial fraud, and anti-money laundering investigations.

Thomas B. is tasked with gathering cyber-threat research from the far corners of the web. The information gathered helps protect The firm from both targeted and indiscriminate attacks by malware and bad actors.

The Challenge

Prior to deploying Silo for Research, The firm was using a DIY approach to cyber-threat investigations by combining consumer browsers, plug-ins, and VPN solutions to perform their threat hunting activities. “We found that our existing perimeter security solutions were blocking where we needed to go on the web. There was no way to visit them without exposing the rest of the network to potentially malicious threats,” Thomas B. said. “In addition, we were using third-party vendors and business partners to outsource malware analysis, increasing costs and exposing sensitive information that we would prefer to keep in-house.”

One of the main business drivers for adopting the Authentic8 solution was maintaining the anonymity of online investigators. “Visiting a web page reveals a lot about the visitor, including their IP address. That IP address can be traced back to the company and jeopardize future intelligence-gathering efforts, so maintaining anonymity is a top priority,” said Thomas B.

Another top concern for the organization was infection and compromise from the very same threats they were hunting for. “Cyber-threat investigations — without the proper safeguards and precautions — can significantly increase network risk,” Thomas B. continued. “We needed a solution that worked in our environment and provided the logical separation to mitigate just about any malware threat, and Silo’s cloud isolation provides that capability.”

THE STORY

Previously used a high cost, resource intensive DIY investigation platform

DIY solution lacked anonymity, prone to tracking and compromise

Needed a cost effective, cyber-threat research solution to gather intelligence of targeted threats

Silo was an all-in-one solution to meet researcher requirements

Maintains anonymity and security of online investigations

Secure team storage for evidence sharing and collaboration

The Implementation

In large organizations, getting approvals to implement a new application can sometimes be harder than implementing the solution itself. "As with any new solution, we had a number of internal departments to coordinate with, educate, and gain approval from, before the roll-out of the Silo Web Isolation Platform," Thomas B. recalled. "Luckily, the solution was very straightforward to deploy across four to five different groups internally, and it is now utilized by multiple teams both inside and outside the security organization."

Working in the highly regulated financial services industry, The firm is required to provide proof of compliance to both internal and external auditors. With integration into Splunk, The firm set up a log pipeline to capture all Silo for Research activity, storing the logs within a central repository to meet those compliance requirements.

"A number of key features in Silo for Research have been instrumental in helping us understand the threats that pose the most risk to the enterprise," Thomas B. stated. "With thousands of alerts per month, time to intelligence is critical for making a determination and implementing an effective response. Silo is an all-in-one solution that helps us do that faster and more easily than our previous DIY solution."

The Result

Since the initial deployment, Authentic8 has been instrumental in helping The firm meet their goals. "Now with Silo for Research deployed, we can work around the IT restrictions and can go anywhere we need to go on the internet. We do all of the threat analysis in-house now and don't have to outsource to anyone. That reduces our cost, but more importantly it allows us to make a faster determination of risk to immediately verify the threat mitigation strategies we have in place," Thomas B. recollected. With DIY investigation solutions, bad actors and fraudsters are able to profile a researcher's web visits based on their resources, such as AWS S3 buckets used for storing evidence during collection. Non-attributable platforms such as Silo for Research can use multiple egress locations to protect the identity of The firm, enable encrypted storage in private cloud-based repositories, and keep counterintelligence efforts in the dark.

"Silo has changed the way we approach cyber-threat hunting, fraud research, and other online investigations," concluded Thomas B. "The cloud-based management and policy framework allows control over Silos's features and functionality, while the isolation platform as a whole keeps our investigators safe and anonymous online."

> *"Silo has changed the way we approach cyber-threat hunting, fraud research, and other online investigations."*

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

© Authentic8, Inc. All rights reserved. 01082021

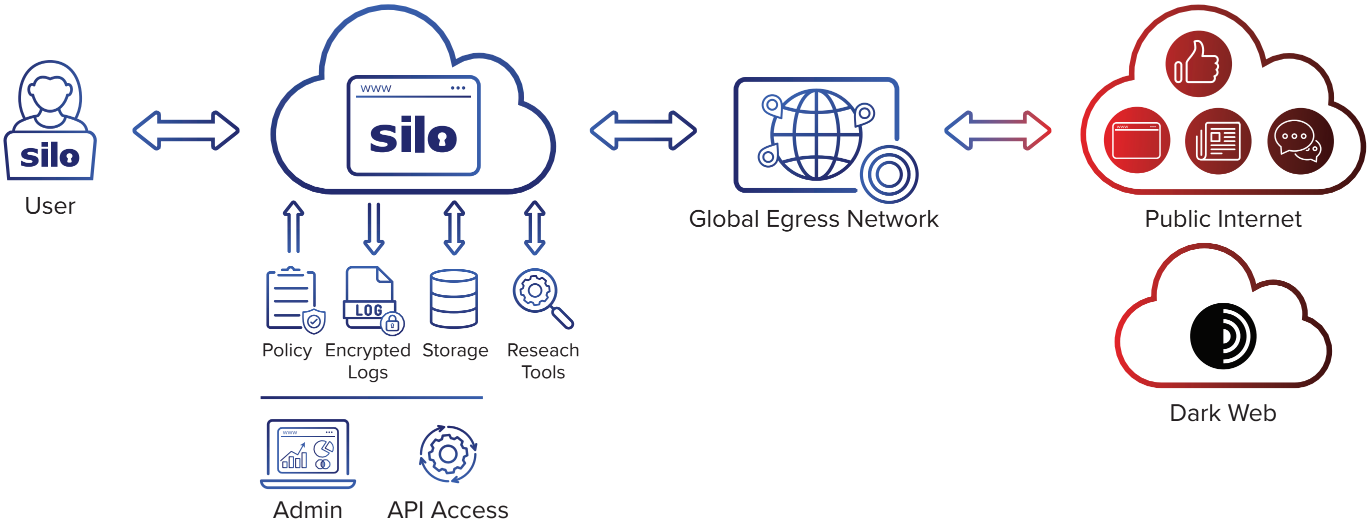
silo
By Authentic8

DATA SHEET

Silo for Research

Secure and Anonymous Online Investigations

Silo for Research (Toolbox) is a secure and anonymous web browsing solution that enables users to conduct research, collect evidence and analyze data across the open, deep and dark web.

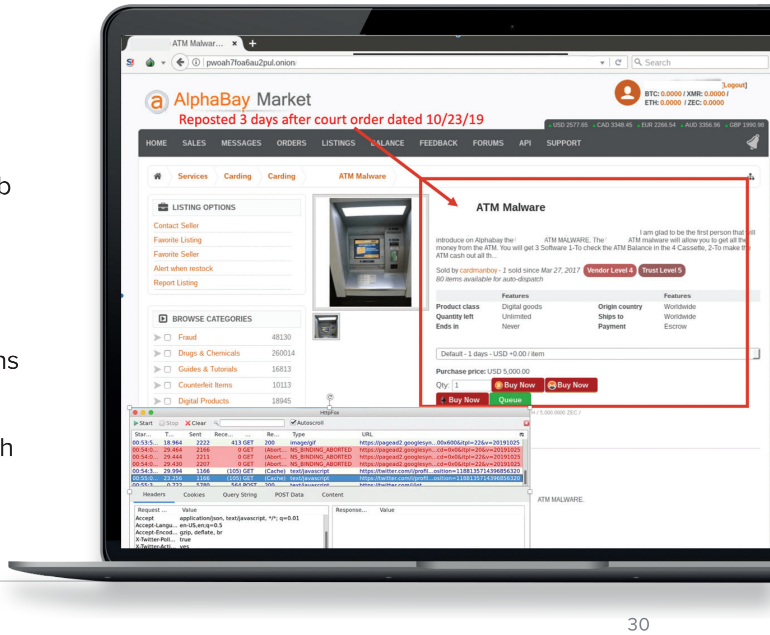


Silo for Research is built on Authentic8’s patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

Research teams can accomplish their goals without introducing risk to the organization or revealing intent. All web activity is logged and encrypted so compliance teams can be sure that the tools are being used appropriately.

The world’s most at-risk enterprises and government agencies rely on Silo for Research to conduct secure and anonymous online investigations:

- **Criminal investigations:** Comply with chain-of-custody policy and securely collect evidence on the open, deep, or dark web
- **Cyber threat intelligence:** Access and analyze suspicious or malicious content with 100% isolation from corporate infrastructure
- **Financial investigations:** Keep your online fraud investigations anonymous and secure, even on the dark web
- **Open-source intelligence (OSINT):** Disguise your identity with a managed attribution platform and global egress network



AlphaBay Market

Reposted 3 days after court order dated 10/23/19

BTC: 0.0000 / XMR: 0.0000 /
ETH: 0.0000 / ZEC: 0.0000

USD 2577.65 CAD 3348.45 EUR 2266.54 AUD 3356.96 GBP 1990.98

ATM Malware

I am glad to be the first person that will introduce on Alphabay the ATM MALWARE. The ATM malware will allow you to get all the money from the ATM. You will get 3 Software 1-To check the ATM Balance in the 4 Cassette, 2-To make the ATM cash out all th...

Sold by cardmanboy - 1 sold since Mar 27, 2017 Vendor Level 4 Trust Level 5
80 items available for auto-dispatch

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 5,000.00

Qty: 1

BROWSE CATEGORIES	
Fraud	48130
Drugs & Chemicals	260014
Guides & Tutorials	16813
Counterfeit Items	10113
Digital Products	18945

```
Star...    T...    Sent  Rece...  ...  Re...     Type                URL
00:53:5... 18.964  2222    413 GET     200       image/gif           https://pagead2.googlesyn...00x600&itpl=22&v=20191025
00:54:0... 29.464  2166      0 GET     (Abort... NS_BINDING_ABORTED  https://pagead2.googlesyn...cd=0x0&itpl=20&v=20191025
00:54:0... 29.444  2211      0 GET     (Abort... NS_BINDING_ABORTED  https://pagead2.googlesyn...cd=0x0&itpl=22&v=20191025
00:54:0... 29.430  2207      0 GET     (Abort... NS_BINDING_ABORTED  https://pagead2.googlesyn...cd=0x0&itpl=22&v=20191025
00:54:3... 29.994  1166  (105) GET     (Cache)   text/javascript     https://twitter.com/i/profil...osition=1188135714396856320
00:55:0... 23.256  1166  (105) GET     (Cache)   text/javascript     https://twitter.com/i/profil...osition=1188135714396856320
00:55:3... 0.722   5780    564 POST    200       text/javascript     https://twitter.com/i/jot
```

```
Request ...       Value
Accept            application/json, text/javascript, */*; q=0.01
Accept-Langu...   en-US,en;q=0.5
Accept-Encod...   gzip, deflate, br
X-Twitter-Poll... true
X-Twitter-Acti... yes

Response...       Value
```

ATM MALWARE.

silo
By Authentic8

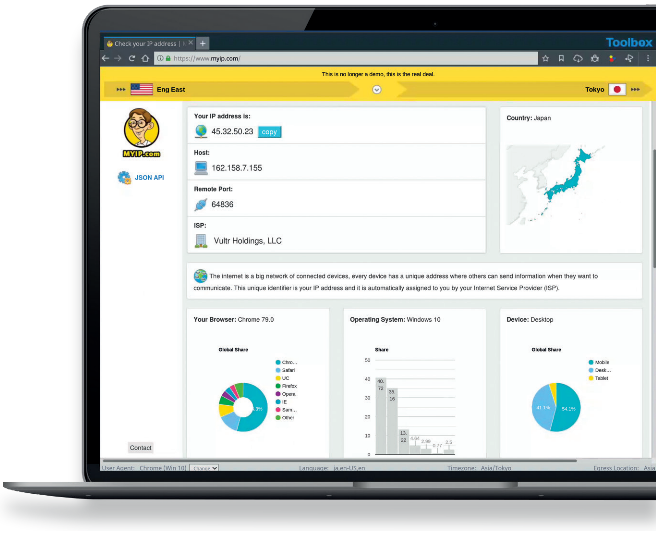
DATA SHEET: SILO FOR RESEARCH

Features and Benefits

FEATURES	BENEFITS
Full Isolation: All web code is executed on Silo servers, not end-user devices	Potentially unsafe content never touches your organizations' assets
Cloud-Based: Turn-key, cloud-hosted solution that creates a clean instance every time	Seamless, immediate deployment with on-demand access from anywhere
Managed Attribution: Configure the browser fingerprint and egress location	Blend in with the crowd to not trip off your intent to others
Access Open, Deep or Dark Web: One-click access to any destination without tainting your environment	Maintain policy, while providing a secure way for users to interact with any destination
Workflow Enhancements: Integrated tools for content capture, analysis and storage	Improve time to insight for analysts with integrated tools
Complete Audit Oversight: Encrypted audit logs of all web activity are captured in one place and easily exported	Simplify analyst compliance and audit, and improve case documentation

Use the Silo Web Isolation Platform to maintain data security, and respect the privacy of your users. Our compliance:

- FedRamp In Progress
- HIPAA
- PII
- PCI
- GDPR
- CCPA



This is no longer a demo, this is the real deal.

Your IP address is: 45.32.50.23

Host: 162.158.7.155

Remote Port: 64836

ISP: Vultr Holdings, LLC

Country: Japan

The internet is a big network of connected devices, every device has a unique address where others can send information when they want to communicate. This unique identifier is your IP address and it is automatically assigned to you by your Internet Service Provider (ISP).

Your Browser: Chrome 79.0

Operating System: Windows 10

Device: Desktop

User Agent: Chrome (Win 10) Language: ja,en-US,en Timezone: Asia/Tokyo Egress Location: Asia

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

© Authentic8, Inc. All rights reserved. 01082021

Silo
By Authentic8

OVERVIEW

Silo for Research (Toolbox) Dark Web

Challenge

Dangerous organizations and individuals operate in the shadows. So when you need to find them online, you have to go on the dark web. But the dark web is a hazardous place where criminals and adversaries have the upper hand by:

- Employing sophisticated counter-surveillance tools
- Booby-trapping sites with malware
- Actively recruiting legitimate analysts and researchers for illicit purposes

As a result, resource-constrained organizations (e.g., local law enforcement) too often lack dark web access, while large organizations (e.g., federal agencies) typically build separate "dirty" infrastructures which are expensive, labor-intensive, slow, and opaque.

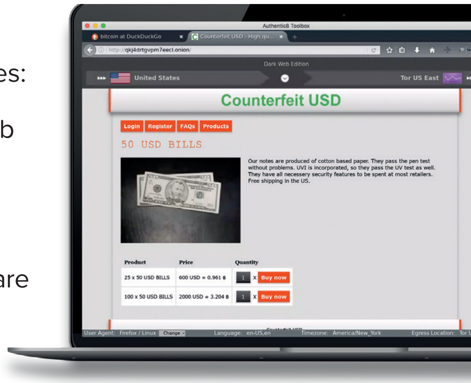
Solution

Silo for Research Dark Web provides simple and safe "point & click" access to dark web content (Tor). Dark web access is seamlessly integrated within Silo for Research and its suite of analyst tools, as compared to a separate and standalone Tor browser. Silo for Research Dark Web extends the Authentic8 global egress network to include designated .onion-capable nodes. Each node is connected via IPSec, but converts requests to SOCKS for access to the Tor network. Each Tor connection is built from scratch based on a randomly selected ingress node, relay, and egress node.

Benefits

In addition to the familiar benefits of Silo for Research, Silo for Research Dark Web provides:

- A single pane of glass for analysts to conduct research on the open, deep, and dark web
- Full isolation from dark web counter-surveillance and threats (e.g. malware)
- Organizational control to manage and deter unauthorized use of the dark web
- Dark web access without the need to install or manage additional applications or software
- Comprehensive audit oversight extended to the dark web



Our notes are produced of cotton based paper. They pass the pen test without problems. UVI is incorporated, so they pass the UV test as well. They have all necessery security features to be spent at most retailers. Free shipping in the US.

Product	Price	Quantity
25 x 50 USD BILLS	600 USD = 0.961 ฿	1 x Buy now
100 x 50 USD BILLS	2000 USD = 3.204 ฿	1 x Buy now

Silo
By Authentic8

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

© Authentic8, Inc. All rights reserved. 01082021