

DARKNET PACK

Darknet Pack is a set of specialized methods providing access to the Dark Web data, aimed to generate high-quality and actionable intelligence

The Dark Web

Gain full access to darknet marketplaces, forums, and more



Clementine Joseph

Personal Email
CLEMENTINE@GMAIL.COM
Phone Numbers
+ 676 89 323 46



Robert Jackson



Vivian Mancos Mary



Thomas Joseph

Username
THOMAS JOSEPH-2453
Crypto Wallet
ADDRESS: [LINK](#)
PASSWORD: Q34RD!RF



Jean Mary

IP Addresses
123.567.34.68.543
Passwords
9876908TRH!345

WHY USE DARKNET DATA IN INVESTIGATIONS?



UNCOVER ILLICIT ACTIVITIES

Trace suspicious transactions and identify individuals involved in financial crime



ENRICH STANDARD INVESTIGATIONS

Gain deeper insights into illicit activities to help deanonymize criminal actors



FIGHT EXTREMIST ACTIVITIES

Monitor Dark Web forums to gather information about potential terror threats



INVESTIGATE CYBERCRIME

Explore emerging hacking tools, zero-day vulnerabilities, malware, exploit kits, etc.



COMBAT ILLEGAL TRADE

Uncover trade in stolen credentials and fake documents, and drugs, arms, and human trafficking, etc.



COUNTER DATA BREACHES

Check if any sensitive data (personal or corporate) has been leaked and trace the source of the breach

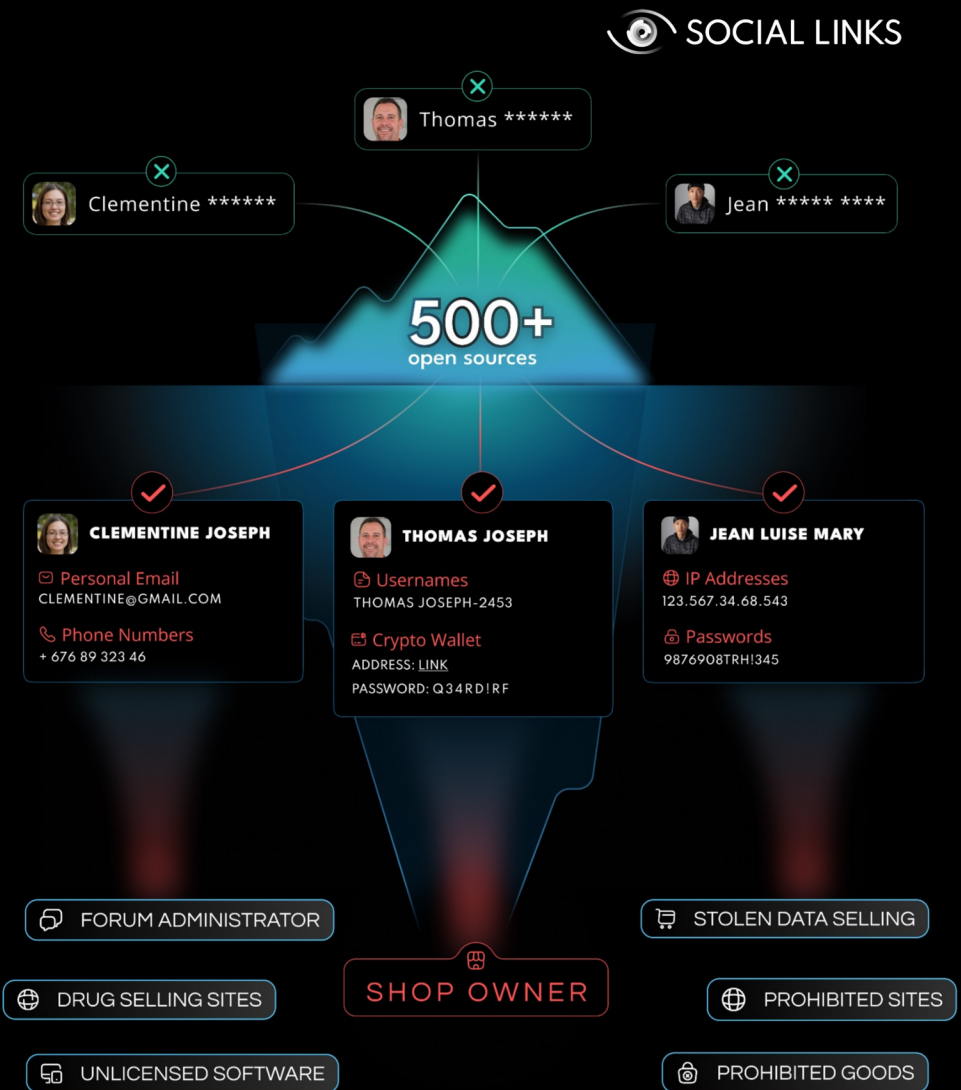
SEARCH ACROSS ALL DATA DOMAINS

THE DARKNET PACK ALLOWS USERS TO:

-  Exposure Checks: shows if employees' passwords have been leaked or if a cyber attack is being planned
-  Darknet crimes: search darknet marketplaces and forums for usernames, account details, listings, and more
-  ClearNet investigations: connects phone numbers and Twitter accounts, crypto wallets and email addresses, and so on

USERS BENEFIT FROM:

-  The integration of Surface Web data and Dark and Deep Web data for comprehensive intelligence
-  A 360 degree solution covering multiple sources from a single workstation
-  Case leads and breakthroughs which would be otherwise impossible



SL DARKNET COVERAGE



STEALER LOGS

Structured data stolen via malware and posted on the Dark Web. It's like a device "snapshot"

Regular Surface Web Investigations & Exposure Checks

Extracting details (usernames, emails, phone numbers, passwords) from accounts held on a given infected computer

 Username and person's name

 Emails & email domains

 Passwords

 Device serial numbers

 Crypto wallets

 Phone numbers

 Browser history

DATA LEAKS

Personal data and account details involved in the breach

Regular Surface Web Investigations & Exposure Checks

Finding connections between phone numbers, social media accounts, crypto wallets, and email addresses

 Username and person's name

 Social media profiles (Facebook, X, Skype, etc.)

 Passwords***

 IP addresses

 Crypto wallets

 Phone numbers

 Emails & email domains

DARK WEB DATA

Data from darknet marketplaces and forums, paste sites, and alternative social media

Dark Web & Deep Web Investigations

Analyzing threads and discussions on forums and identifying the authors, viewing marketplace listings, and investigating vendors

 Comments & threads on forums

 Username and person's name

 Crypto wallets

 Emails & email domains

 Phone numbers

 Vendors from marketplaces and products they sell

STEALER LOGS: A CRUCIAL RESOURCE FOR INVESTIGATORS



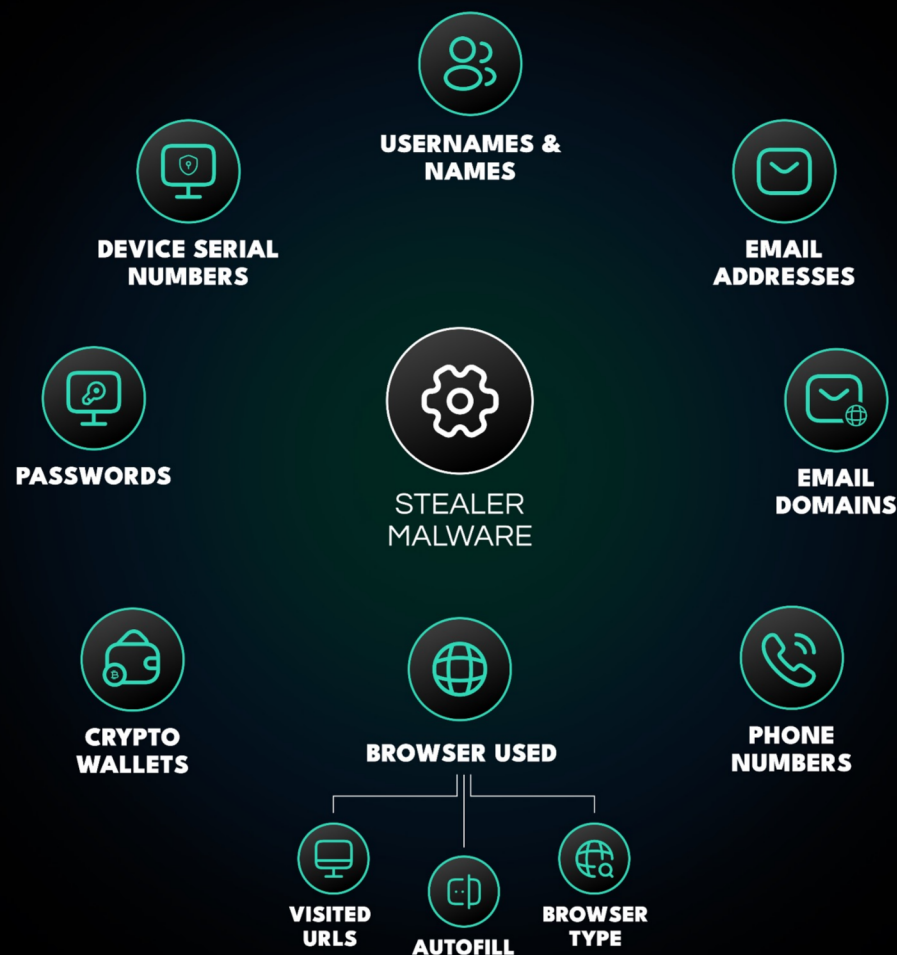
This feature allows users to access browser history, device serial numbers, and other sensitive details from an infected device. It facilitates comprehensive investigations and links related emails or accounts to specific devices.

INFOSTEALERS

are malware, usually downloaded via email, that infects the device and starts stealing data

STEALER LOGS

are repositories containing stolen data that has been posted on the Dark Web



STEALER LOGS: HOW IT WORKS



EMAIL

For example, you find an email address via social media but have no further leads



DEVICE SERIAL NUMBER

The Stealer Logs feature can connect the email address to a specific device



OTHER EMAILS CONNECTED WITH THE DEVICE

You can then extract other email addresses connected to the same device

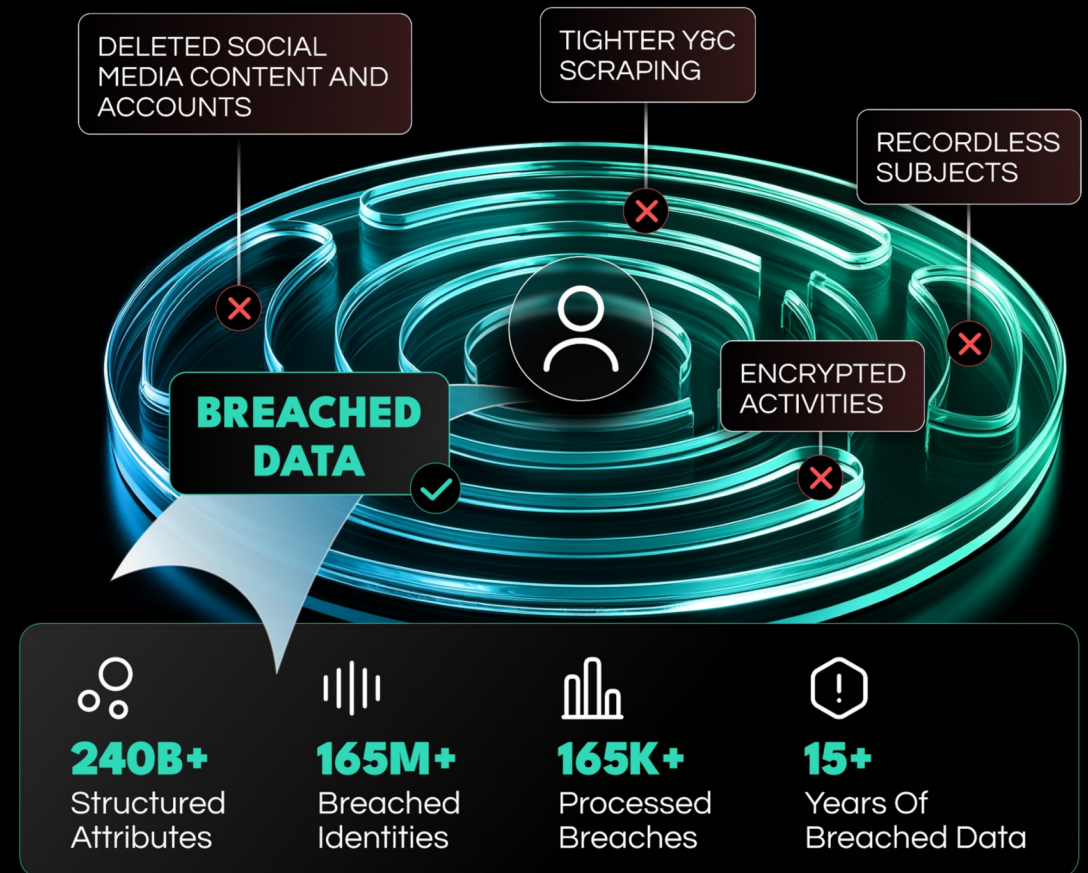
DATA LEAKS: A TREASURE TROVE FOR INVESTIGATIONS



Data leaks are an essential methods set for any type of intelligence, providing access to a wide range of confidential information, both personal and corporate.

Evidence and insights gained through breaches significantly expand the area of research.

Sometimes, a leak from a small food delivery service is what connects a phone number to a name and solves your case.



DATA LEAKS: HOW IT WORKS

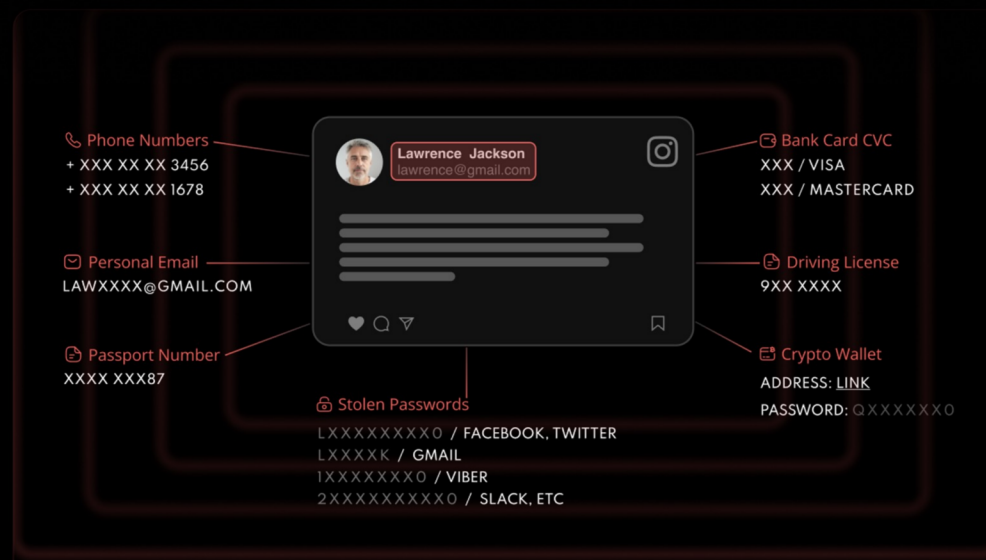


Imagine you've found **A PHONE NUMBER** on social media without further leads

Armed with this input, it's possible to extend the research chain to



Now it's possible to use found **EMAIL AND NAME** in further investigation



OBSERVE ANY CORNER OF THE DARK WEB

- Access hundreds of forums, marketplaces, and other sites across the Deep and Dark Web
- Monitor encrypted and password-protected content, indexed by entities, keywords, sites, and more
- Discover any threats from the Dark Web with standardized and structured data feeds

60%



An estimated 60% of all DarkNet data comes from sources that require some form of authenticated or account-level access.

ENTITY

- ALIAS (USERNAME) & PERSON (NAME)
- ✉ EMAIL ADDRESS
- ☎ PHONE NUMBER
- ₿ CRYPTOCURRENCY
- ✉ EMAIL DOMAIN
- 🌀 PRODUCTS
- 🗑 VENDORS
- 💬 COMMENTS & THREADS



TOR



DEEP WEB



TELEGRAM



DARK WEB MARKETPLACE



PASTE SITES



I2P
ANONYMOUS NETWORK



CLOSED FORUMS



ALTERNATIVE SOCIAL MEDIA PLATFORMS



250 Dark Web Forums



100 Dark Web Marketplaces
(Including Data Shops)



10,000 Telegram Channels & Groups



150 Ransomware Websites

DARK WEB DATA: HOW IT WORKS



SEARCH BY PHRASE: “WEED”

For example, you want to conduct a search across social media to find users posting relevant content



RELEVANT POST OR LISTING WITH DETAILS

Automated search can return all posts containing the relevant keyword



EXTRACT USERNAME, VENDOR, ETC.

From this post, you can extract alias, vendor, and other related information, to extend the investigation