



SAMPLE DELIVERABLE · ANONYMISED REAL DATA

EXPOSURE INTELLIGENCE REPORT · STEALER · RANSOMWARE · BREACHES

example.com

GLOBAL SUMMARY

905

 exposed services

Domain services in infostealer logs, plus the ransomware archives and data breaches that name the domain.

ONLY IN DARKEYE		
 INFOSTEALER LOGS	 RANSOMWARE	 BREACHES
251 domain services	51 third-party archives	603 data breaches
24,709 domain credentials 2,094 infected machines	677 people of the domain Data read inside the files that ransomware groups publish.	9,510 addresses of the domain

2026-10-16

EXPOSURE INTELLIGENCE REPORT

DARKEYE

SUBJECT	Exposure of example.com, its people and its services in infostealer logs, ransomware leak archives and data breaches. Risk analysis and remediation plan.
SCOPE	One domain and its subdomains; 251 distinct internal hosts observed.
TECHNICAL SOURCE	DarkEye records: infostealer logs, ransomware files and data breaches.
CLASSIFICATION	Sample on anonymised real data.



For additional information regarding DARKEYE, please visit: www.darkeye.io

Sample on anonymised real data

00 · THE FIRST THING TO KNOW

GLOBAL SUMMARY OF THE EXPOSURE

905 exposed services

The services and sources that expose the domain, in the order this report follows: infostealer logs, ransomware archives and data breaches. Each block gives the key figures for one source and, where there is one, its most serious finding.

04 INFOSTEALER LOGS

251 domain services

24,709 domain credentials
2,094 infected machines
7 stealer families
Lumma, Meduza, META, New family, RedLine, StealC, Vidar

MOST EXPOSED SERVICES		
app01.example.com	Administration and management	5,871
idp.example.com	Single sign-on	4,043
app02.example.com	Corporate mail	2,850
app03.example.com	Administration and management	2,413
app04.example.com	Corporate mail	1,066
WHO THE CREDENTIALS BELONG TO		
10,381 domain addresses	6,793 ID-number usernames	6,709 usernames only
664 external addresses	162 with no username	

MOST SERIOUS FINDING **CRITICAL** C-01 Single sign-on credentials in stealer logs: 4,057.

05 RANSOMWARE Data that can only be found on darkeye.io.

ONLY IN DARKEYE

51 third-party archives

677 people of the domain
2,136 records inside the files
7 ransomware groups
PUBLISHED
2023-04 – 2026-09

ARCHIVES NAMING THE MOST PEOPLE		
McGraw Hill, Inc. (mheducation.com)	shinyhunters · 28081	205
Arelance Group	medusa · 14625	144
Air Miles España, S.A	everest · 24186	110
TYPES OF DATA IN THE RECORDS		
IDENTITY	CONTACT	LOCATION
WORK AND STUDIES	CREDENTIALS	IDENTIFIERS
DATES		
OTHER		

MOST SERIOUS FINDING **CRITICAL** C-03
Domain email addresses in ransomware records: 677, across 51 sources. The most matches come from McGraw Hill, Inc. (mheducation.com) (shinyhunters).

06 BREACHES

603 data breaches

9,510 addresses of the domain
48,317 matching records
SOURCE DATES
2023-12 – 2026-09

BREACHES WITH THE MOST RECORDS		
hazteoir_org 4 de abril.sql.gz	15257a	5,210
hazteoir_org.sql.gz	4f2948	5,210
Dropbox_BF.7z	99cf45	3,577
TYPES OF DATA IN THE RECORDS		
IDENTITY	CONTACT	LOCATION
WORK AND STUDIES	CREDENTIALS	IDENTIFIERS
DATES		
OTHER		

MOST SERIOUS FINDING **SIGNIFICANT** C-08 Domain email addresses in breaches: 9,510.

Map of the report

Follow the trail from the first finding to the actions it calls for. The appendices hold the detail needed to check each conclusion.

NO.	PART	A QUESTION YOU MAY HAVE	WHAT YOU'LL FIND
00	The first thing to know	What is exposed, and where?	Every exposed service, source by source
What the search found			MOVEMENT 1 / 3
01	How to read the evidence	Where did we look?	Infected machines, leaked files and breaches
02	Exposure map	Which services appear in the data?	Services and accounts, grouped by source
03	The sources behind the findings	Where did the records come from?	Source families, in order, and their dates
What the records reveal			MOVEMENT 2 / 3
04	The machines behind the accounts	Which machines and services are involved?	Machines, services and available metadata
05	Inside the ransomware archives	What do the leaked files reveal about the domain?	The information found inside the main leaks
06	Which breaches carry the domain's addresses	Where have the domain's addresses appeared?	The main breaches, their records and what they contain
07	Which findings belong to this scope	Which matches should count?	How we separate relevant records
08	What the records cannot confirm	What still needs an internal check?	Questions the source data cannot settle
What to do with the findings			MOVEMENT 3 / 3
09	From exposed data to possible consequences	What could these findings mean together?	A scenario tied to specific findings
10	Risk scenarios	Which scenarios deserve attention first?	Probability × impact matrix
11	Action plan	What to do, in what order, at what cost?	Each finding → scenario → measure
12	Before closing the review	What would leave the exposure unresolved?	Before you close the report
13	Continuous monitoring	How will you know if this changes?	DarkEye alerts and API
Appendices verify every claim			EVIDENCE
A-D	Sources, method, scale, glossary	Where does each finding come from?	Evidence records, query log

What the search found

MOVEMENT 1 / 3

Sample on anonymised real data

This report was generated automatically from the live DarkEye corpus for a real organisation, as a preview of the format. Its domain has been replaced by example.com and sensitive values (documents, passwords, machine identifiers) are masked. Figures, findings and the third-party archives are real.

One domain, several places to look

Domain and subdomains	example.com and every *.example.com host
Internal hosts observed	251
Collections searched	Stealer logs, ransomware archives and breaches, in one index
Attribution	Confirmed by exact host; de-duplicated by content

What each source can tell us

VECTOR	WHAT IT TELLS US	DATES	WHAT IT CONTAINS	WHAT TO FOLLOW
Infostealer log	Which machine held the credential?	Log date, where available	One machine: login address, username, password, host	Services found on the same machine
Ransomware archive	What is inside the stolen documents?	Publication or discovery date	Each document: exports, spreadsheets, scans	The contents of each document
Data breach	Was this address in a database?	Date recorded by the source	An address, sometimes a password or hash	The other fields alongside the address

Exposure by service and source

We searched for example.com and its subdomains in stealer logs, ransomware archives and breaches. The results below are grouped by service and source.

SERVICE AREA	ENTITY	STEALER	RANSOMWARE	BREACH	WHAT WAS FOUND
Single sign-on	3 hosts	4,057	—	—	Check which services use this account and whether additional authentication is required.
VPN and remote access	2 hosts	643	—	—	Check whether these remote-access accounts remain active and how they are protected.
Corporate mail	10 hosts	4,412	—	—	Review the mailbox account, its sign-ins and any access to messages or contacts.
Administration and management	6 hosts	8,434	—	—	Check the account permissions and which records the management portal makes available.
Internal platforms	24 hosts	1,358	—	—	Check which internal records are available through these accounts.
Other services	206 hosts	5,805	—	—	
People and addresses	Domain addresses	—	677	9,510	Addresses associated with the domain in breaches and third-party ransomware archives.

Each source adds a different part of the picture.

Breaches show where addresses associated with the domain have appeared. Stealer logs also identify the services linked to captured credentials. The table brings these findings together.

»» See what was found and which source it came from.

Where the findings come from

Each family of sources is listed in the order this report follows: infostealer logs first, then ransomware archives and finally data breaches. The parts that follow open each one.

SOURCE FAMILY	SOURCES	NETWORK	WHAT IT EXPOSES	MAX. SEVERITY
Infostealer logs (Lumma, Meduza, META, New family, RedLine, StealC, Vidar)	2,094 machines	TELEGRAM · TOR	24,709 credentials for 251 internal hosts.	CRITICAL
Ransomware leak sites (shinyhunters, medusa, everest, play, clop +2) Only available on darkeye.io	51 archives	TOR	677 people with personal data read from documents.	CRITICAL
Traditional breaches and combolists	603 breaches	CLEAR	9,510 corporate addresses, many with a password.	SIGNIFICANT

Dates that put the findings in context

DATE	EVENT	SOURCE
2024-01	play publishes the archive of Televerde (42 people of the domain).	10362
2024-10	medusa publishes the archive of Arelance Group (144 people of the domain).	14625
2025-05	play publishes the archive of The Seydel Companies (22 people of the domain).	19664
2025-11	everest publishes the archive of Air Miles España, S.A (110 people of the domain).	24186
2026-01	shinyhunters publishes the archive of SoundCloud (29 people of the domain).	25719
2026-03	shinyhunters publishes the archive of European Commission (*.europa.eu): 15 people of the domain.	27648
2026-04	shinyhunters publishes the archive of McGraw Hill, Inc. (mheducation.com): 205 people of the domain.	28081
2026-08	shinyhunters publishes the archive of Questel SAS (12 people of the domain).	31161

»» The next step is to follow the credentials back to the machines.

What the records reveal

MOVEMENT 2 / 3

2,094 machines with exposed credentials for this domain



THE DETAIL TO FOLLOW

The machine groups the clues: which domain services appear together, which dates are recorded and what other service references the log contains.

The machine to review first – MX-01

Finding C-01. This log shows which services were associated with the machine.

MACHINE ID (FILENAME)	CREDENTIALS IN THE LOG 116
DOMAIN HOSTS IN THE LOG 36	

SERVICES FOUND	LOGIN DOMAINS	CREDS	SEVERITY
Single sign-on	idp.example.com	10	CRITICAL
VPN and remote access	vpn.example.com	1	CRITICAL
Administration and management	app05.example.com, app01.example.com, app03.example.com	15	SERIOUS
Corporate mail	app04.example.com, webmail.example.com	7	SERIOUS
Internal platforms	app06.example.com, app07.example.com, app08.example.com	5	SIGNIFICANT
Other services	app09.example.com, app10.example.com, app11.example.com	78	MINOR

Start by reviewing the accounts found in these logs.

Stealers collect login details from infected machines. The domains listed here help identify which accounts and services need to be checked.

Where to focus the machine review

MACHINE	MACHINE ID	FAMILY	LOG DATE	DOMAIN SERVICES	NOTE
MX-01		—	—	Single sign-on, VPN and remote access, Corporate mail, Administration and management, Internal platforms	116 credentials
MX-02		Meduza	2024-05-25	Single sign-on, VPN and remote access, Corporate mail, Administration and management, Internal platforms	76 credentials
MX-03		RedLine	2021-08-09	Single sign-on, VPN and remote access, Corporate mail, Administration and management, Internal platforms	64 credentials
MX-04		Meduza	2024-07-31	Single sign-on, VPN and remote access, Corporate mail, Administration and management	56 credentials
MX-05		Lumma	—	Single sign-on, VPN and remote access, Corporate mail, Administration and management, Internal platforms	51 credentials
MX-06		—	—	Single sign-on, VPN and remote access, Corporate mail, Administration and management	48 credentials
MX-07		Vidar	2023-01-03	Single sign-on, VPN and remote access, Corporate mail, Administration and management	48 credentials
MX-08		Lumma	2023-09-14	Single sign-on, VPN and remote access, Corporate mail, Administration and management	48 credentials

Other services found in these logs

We checked the files linked to the same machines for Steam, Telegram, wallets, FTP and VPN. These references describe what was found on those machines; they do not establish that the services belong to the organisation.

Logs checked: 2,094 / 2,094.

SERVICE	MACHINES	DOMAINS AND APPLICATIONS	EVIDENCE
Steam	862	Steam checkout.steampowered.com forums.steampowered.com help.steampowered.com steamcommunity.com steampowered.com 2 more domains	File listing Login domain Service record
Telegram	211	Telegram es.t.me web.telegram.org	File listing Login domain Service record
Wallets	150	Electrum MetaMask exchange.blockchain.com login.blockchain.com pit.blockchain.com	File listing Login domain Service record
FTP	49	ag.....com al.....com am.....com au.....com bd.....com 30 more domains	File listing Service record
VPN	407	NordVPN OpenVPN ProtonVPN 21.....com account.protonvpn.com ap.....com bb.....com ci.....es 53 more domains	File listing Login domain Service record

Up to five domains are shown for each service.

Machines with these references

Showing eight machines with the most relevant domain credentials.

MACHINE	SERVICES FOUND	LOG DATE	COUNTRY	STEALER FAMILY
MX-01	VPN	—	—	—
MX-02	Wallets, VPN	2024-05-25	ES	Meduza
MX-03	VPN	2021-08-09	ES	RedLine
MX-04	VPN	2024-07-31	ES	Meduza

MACHINE	SERVICES FOUND	LOG DATE	COUNTRY	STEALER FAMILY
MX-05	Steam, Telegram, Wallets, VPN	—	ES	Lumma
MX-06	Steam, Telegram, VPN	—	ES	—
MX-07	VPN	2023-01-03	—	Vidar
MX-08	Steam, Telegram, VPN	2023-09-14	ES	Lumma

A file listing shows that a related file or folder was present. A service record or login domain provides additional evidence. Only domains and metadata are shown.

The trail continues inside the leaked files.



THE DETAIL TO FOLLOW

The useful detail is inside the records. Read each summary alongside its source to see what information accompanies the domain's email addresses.

An email address can appear in files published under another organisation's name. Here we follow those references into the records and summarise what accompanies them.

SOURCE	GROUP	ORGANISATION NAMED IN THE LEAK	PUBLISHED	DOMAIN ADDRESSES	WHAT APPEARS IN THE RECORDS
28081	shinyhunters	McGraw Hill, Inc. (mheducation.com)	2026-04-12	205	Email references; see the sample summary for detail.
14625	medusa	Arelance Group	2024-10-08	144	Personal data read from the documents: academic record, age, city, date of birth, employer, first name, phone number, postal code.
24186	everest	Air Miles España, S.A	2025-11-24	110	Email references; see the sample summary for detail.
10362	play	Televerde	2024-01-06	42	Personal data read from the documents: city, country, employer, first name, job title, phone number, postal code, surname.
25719	shinyhunters	SoundCloud	2026-01-23	29	Email references; see the sample summary for detail.
19664	play	The Seydel Companies	2025-05-01	22	Email references; see the sample summary for detail.
27648	shinyhunters	European Commission (*.europa.eu)	2026-03-28	15	Email references; see the sample summary for detail.
31161	shinyhunters	Questel SAS	2026-08-02	12	Email references; see the sample summary for detail.
23703	clop	CSCGLOBAL.COM	2025-10-27	11	Email references; see the sample summary for detail.
6034	medusa	Open University of Cyprus	2023-04-06	9	Personal data read from the documents: country.

SOURCE	GROUP	ORGANISATION NAMED IN THE LEAK	PUBLISHED	DOMAIN ADDRESSES	WHAT APPEARS IN THE RECORDS
12985	play	Air Cleaning Specialists	2024-06-12	9	Email references; see the sample summary for detail.
13284	medusa	Viasat	2024-07-07	9	Personal data read from the documents: city, employer, first name.

The table shows the archives with the most addresses of the domain. In this sample, only those archives have a summary below; the full report includes one for every archive.

What we found in these records

Each summary is based on up to five records from the leak.

01 McGraw Hill, Inc. (mheducation.com) shinyhunters 205 people of the domain2026-04-12 The records include contact details for five people, with roles such as Instructor, business unit SEM, country Spain, phone numbers, and dates from 2021 and 2023. Currency codes and salutation preferences are also present in the populated data. FIELDS IN THE RECORDS CONTACT email CREDENTIALS password or hash IDENTIFIERS numeric id DATES date OTHER text Source · 28081	5 records reviewed
02 Arelance Group medusa 144 people of the domain2024-10-08 Records include names, emails, and location details like city, state, postal code, and country. Documents contain references to HTML and text files alongside these contact and geographic entries. FIELDS IN THE RECORDS IDENTITY user name edad nombre nombrefichero CONTACT email email correcto telfijo telfijo2 telmovil LOCATION ciudad WORK AND STUDIES formacion titulacion DATES fecha nac OTHER responsable dominio id candidato categoria text carpeta Source · 14625	5 records reviewed

03 Air Miles España, S.A

everest

5 records reviewed

110 people of the domain 2025-11-24

The records contain five entries sharing identical communication and action codes, all with an incoming date of 11/11/2025. Fields include customer and line identifiers, names, postal codes, subject codes, and placeholder values for several operational fields.

FIELDS IN THE RECORDS IDENTIFIERS numeric id OTHER text

Source · 24186

04 Televerde

play

5 records reviewed

42 people of the domain 2024-01-06

Records include contact identifiers, names, company names, country data, account identifiers, and problem descriptions. One record has a stream value, and dates appear only in document filenames, not in the records themselves.

FIELDS IN THE RECORDS IDENTITY first name last name account name CONTACT mailing country phone account phone LOCATION country billing country billing city WORK AND STUDIES company title OTHER contactid eloqua contact id contact id account id contact owner account owner industry data source list source

Source · 10362

05 SoundCloud

shinyhunters

5 records reviewed

29 people of the domain 2026-01-23

Five SoundCloud user profiles include details like names, usernames, profile links, avatar images, dates of creation and updates, follower and following counts, like counts, subscription type, and artist station identifiers. All five records show free creator subscriptions, no verified status, no comments or playlists, and dates spanning from 2012 to 2019.

FIELDS IN THE RECORDS IDENTIFIERS numeric id DATES date OTHER text

Source · 25719

06 The Seydel Companies

5 records reviewed

play

22 people of the domain 2025-05-01

We could not produce a reliable summary of these records.

FIELDS IN THE RECORDS CONTACT email OTHER text

Source · 19664

07 European Commission (*.europa.eu)

5 records reviewed

shinyhunters

15 people of the domain 2026-03-28

Multiple email messages were sent from various senders to two recipients, each with a recorded time. Each message included a subject line, sender label, and related details from the email content.

FIELDS IN THE RECORDS CONTACT email IDENTIFIERS numeric id OTHER text

Source · 27648

08 Questel SAS

5 records reviewed

shinyhunters

12 people of the domain 2026-08-02

Records include contact details such as names, job titles, companies, locations, communication preferences, identifiers, and dates for creation or modification. Several entries also show activity dates, match statuses, owner names, and source information.

FIELDS IN THE RECORDS CREDENTIALS password or hash IDENTIFIERS numeric id DATES date OTHER text

Source · 31161

09 CSCGLOBAL.COM

5 records reviewed

clop

11 people of the domain 2025-10-27

The sample contains email addresses, unlabelled numeric values and dates from 2014.

FIELDS IN THE RECORDS IDENTITY client name CONTACT email email cadm email cfac email cli LOCATION cod.postal cadm cod.postal cfac cod.postal cli cod.postal tit IDENTIFIERS numeric id DATES date OTHER acceso cli c.administrativo c.facturacin cod. dominio direccin cadm direccin cfac direccin cli direccin tit dominio

Source · 23703

10

Open University of Cyprus

medusa

5 records reviewed

9 people of the domain 2023-04-06

Records include Erasmus details: contact information, website links, academic programs, disability support services, mobility and insurance contacts, plus one email from another archive. They cover academic years from 2021/2022 through 2028/2029.

FIELDS IN THE RECORDS	IDENTITY	name	contact person name	name of institution	CONTACT	email		
		contact telephone						
	LOCATION	country	WORK AND STUDIES	sms academic fiels	sta academic fiels	IDENTIFIERS		
	numeric id	DATES	date	date of departure	OTHER	text	contact fax	id
key action	signed agreement		smp agreed positions	sms agreed positions				

Source · 6034

11

Air Cleaning Specialists

play

5 records reviewed

9 people of the domain 2024-06-12

The sample contains email addresses.

FIELDS IN THE RECORDS	CONTACT	email

Source · 12985

12

Viasat

medusa

5 records reviewed

9 people of the domain 2024-07-07

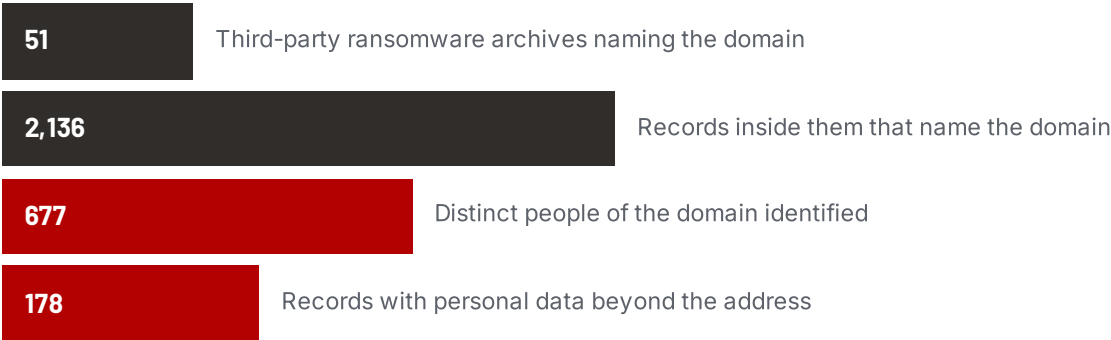
The records include client names, phone numbers, country codes, payment terms, credit limits, and modification dates. All entries have zero balances, pending service invoices, and payment methods of transfer and receipt.

FIELDS IN THE RECORDS	IDENTITY	name	CONTACT	additional phone no 1	additional phone no 2	LOCATION	cpi	
	address	city	country_region code	WORK AND STUDIES	company	OTHER	alias	vat registration no_
	bill-to customer no_	blocked	bloqueado	c.p.	comentario	compañía	contact	contacto
cód. divisa								

Source · 13284

From archives to people

The figures below show how the files relate to the domain.



A closer look at the types of data

These field names help check the summaries against the structure of the original records.

SOURCE	FIELDS PRESENT IN THE RECORDS
28081	CONTACT email CREDENTIALS password or hash IDENTIFIERS numeric id DATES date OTHER text
14625	IDENTITY user name edad nombre nombrefichero CONTACT email email correcto telfijo telfijo2 telmovil LOCATION ciudad WORK AND STUDIES formacion titulacion DATES fecha nac OTHER responsable dominio id candidato categoria text carpeta
24186	IDENTIFIERS numeric id OTHER text
10362	IDENTITY first name last name account name CONTACT mailing country phone account phone LOCATION country billing country billing city WORK AND STUDIES company title OTHER contactid eloqua contact id contact id account id contact owner account owner industry data source list source
25719	IDENTIFIERS numeric id DATES date OTHER text
19664	CONTACT email OTHER text
27648	CONTACT email IDENTIFIERS numeric id OTHER text
31161	CREDENTIALS password or hash IDENTIFIERS numeric id DATES date OTHER text
23703	IDENTITY client name CONTACT email email cadm email cfac email cli LOCATION cod.postal cadm cod.postal cfac cod.postal cli cod.postal tit IDENTIFIERS numeric id DATES date OTHER acceso cli c.administrativo c.facturacin cod. dominio direccin cadm direccin cfac direccin cli direccin tit dominio

SOURCE

6034

IDENTITY

name

contact person name

name of institution

CONTACT

email

contact telephone

LOCATION

country

WORK AND STUDIES

sms academic fiels

sta academic fiels

IDENTIFIERS

numeric id

DATES

date

date of departure

OTHER

text

contact fax

id

institution website

key action

signed agreement

smp agreed positions

sms agreed positions

12985

CONTACT

email

13284

IDENTITY

name

CONTACT

additional phone no 1

additional phone no 2

LOCATION

cpi

address

city

country_region code

WORK AND STUDIES

company

OTHER

alias

vat registration no_

bill-to customer no_

blocked

bloqueado

c.p.

comentario

compañía

contact

contacto

county

cód. divisa

»» Breaches complete the picture: where the domain’s addresses have appeared.

603 data breaches carry addresses of the domain

Each row shows a breach containing addresses associated with the domain and how many were found. The summaries below explain what other information appears alongside them.

SOURCE	BREACH	COUNTRY	DATE	MATCHING RECORDS
15257a	hazteoir_org 4 de abril.sql.gz		2024-04-07	5,210
4f2948	hazteoir_org.sql.gz		2024-04-07	5,210
99cf45	Dropbox_BF.7z		2026-01-30	3,577
5041d9	VerificationsIO_BF.7z.011		2025-12-03	3,204
39563b	Apollo.io DB 816millions.rar	IO	2025-05-30	2,436
f24bb4	pureincubation-com.7z.001	CU	2026-05-11	2,102
4d9634	Full Clouds Cit0day_2.7z.001		2024-03-25	1,463
fa8569	Cit0day [cit0day.in] breaches.csv		2025-03-31	1,380
6243a2	OnlinerSpambot_BF.7z		2026-01-30	1,109
617316	AntiPublic_BF.7z		2026-01-30	1,071
2ea724	ANTIPUBLIC #1.tar.zip.001		2024-03-11	850
08c010	Exploit.in.rar	IN	2025-03-31	830

The table shows the breaches with the most records. In this sample, only those breaches have a summary below; the full report includes one for every breach.

Types of data found

These labels describe the information in the records. Where column names are missing, we show the type of data we could recognise.

IDENTITY

birth_date

CONTACT

email

email_lower_sha256

LOCATION

city

province

CREDENTIALS

password or hash

IDENTIFIERS

numeric id

DATES

date

OTHER

text

done

bcn

comunicacion_ph

What we found in these records

Each summary is based on up to five records from the leak.

01

hazteoir_org 4 de abril.sql.gz

DBs Backup

5,210 matching records2024-04-07

5 records reviewed

All entries come from the same document source and have no alerts or events.

FIELDS IN THE RECORDS

CONTACT

email

IDENTIFIERS

numeric id

DATES

date

OTHER

text

Source · 15257ad02463

02

hazteoir_org.sql.gz

DBs Backup

5,210 matching records2024-04-07

5 records reviewed

Five timestamps from a MAX(created) query span 2013-09-08 to 2015-08-05, all linked to the document transformed_JSONL_file_ultimafirma-MySQL_file.part06.

FIELDS IN THE RECORDS

CONTACT

email

IDENTIFIERS

numeric id

DATES

date

OTHER

text

Source · 4f294816734d

03

Dropbox_BF.7z

B F R e p o V 3 F i l e s

3,577 matching records2026-01-30

5 records reviewed

Five records pair email addresses with encrypted data strings and document filenames. The documents consist of multiple TXT files and one numbered file, containing no personal identifiers besides the emails.

FIELDS IN THE RECORDS

CONTACT

email

CREDENTIALS

password or hash

OTHER

text

Source · 99cf4513df68

04

VerificationsIO_BF.7z.011

Kedr | Forum 🌿

3,204 matching records2025-12-03

5 records reviewed

The records include five entries from a transformed JSONL file. Each entry has a unique identifier, a status value of "1.0", and a hashed email value. No names, emails, or other personal details are included.

FIELDS IN THE RECORDS

IDENTITY

firstname

lastname

dob

CONTACT

email_lower_sha256

phone

LOCATION

city

state

zip

country

OTHER

done

fax

mobile

Source · 5041d95dd8a3

05

Apollo.io DB 816millions.rar

5 records reviewed

Database World ROC

2,436 matching records

2025-05-30

IO

The records include personal details such as names, job titles, normalized roles, organizations, locations (city, region, country, postal codes), employment start dates, professional connection counts, relevance scores, and processing timestamps.

FIELDS IN THE RECORDS

CONTACT

email

CREDENTIALS

password or hash

IDENTIFIERS

numeric id

DATES

date

OTHER

text

Source · 39563b88cb93

06

pureincubation-com.7z.001

5 records reviewed

Database World ROC

2,102 matching records

2026-05-11

CU

The records include contact details, organizational information, names with roles and departments, addresses with postal codes, activity dates, company names, job titles, salary ranges, industry classifications, and source domains.

FIELDS IN THE RECORDS

IDENTIFIERS

numeric id

DATES

date

OTHER

text

Source · f24bb4c92e51

07

Full Clouds Cit0day_2.7z.001

5 records reviewed

DBs w MTDT

1,463 matching records

2024-03-25

Each record links an email address to a short alphanumeric code and a TXT file with numerical values and hash/no-hash markers. The files cover multiple domains and use varied names.

FIELDS IN THE RECORDS

CONTACT

email

CREDENTIALS

password or hash

IDENTIFIERS

numeric id

DATES

date

OTHER

text

Source · 4d9634e986a8

08 Cit0day [cit0day.in] breaches.csv

5 records reviewed

LKnet reserve chat

1,380 matching records 2025-03-31

Five records pair email addresses with short text values and document filenames. Some filenames share identical numerical scores and hash markers across multiple entries.

FIELDS IN THE RECORDS CONTACT email CREDENTIALS password or hash IDENTIFIERS numeric id DATES date OTHER text

Source · fa856950467a

09 OnlinerSpambot_BF.7z

5 records reviewed

B F R e p o V 3 F i l e s

1,109 matching records 2026-01-30

The sample contains email addresses.

FIELDS IN THE RECORDS CONTACT email CREDENTIALS password or hash IDENTIFIERS numeric id OTHER text

Source · 6243a2c19cdd

10 AntiPublic_BF.7z

5 records reviewed

B F R e p o V 3 F i l e s

1,071 matching records 2026-01-30

Each record links an email address to a string identifier and a specific numbered TXT file document. The documents use sequential numbering with different prefixes.

FIELDS IN THE RECORDS CONTACT email CREDENTIALS password or hash IDENTIFIERS numeric id DATES date OTHER text

Source · 617316111f74

11 ANTIPUBLIC #1.tar.zip.001

5 records reviewed

DBs Backup

850 matching records 2024-03-11

Records pair email addresses with alphanumeric or text labels and document filenames with numeric codes.

FIELDS IN THE RECORDS CONTACT email CREDENTIALS password or hash IDENTIFIERS numeric id DATES date OTHER text

Source · 2ea7246dcce1

12

Exploit.in.rar

LKnet reserve chat

5 records reviewed

830 matching records 2025-03-31 IN

The records link email addresses to alphanumeric codes and document filenames. Documents reference numbered TXT files, with codes varying in format and length; no personal identifiers beyond these email-code pairs exist.

FIELDS IN THE RECORDS

CONTACT

email

CREDENTIALS

password or hash

IDENTIFIERS

numeric id

DATES

date

OTHER

text

Source · 08c0104283c5

»» The records show what is exposed. The next question is what that information could make possible.

07 · WHICH FINDINGS BELONG TO THIS SCOPE

DARKEYE · HOST-LEVEL ATTRIBUTION

Which findings belong to this scope

A machine can contain accounts for many services. We separate the domain's credentials from the other references, so the totals describe the scope being investigated.

ITEM ENCOUNTERED	VERDICT
Accounts for other services found on the same machines.	Shown as context where relevant. Only credentials linked to the domain count towards its totals.
A host contains the domain name but is not part of that domain.	Excluded from the totals: the host must match the domain or one of its subdomains.

››› **A useful finding needs a clear link to the domain.**

08 · WHAT THE RECORDS CANNOT CONFIRM

CHECKS TO COMPLETE INTERNALLY

What the records cannot confirm

The records establish exposure. Some questions can only be answered by comparing them with your own systems.

QUESTION TO RESOLVE	HOW TO CHECK IT
Are the exposed accounts still active?	Compare the records with the identity directory and password-reset history.
Who manages each machine?	Match the available metadata with the device inventory and responsible team.
Has any exposed information been used?	Review authentication and security events around the recorded dates.

No result means no match was found in the sources checked. It does not rule out exposure elsewhere.

What to do with the findings

MOVEMENT 3 / 3

How these findings could connect

Consider the findings together. The sequence below illustrates possible consequences if the accounts remain usable or the information is misused; it is not a reconstruction of an observed attack.

- 01 ● A domain account appears in a log** · C-01
The record links a credential to a service. The first check is whether the account remains active and protected.
- 02 ● Remote access needs attention** · C-02
If the VPN credential remains usable, its permissions and additional authentication controls determine the exposure.
- 03 ● One account may connect several services** · C-01
Check which applications the single sign-on account can reach and whether its active sign-ins have been revoked.
- 04 ● The leaked records add context** · C-03
Contact details and other recorded information can make an impersonation attempt more convincing. Review what the samples actually contain before assessing that risk.

WHERE TO INTERVENE

Start with the linked account-protection measures: M-01, M-03, M-02.

Assign an owner, check the account status and record the action taken.

Which consequences deserve attention first?

These scenarios help prioritise the response. Each one points back to the findings that support it.

	SCENARIO	MECHANISM	FINDINGS	PROB.	IMPACT	MEASURES
A	Account takeover and lateral movement	If the credentials still work, they could allow access to the account and connected services. Check account status and authentication controls.	C-01, C-04, C-05, C-07	High	Very high	M-01, M-02, M-05
B	Remote network intrusion	Remote access may be possible if the account remains active and its access controls do not stop the sign-in.	C-02	High	High	M-01, M-03
C	Impersonation and fraud by mail	Exposed contact details may make a fraudulent message more convincing, including requests to change payment details.	C-04	Medium	High	M-02, M-06
D	Misuse of personal information	Personal details in the leaked records could support impersonation. The possible misuse depends on the information present.	C-03, C-05, C-09	Medium	High	M-07, M-08
E	Reused passwords tried on other services	An exposed username and password may also work on another service if they were reused.	C-06, C-08	High	Medium	M-01, M-04

Compare the scenarios

	Moderate impact	High impact	Very high impact
HIGH PROBABILITY	E	B	A
MEDIUM PROBABILITY		C D	
LOW PROBABILITY			

- Start with the scenarios that combine greater potential impact and fewer conditions for misuse.
- Use the linked finding codes to see which evidence supports each scenario.
- Personal information needs a different response from a password: assess the scope and consider protection against misuse.

11 · ACTION PLAN

EACH FINDING → A SCENARIO → A MEASURE

Eight measures, seven within fifteen days

Assign an owner and a deadline to each action. Start with the accounts and machines linked to the most serious findings, then record what has been resolved.

IMMEDIATE: WITHIN 72 HOURS

NO.	MEASURE	OWNER	TIMING	COST	SCEN.
M-01	Force a password reset and phishing-resistant MFA on every account seen in a stealer log; revoke active sign-ins.	CISO	72 h	Low	A, B, E
M-02	Enforce MFA on mail and single sign-on, and alert finance and administration teams to the impersonation pretexts found.	CISO	72 h	Low	A, C
M-03	Rotate VPN and remote-access credentials and require MFA on every remote entry point.	Network team	72 h	Low	B

WITHIN 15 DAYS

NO.	MEASURE	OWNER	TIMING	COST	SCEN.
M-05	Hunt the infected machines across the fleet, re-image them and confirm the new credentials are not leaking again.	SOC	15 d	Medium	A
M-07	Notify the people whose identity data is in the archives and offer them a fraud-alert service.	DPO	15 d	Medium	D
M-08	Open the breach file with each affected provider: notification status, data scope, deletion of obsolete extracts.	DPO, legal	15 d	Low	D
M-04	Ban reused and trivial passwords; detect and reset shared passwords seen across many machines.	CISO	15 d	Low	E

SHORT TERM: ONE TO THREE MONTHS

NO.	MEASURE	OWNER	TIMING	COST	SCEN.
M-06	Out-of-band dual validation for any change of bank details, incoming or outgoing.	Finance	1 month	Low	C

From finding to measure

This table connects the evidence to the proposed response. Use it to track which finding each action addresses.

FINDING	WHAT IS CIRCULATING	FEEDS	ADDRESSED BY	FIRST DEADLINE
C-01	Single sign-on credentials in stealer logs	A	M-01, M-02, M-05	72 hours
C-02	VPN and remote-access credentials in stealer logs	B	M-01, M-03	72 hours
C-03	Domain email addresses in ransomware records	D	M-07, M-08	72 hours
C-04	Corporate-mail credentials in stealer logs	A, C	M-01, M-02, M-05, M-06	15 days
C-05	Matching email addresses link stealer logs with other sources	A, D	M-01, M-02, M-05, M-07, M-08	15 days
C-06	Passwords repeated across at least ten machines	E	M-01, M-04	15 days
C-07	8,434 credentials for administration and management portals exposed	A	M-01, M-02, M-05	15 days
C-08	Domain email addresses in breaches	E	M-01, M-04	15 days
C-09	Credentials for internal platforms	D	M-07, M-08	15 days

Regulatory perspective

The table lists the texts to be examined. It does not constitute legal advice.

TEXT	WHAT IT REQUIRES	RELATED FINDINGS
GDPR, Art. 33 and 34	Breach notification within 72 hours of awareness; information to data subjects when risk is high.	stealer and ransomware findings
GDPR, Art. 28 and 33(2)	Processors (the breached providers) must notify the controller without undue delay.	ransomware findings
GDPR, Art. 32	Security of processing, including endpoint protection of staff devices.	stealer findings
NIS2 Directive, Art. 21 and 23	Supply-chain security and incident reporting.	ransomware findings

Avoid leaving the job half done

APPROACH	WHY IT FAILS
Relying only on a removal request	A removal request does not establish whether copies remain elsewhere.
Reviewing only breach passwords	Stealer records can point to additional accounts and machines that also need review.
Resetting a password without cleaning the machine	If the infection remains, a new password may also be captured.
Waiting for the archives to disappear	Published files may be copied and redistributed after the original post disappears.

A password change and a machine check belong in the same response. Published personal information also needs follow-up, even after the accounts are secured.

Questions to ask internally

- 01 Have the exposed accounts been identified and protected with MFA?
- 02 Is single sign-on protected by phishing-resistant MFA today?
- 03 Which source machines have been identified and checked?
- 04 Which suppliers in the ransomware archives handle the domain's data?
- 05 Are personal devices allowed to hold corporate credentials?
- 06 Who is alerted when a new machine with a domain credential appears?

How to tell whether the response is working

The response should leave a record: accounts secured, machines checked and new appearances investigated. These indicators make progress visible at the next review.

MONITORED ITEM	WHAT TRIGGERS THE ALERT	SEVERITY	RECIPIENT
The domain and its subdomains	New credentials or leaked records linked to the domain.	CRITICAL	CISO
Single sign-on and VPN login addresses	A new credential for one of these services.	CRITICAL	CISO
Machine identifiers already seen	New records from a known machine; check whether the infection persists or has returned.	SERIOUS	SOC
Strategic suppliers	A supplier appears in a new ransomware publication.	SERIOUS	CISO

What to check at the next review

INDICATOR	VALUE AS OF 2026-10-16	TARGET
Domain credentials from stealer logs	24,709	Reset within 72 hours
Infected machines with a domain credential	2,094	Cleaned and monitored
Ransomware archives naming the domain	51	Beyond the domain's control
People exposed in archives	677	Notified and fraud-protected

THE NEXT REVIEW SHOULD SHOW WHAT HAS CHANGED.

Record which accounts have been secured, which machines have been checked and which questions remain open.

Summary of findings

NO.	SEVERITY	VECTOR	FINDING	SOURCE	STATUS	CONFID.
C-01	CRITICAL	STEALER	Single sign-on credentials in stealer logs: 4,057.	Stealer logs	Online	Confirmed
C-02	CRITICAL	STEALER	VPN and remote-access credentials in stealer logs: 643.	Stealer logs	Online	Confirmed
C-03	CRITICAL	RANSOMWARE	Domain email addresses in ransomware records: 677, across 51 sources. The most matches come from McGraw Hill, Inc. (mheducation.com) (shinyhunters).	Ransomware	Online	Confirmed
C-04	SERIOUS	STEALER	Corporate-mail credentials in stealer logs: 4,412.	Stealer logs	Online	Confirmed
C-05	SERIOUS	CROSS-VECTOR	Matching email addresses link stealer logs with other sources: 71.	Cross-vector	Online	Confirmed
C-06	SERIOUS	STEALER	Passwords repeated across at least ten machines: 53.	Stealer logs	Online	Confirmed
C-07	SERIOUS	STEALER	8,434 credentials for administration and management portals exposed.	Stealer logs	Online	Confirmed
C-08	SIGNIFICANT	BREACH	Domain email addresses in breaches: 9,510.	Breaches	Online	Confirmed
C-09	SIGNIFICANT	STEALER	Credentials for internal platforms: 1,358.	Stealer logs	Online	Confirmed

Review date: 2026-10-16. Finding codes link the evidence to the scenarios and actions. Appendix C explains the ratings.

Source register

CODE	SOURCE	NETWORK	PUBLICATION	STATUS	FINDINGS
S-01	Infostealer log channels and markets	TELEGRAM · TOR	—	Online	stealer findings
S-02	shinyhunters leak site · McGraw Hill, Inc. (mheducation.com)	TOR	04.2026	Online	C-03
S-03	medusa leak site · Arelance Group	TOR	10.2024	Online	C-03
S-04	everest leak site · Air Miles España, S.A	TOR	11.2025	Online	C-03
S-05	play leak site · Televerde	TOR	01.2024	Online	C-03
S-06	shinyhunters leak site · SoundCloud	TOR	01.2026	Online	C-03
S-07	play leak site · The Seydel Companies	TOR	05.2025	Online	C-03
S-08	shinyhunters leak site · European Commission (*.europa.eu)	TOR	03.2026	Online	C-03
S-09	shinyhunters leak site · Questel SAS	TOR	08.2026	Online	C-03
S-10	Breach compilations and combolists	CLEAR	—	Online	breach findings

An evidence record, as exported

This record shows how a finding is linked to its source. Sensitive identifiers are masked.

Finding and source	C-01 · most exposed machine · stealer logs
Machine	
Credentials	116
Internal hosts	36

Method, queries and limitations

Search date: 2026-10-16. Domain credentials are matched by host and grouped by their log identifier. Repeated credential sets are grouped by content. The leak summaries use up to five records per source; they describe those samples.

NO.	COLLECTION	QUERY	PURPOSE	RESULT
01	Stealer	domain example.com	Machines and credentials	24,709
02	Ransomware	domain example.com	People in archives	677
03	Breach	domain example.com	Addresses in breaches	9,510

How we keep the findings relevant

1. The search starts with the domain and its subdomains. Matches are reviewed in that context.
2. The report uses records already held in the collected sources. It does not test the exposed credentials against services.
3. Domain credential counts use exact host or subdomain matches. Duplicate credential sets are grouped by content.
4. The report summarises the evidence using counts, domains and metadata. Passwords and full personal records are not displayed.

A method validated in peer-reviewed research

The extraction of personal data from ransomware archives — documents, spreadsheets, SQL dumps and scans — follows a methodology published in an academic journal (DOI: [10.3390/electronics14214327](#)).

Limitations

- The sources checked do not cover every place where information may circulate. No match in this search does not prove there is no exposure.
- Private forums that require an invitation are outside this search.
- Credentials are grouped by machine and repeated sets are deduplicated by content.
- Scanned documents are read with OCR. Poor image quality can leave some text unread.

APPENDIX C · RATING SCALE

FOUR-LEVEL SCALE

Rating scale

LEVEL	DEFINITION	EXAMPLE IN THIS REPORT
CRITICAL	Exposure prioritised for immediate review because of the affected service or potential consequences.	A single sign-on or VPN credential whose status needs checking.
SERIOUS	Information that could support account misuse or make impersonation more credible.	A corporate mailbox, a reused administrator password.
SIGNIFICANT	Signal to investigate or partial exposure.	Addresses in a breach, internal credentials.
MINOR	Low-sensitivity information that completes a profile.	Generic addresses with no associated secret.

CONFIDENCE	DEFINITION
Confirmed	The record was read in full context and its link to the scope is established.
Probable	The record was read; ownership of the device or account cannot be fully verified from the source.
To confirm	The link to the scope is not established. An internal check will settle it.

Probability: A qualitative estimate of the conditions needed for a scenario to occur. It is not a measured frequency.

Impact: The potential consequences for accounts, services and people if the scenario occurs.

APPENDIX D · GLOSSARY

Glossary

TERM	DEFINITION
Infostealer	Malware that collects login details and other information from a machine. Examples include Lumma, RedLine, Vidar and StealC.
Stealer log	A set of records collected by an infostealer, which may include login details and machine metadata.
HWID	A machine identifier that helps relate records from the same computer.
Ransomware leak site	A site used to publish information about ransomware victims and leaked files.
Document parsing	Reading the contents of a leaked file to identify the information it contains.
Pivot by value	Searching for the same value in other sources to connect related records.
Credential stuffing	Automated testing of leaked login/password pairs against other services.

Created by DarkEye

**FOLLOW THE
EVIDENCE.
DECIDE WHAT
COMES NEXT.**

Connect the accounts, machines and leaked records that matter to your organisation.

Use the findings to focus your response and track what changes over time.

