// PERSONAL OSINT SELF-AUDIT — ATTACKER'S-VIEW ASSESSMENT

DIGITAL FOOTPRINT & EXPOSURE REPORT

Outward Lens · Intelligence-Dossier Edition · Full sample report

SUBJECT	Daniel Kessler · dkessler@gmail.com (fictional persona)
SCOPE	subject + household (spouse identifiers included, masked)
REPORT DATE	12 September 2026
PERSPECTIVE	external researcher — public data + licensed leak intel only
REPORT ID	DFER-SAMPLE-001 (fictional subject, invented data)
EDITION	Full sample report · fictional case



SAMPLE REPORT - FICTIONAL SUBJECT. All names, data and findings are invented.

No plaintext passwords or raw breach records appear in this document. All credentials are masked. All person data is fictional.

WHAT THE INTERNET KNOWS ABOUT YOU

*Everything below was assembled from **public sources and leaked data only**. No access to any of your accounts was used. **An attacker can produce this page for $0–50.** (Sample: the subject is fictional.)*



self-published headshot · face-search score 96/100

FULL NAME	**Daniel Kessler** — consistent across registry filings, delivery-leak records and public profiles	*äriregister.ee · Bringma leak*
DATE OF BIRTH	**14.03.1990** — leak-confirmed; also public on your dev.to profile	*Bringma leak + dev.to*
CITIZENSHIP	German — beneficial-owner declarations re-filed publicly every year 2024→2026	*äriregister.ee*
ROLE	Founder, Kessler Labs OÜ (product: Cachehawk) · ex-Staff Engineer, Northwind Analytics	*TheOrg · your sites*

FAMILY & HOUSEHOLD

WIFE	Marta Kessler (née Nowak; DOB 1988) · m****.n****@gmail.com (3 breaches, incl. Canva 2019) · m******@gmx.de (plaintext password, 8+ combolists) · +48 *** ** ** 12 · 10 leak files / 3 HIBP breaches	*Canva 2019 · edu-portal DB · combolists*
CHILDREN	one daughter, born ~2019 — **her name is not found in any source — yet**; enrollment implied by a school-portal record	*spouse leaks · absence verified*
CROSS-LINK	her phone sits inside YOUR delivery record; your emails inside HER broker profile — the data joins the couple in both directions	*leak-data joins*

LOCATION TIMELINE

ERA	WHERE — DOWN TO GPS + DOOR CODES	SOURCE
2013–2017	Munich — Hohenzollernstraße 112, 80799 München (48.1563, 11.5489) · Türkenstraße 54 apt 7 (48.1522, 11.5741 — delivery note: 'door code 4***')	*Bringma delivery leak*
2018–2020	Warsaw — ul. Hoza 51 apt 12, 00-681 Warszawa (52.2251, 21.0138)	*broker residue*
2016-ERA IPS	85.214.132.40 + 78.47.219.55 anchor the Munich era (residential DSL + self-hosted VPS)	*Bringma · forum DB*
2021 →	Lisbon — billing city in merchant databases (your own leak-intel account profile proves merchants hold it)	*merchant DBs*
RESIDUE	'Lisboa' leaks from 'GDPR-redacted' WHOIS on all 3 Cloudflare domains — a city-grade current-location signal	*live RDAP/WHOIS*
ENTITY	Tartu mnt 43, Tallinn 10128 — registered address of Kessler Labs OÜ, re-confirmed on your own /legal page	*Estonian e-register*

PHONES & EMAILS

MAIN PHONE	**+49 151 2377 4810** — in 3 scraped datasets (WhatsApp DE scrape, Telegram 50M directory, ID↔phone map); the join key to everything above	*raw leak index*
SECOND	+48 *** ** ** 12 — your wife's number, carried inside YOUR leaked delivery record	*Bringma leak*
EMAILS	**dkessler@gmail.com** — 41 catalogued breaches · **dkess@gmx.net** — 12 dump files, stealer-harvested · **daniel@kesslerlabs.dev** — 2026 lead-gen DBs · + wife's two (masked)	*HIBP · raw index · lead-gen DBs*

DIGITAL IDENTITY

TELEGRAM	@danielkessler · ID 48151623 — permanently bound to your phone in 3 directory scrapes; 812 hit blocks across 320 circulating files	*TG scrapes / raw index*
HANDLES	GitHub dkess (since 2013) · HN danielkessler (9 yrs, karma 812) · Reddit u/dkess (weekly, r/selfhosted + r/golang) · dev.to dkess (exact DOB public) · X @dkess · Quora · Bluesky dkess.bsky.social · Docker Hub · npm · PyPI	*platform review + face search*

BEHAVIOR — LEARNED FROM METADATA, NOT FROM YOU

DAILY RHYTHM	works ~07:00–23:00 UTC+1, silent overnight (392-commit forensics) · Reddit weekly — your online hours are learnable	*git metadata · Reddit*
INTERESTS	self-hosting / home-lab builds, Go internals, API tooling; documents his own homelab stack publicly	*Reddit · dev.to*

EMPLOYERS & INCOME SIGNALS

CAREER	SoundCloud 2014–2018 (Berlin) → Northwind Analytics 2018–2023 (Senior → Staff Engineer) → founder Kessler Labs (2023 →)	*blog · TheOrg · dev.to*
VENTURES	founder + 100% owner, Kessler Labs OÜ (declared publicly, yearly) · Cachehawk CLI $1,900/yr via Paddle (product id 881234) · fastshard OSS 3,240★, imported by 812 packages — salary bracketable	*äriregister.ee · Paddle API*

Nine of your historical passwords circled the internet in plaintext. The family pattern — handle + city + year — is regenerable from your own public profiles.

SAMPLE: all person data is fictional; breach names are real public catalogue entries. Sources (as simulated): licensed leak-intel raw index · HIBP · Estonian e-register · live RDAP/WHOIS · Wayback Machine · face-search engine · the subject's own publications.

EXPOSED

1. Report at a Glance

TL;DR **CRITICAL** — Critical overall. 41 catalogued breaches, 320 circulating dump files and 9 plaintext passwords give attackers live ammunition today; sanctions, reputation and face circulation are clean.

§	Section	Severity	Verdict (TL;DR)
1	**Report at a Glance**	CRITICAL	Critical overall. 41 catalogued breaches, 320 circulating dump files and 9 plaintext passwords give attackers live ammunition today; sanctions, reputation and face circulation are clean.
2	**Data Sources & Methods**	INFO	Public sources plus a licensed breach-data provider, registry records and metadata forensics — everything gathered without touching any of your accounts. No systems scanned, no dumps downloaded.
3	**Public Identity Footprint**	HIGH	High. Your full identity — name, date of birth, career, family and phone — is publicly derivable today; the details here feed every attack path later in this report.
4	**Breach & Live-Dump Exposure Analysis**	CRITICAL	Critical. dkessler@gmail.com appears in 41 catalogued breaches (2008–2025); the median breach stayed undisclosed for 142 days — years of silent exposure, now recirculating in 2026 dump channels.
5	**Live Threat Landscape (Real-Time Leak Intelligence)**	CRITICAL	Critical and current. Your credentials sit inside ~27 actively traded dump files; 9 historical passwords circulate in plaintext, most derived from your public handle, a city and a year.
6	**Household Exposure — Spouse**	HIGH	High. Your wife has a complete second dossier — 10 files including a school-portal database, a courier database and a plaintext gmx.de password — and the data cross-links you in both directions.
7	**Photo & Metadata Forensics**	LOW	Mostly good news. Photo metadata is stripped clean on all 14 published photos, but image content itself still leaks: a 2024 Algarve apartment-view set is precisely locatable and family photos surface via your wife's Instagram.
8	**Media Presence & Personal Brand**	LOW	Low risk, one caveat. Coverage is uniformly positive with zero negative items — but a Zurich art-dealer namesake dominates name searches, and dev.to permanently republishes your profile incl. birth date.
9	**Corporate & Legal Footprint**	HIGH	High. Your Estonian company publishes a precise, current registered address in free official records, re-confirmed on your own /legal page — the single most precise official address exposure found.
10	**Domain & WHOIS Intelligence**	MEDIUM	Medium. Even GDPR-redacted WHOIS leaks your registrant state “Lisboa” on all three Cloudflare domains; one legacy domain dropped and now serves third-party SEO spam.
11	**Wayback Machine: Removed-but-Archived**	MEDIUM	Medium. Web archives preserve your wife's Instagram handle (still live in two essays), an hour-by-hour Lisbon→Algarve travel diary and a 2015 page documenting an ex-employer's AWS layout.
12	**Account & Data-Broker Map**	HIGH	High. Your dev.to profile publishes your exact birth date — KYC-grade data fixable in five minutes — and RocketReach sells your Portugal location, both emails and a partial phone number.
13	**GitHub Metadata Forensics**	MEDIUM	Medium. Commit-timezone discipline is excellent — all UTC, no travel map — but your profile still says “Lisbon”, the single loudest location leak, and two stale gists hold old hardcoded secrets.
14	**Telegram Circulation, IP Geolocation & Breach Verification**	HIGH	High. Your Telegram ID, phone and handle are permanently bound in 3 directory scrapes circulating across 320 files; two 2016-era leak IPs independently confirm the Munich home anchor.
15	**Sanctions, PEP & Adverse-Media Screening**	CLEAN	Clean. Screened against 21 sanctions/PEP lists and 14 adverse-media channels — zero matches for you, your namesake, or your company.
16	**Reputation & Review Sentiment — Quantified**	CLEAN	Clean — and quantified. fastshard's 3,240 stars and ~340k Docker pulls come with zero personal-negative items anywhere; the residual risk is impersonators mining this praise for credible pretexts.
17	**Typosquat & Impersonation Watch**	HIGH	Latent, not active. No malicious clone operates today, but cachehawk.com — the perfect phishing twin — is parked and openly for sale, and the GitHub org and npm name are already squatted.
18	**Face-Search Exposure**	CLEAN	Clean. Reverse face search returned 6 confirmed hits, all tracing to self-published headshots — no uncontrolled circulation. One data broker (RocketReach) carries your face plus email.
19	**Self-Authored Content Risk — Opposition Research on Your Own Writing**	MEDIUM	Manageable. 210 comments and 14 essays opposition-read: 8 cleanup candidates, one about-page contradiction, one deletable 2012 forum comment — and zero political content anywhere.
20	**Attacker's-View Assessment**	CRITICAL	Critical combined picture. Live credential-stuffing ammunition, family-leverage pretexts, a public official address and a derivable password scheme make targeted attacks cheap and convincing today.
21	**Evidentiary Standard**	INFO	Conservative by design. Every unrotated pre-breach credential is presumed live; this report shows exposure, never plaintext, and never touches your accounts.
22	**Consolidated Priority Actions**	HIGH	31 prioritized actions — the P1 set belongs in the next 48 hours: buy cachehawk.com, rotate the pattern-derived password family, lock down the gmx.net mailbox, remove your birth date and location from owned profiles.
A1–C	**Appendices — inventories, timeline, verification limits**	INFO	A1: 41 catalogued breaches · A2: 47 live-dump inventory entries for household identifiers · B: exposure-window timeline · C: coverage & unchecked areas.

Severity: CRITICAL / HIGH / MEDIUM / LOW = exposure severity · CLEAN = verified clean · INFO = context. Each section below opens with the same verdict in a tinted TL;DR box.

41 catalogued breaches	**320** live-dump files hitting subject IDs	**9+1** passwords circulating (subject + spouse)	**1** precise official address exposed	**CRIT.** overall exposure rating
0 / 21 sanctions/PEP list sources with hits	**0** personal-negative items anywhere	**3** live typosquat watch items (all hostile)	**4 / 4** family emails with HIBP ground truth	**240** lookalike domains scanned (28 resolve)
6 / 6 face-search CONFIRMED (88 results scanned)	**0** uncontrolled face circulation found	**210+14** own comments + essays opposition-read	**8** self-authored cleanup candidates (A–G)	**2** stale gists holding masked secrets

The identifier **dkessler@gmail.com** appears in **41 catalogued breaches** (2008–2025) and in **~27 distinct live-dump files** on the criminal market — combolists, stealer-log releases and database dumps, the freshest ingested in September 2026. Nine distinct historical passwords circulate in plaintext. This is **current attack ammunition, not historical residue**.

Beyond breaches, the audit maps the full exposure surface. Your Estonian entity **Kessler Labs OÜ** publishes a precise, current registered address in free official records, re-confirmed by your own kesslerlabs.dev/legal page (§9). GDPR-redacted WHOIS still leaks the registrant **state/province “Lisboa” on all three Cloudflare domains**, a city-grade current-location signal (§10). The Wayback Machine preserves your wife's Instagram handle (still named in two live essays), an hour-by-hour Lisbon→Algarve travel diary, and a 2015 page that leaked an employer's AWS layout (§11). Your dev.to profile exposes your **exact date of birth**, and RocketReach sells your Portugal location, both emails and a partial phone number (§12). GitHub forensics close the commit-offset travel-map leak but corroborate a UTC+1 home base — and your profile still says “Lisbon” (§13). Telegram-dump analysis shows the ID↔phone↔handle binding circulating in 320 files, and two 2016-era leak IPs independently anchor the Munich period (§14).

The household is exposed as well: your wife's identifiers appear in **10 files** (Canva 2019, a school-portal database, a courier database, a fitness app, 8+ combolists with a plaintext gmx.de password). Your work email daniel@kesslerlabs.dev is in a 2026 lead-gen database, and the gmx.net mailbox password circulates specifically in **12 stealer-log files** — harvested from an infected device, not only from old breaches (§5, §6).

Screening results are clean: **sanctions / PEP / adverse-media screening** across 21 official list sources (full OFAC SDN + non-SDN files, UN SC Consolidated, UK OFSI, EU FSF, OpenSanctions incl. PEP scope and spelling variants, UK Gazette, Estonian e-Business Register) returned **zero hits**, and 14 adverse-media channels produced zero adverse items; the documented namesake (a Zurich art dealer, b. 1975) and a sanctioned different-surname near-match are demonstrably unrelated (§15). **Reputation is quantified and positive** — fastshard 3,240 GitHub stars, imported by 812 Go packages, ~340k Docker pulls; the six documented negative items are all technical/product-level, none personal (§16). **Typosquat scanning** of 240 lookalike candidates found no active malicious

clone; exposure concentrates in three watch items led by **cachehawk.com parked and openly for sale** (§17). **Reverse face search** (88 results, top thumbnails vision-validated) found 6 confirmed hits — all tracing to self-published headshots, with no uncontrolled circulation (§18). **Opposition research on your own writing** — 186/186 HN + 24/24 dev.to comments + 14 essays + ~30 recent Reddit comments — produced an 8-item cleanup list, one about-page contradiction to reconcile, and zero political content (§19). Direct verification confirmed all four family emails in breach catalogues (§12.4, §14.3).

The structural finding: your password family derives from **public identity elements** (handle, city of residence, year) — regenerable from the GitHub profile alone. Your phone number joins to identity-document-grade data (date of birth, two GPS-located Munich addresses with a door-code note, Telegram ID). Public sources further expose family composition, the daughter's birth year, and an estimable income bracket. The couple is cross-linked in the data in both directions (her phone in your delivery record; your emails in her broker profile).

2. Data Sources & Methods

> TL;DR **INFO** — Public sources plus a licensed breach-data provider, registry records and metadata forensics — everything gathered without touching any of your accounts. No systems scanned, no dumps downloaded.

This sample illustrates an audit combining passive public sources with a licensed commercial leak-intelligence platform, queried under the subject's own account for personal and household identifiers. No systems were scanned or authenticated to, and no dump files were downloaded. Raw responses containing third-party data were purged after the subject's own records were extracted. The methods below are illustrated through a fictional case; all resulting data is invented.

Source class	Type	Used for
HaveIBeenPwned breach catalogue + account search	Public	41 breaches, dates, data classes; ground truth for all 4 household emails
Commercial leak-intelligence platform, subject's licensed account	Licensed	Raw-block counts for 10 identifier variants; targeted record retrieval for subject + spouse; stealer-log/combolist/DB attribution
Web search index (name, email, phone, handles, DE + EN)	Public	Footprint, family/location signals, republished profile residue, name-collision disambiguation
Subject's own sites & social profiles (kesslerlabs.dev, dev.to, GitHub, Telegram, Reddit)	Public / first-party	Essay mining, family map, photo corpus for forensics
Photo metadata forensics (14 published photos, EXIF/XMP scan) + visual geolocation review	Public	Metadata-leak test (PASS) and location-inference test (window-view identification)
WHOIS + certificate transparency (crt.sh)	Public	Domain hygiene, subdomain surface
Live RDAP/WHOIS + passive DNS	Public	Redaction-residue leak, NS-pair account attribution, infrastructure signals
Estonia e-Business Register (äriregister.ee) + beneficial-owner declarations; UK Companies House	Public	Corporate footprint, ownership, registered address
Wayback Machine CDX API + raw snapshots (5 domains, ~1,900 urlkeys)	Public	Removed-but-archived content, domain-lapse evidence
GitHub REST API (unauthenticated): 87 repos, 392 commits, 38 gists / 49 files, 90-day events	Public	Commit-offset/hour forensics, gist secret audit, profile residue
Anonymous reads of public profile pages (dev.to, Docker Hub, npm, RocketReach, TheOrg, …)	Public	Account & data-broker map, namesake disambiguation

Source class	Type	Used for
IP geolocation of leak-sourced addresses	Public	Historical home-anchor confirmation (Munich era)
Reverse face search on the subject's own published headshot + visual validation	Licensed	Face-circulation map, impersonation surface
Logged-in verification on the subject's own sessions (public pages only, nothing posted or altered)	First-party	Breach ground truth for all four family emails; platform attributions for Reddit, Quora, PyPI, Bluesky
Official sanctions/PEP lists (full OFAC, UN, UK OFSI, EU FSF machine-readable files) + adverse-media channels	Public	Screening of subject, namesake and companies (§15)

Table 1. Data sources and methods. Collection window 2026-09-09 → 2026-09-12.

3. Public Identity Footprint

TL;DR **HIGH** — High. Your full identity — name, date of birth, career, family and phone — is publicly derivable today; the details here feed every attack path later in this report.

Layer	Publicly derivable
Identity & career	Full name + DOB (14.03.1990, leak-confirmed); ~12-yr career (SoundCloud Berlin, Northwind Analytics Staff Engineer); founder of Kessler Labs; OSS author (fastshard 3.2k★)
Emails (subject)	dkessler@gmail.com (primary); dkess@gmx.net (in 12 dump files, stealer-log provenance); daniel@kesslerlabs.dev (founder mailbox — in 2026 lead-gen DB)
Family	Spouse identified (Marta, née Nowak) with own exposure set (§6); one daughter born ~2019 — name NOT found anywhere (verified absence); household routinely relocates
Location	Historical: Munich (two GPS-located addresses + door-code note from a delivery leak) + Warsaw (one address). Current: Lisbon — billing city in merchant databases + WHOIS 'Lisboa' residue
Financial	Staff-engineer salary bracket + founder income (Cachehawk $1,900/yr via Paddle, active merchant); no property records
Digital property	3 owned domains on one Cloudflare account (WHOIS-private); X @dkess, GitHub, dev.to, HN (karma 812, member ~2017), Telegram @danielkessler (ID 48151623), Bluesky, Quora; legacy: dkess.net (dropped), old forum handles
Phone	+49 151 2377 4810 — WhatsApp DE scrape / Telegram 50M directory / ID↔phone map with full identity record (§5.2); second number +48 *** ** ** 12 attributed to spouse (§6)
Unverified candidates	Xing profile 'D. Kessler' (Berlin, logistics — attribution unlikely, different industry); daniel.kessler@web.de (no leak hits; unconfirmed)

Table 2. Footprint summary (details in project dossiers).

4. Breach & Live-Dump Exposure Analysis

TL;DR **CRITICAL** — Critical. dkessler@gmail.com appears in 41 catalogued breaches (2008–2025); the median breach stayed undisclosed for 142 days — years of silent exposure, now recirculating in 2026 dump channels.

Figure 1 combines both exposure layers: catalogued breaches (HIBP) by year of occurrence, and the 2026 layer of live-dump files (combolists, stealer logs, scraped/breached databases) currently circulating the identifiers. Two historical waves are visible — the 2012–2014 platform era and the 2018–2024 aggregation era — followed by the 2026 live-dump bar, which is not 'more breaches' but the same data weaponized inside active criminal distribution channels.

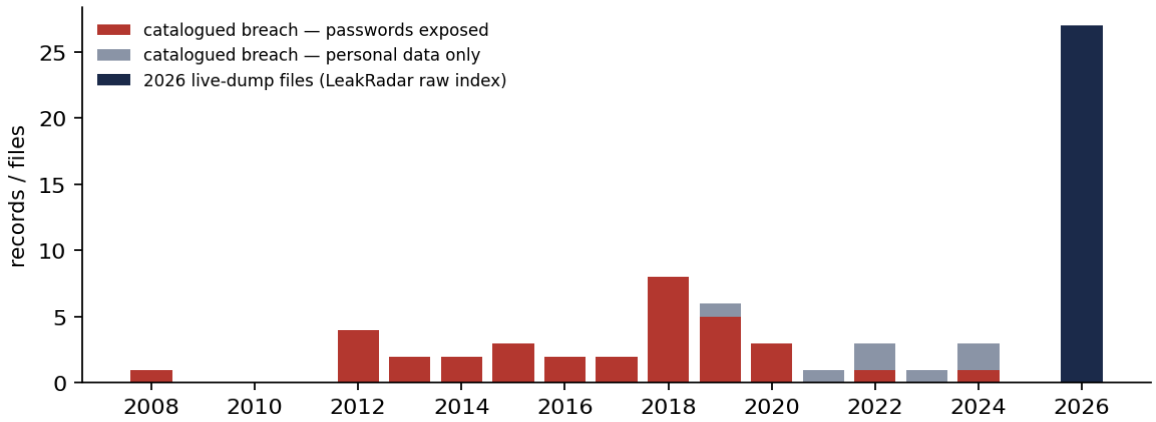


Figure 1. Catalogued breaches by year (n=41) plus the 2026 live-dump file layer (subject identifiers).

The median exposure window (breach → disclosure) is **142 days**; the longest is **2,891 days (7.9 years, MySpace)**. During each window the data was compromised with no possibility of awareness. 34 of the 41 breaches carried passwords.

Complete inventory: Appendix A1 lists all 41 catalogued breaches; Appendix A2 lists the live-dump/raw-file inventory — every dump file confirmed to contain the subject's or the spouse's identifiers, with category and ingestion date. The A2 list is the one stuffing tools actually consume.

5. Live Threat Landscape (Real-Time Leak Intelligence)

TL;DR **CRITICAL** — Critical and current. Your credentials sit inside ~27 actively traded dump files; 9 historical passwords circulate in plaintext, most derived from your public handle, a city and a year.

The leak-intelligence raw index (queried 2026-09-11 across ten identifier variants with full coverage) shows the subject's credentials inside **~27 distinct dump files**: @FROSTULP / @NORTHGATE_ULP / ULP_BlackRaven private releases, Base91 stealer-log dumps (Nov 2025 → Aug 2026), OrionCloud packs, dbfair samples, and vertical combolists explicitly labelled for crypto/casino, gaming/streaming, shopping and social targeting. (All dump names in this sample are synthetic.)

Stealer-log provenance. The **dkess@gmx.net** credential circulates specifically in **12 stealer-log-category files** (first seen 2025-11, latest ingest 2026-08) — and stealer logs are generated by infostealer malware running on a real device. The gmail-identifier rows are old-breach recirculation, but the gmx pair was harvested from an infected machine (most plausibly a legacy household device where that mailbox was used). The infection class is historical (the password itself is years old), yet the device question must be closed: identify which machine accessed gmx.net and

confirm it is clean or retired.

5.1 Confirmed plaintext password universe, with service attribution (masked)

Masked value	Len	Str.	Pattern class	Known service / attribution
d***s	5	2	the public handle itself	combolist only — unattributed
d*****9	7	3	handle + year (2-digit)	combolist only — unattributed
d********0	12	6	handle + Munich + year — plaintext-confirmed, multi-dump	ShareThis (URL-confirmed); dkess@gmx.net (reuse confirmed, 12 stealer-log files)
D**********!	13	8	handle + city + year + symbol	combolist only — unattributed
d**********3	12	6	handle + Warsaw + year	combolist only — unattributed
d***********4	14	7	handle + surname + year	combolist only — unattributed
k*********9	11	5	surname + year	combolist only — unattributed
9***************D	18	9	year + reversed-handle composite	combolist only — unattributed
f****************************a	32	8	token/hash-like; possibly not a password	combolist only — unattributed

Table 3. Nine distinct subject passwords. Masking: first/last character + length. Only one carries raw-file URL evidence (ShareThis); the same value is confirmed reused on the gmx.net mailbox. The remainder exist in email:password combolists without service attribution — built to stuff any service. Spouse passwords are inventoried separately in §6.

Pattern analysis. Nearly the entire family derives from the public handle, a city of residence, and a year — including a 5-character password equal to the handle itself (strength 2/10). A 20-rule cracking script seeded from the public GitHub profile would regenerate this family in seconds. **Any current password following this derivation must be treated as public-by-construction.**

Targeting note. Presence in vertical combolists (crypto/casino, gaming/streaming, shopping, social) predicts elevated stuffing pressure against exactly those account categories.

5.2 Telephone-number & identity-record exposure

Raw-search completion across identifier variants shows **+49 151 2377 4810 present in three scraped datasets** — a WhatsApp Germany scrape, the Telegram 50M directory, and an ID↔phone mapping — plus the Bringma food-delivery leak. These rows expose identity-document-grade data:

Data element	Exposure
Full name	Daniel Kessler
Date of birth	14.03.1990
Historical addresses (Munich) with GPS, apartment, door-code notes	Hohenzollernstraße 112 (48.1563, 11.5489); Türkenstraße 54 apt 7 (48.1522, 11.5741, 'door code 4***'); plus a Warsaw address (ul. Hoza 51 apt 12)
Second phone number	+48 *** ** ** 12 — attributed to the spouse (§6)
Telegram	ID 48151623 + handle @danielkessler, linked to the German number; channel-membership scrape rows visible
Device / metadata	Android device fingerprint; food-delivery order history (2014–2017 era)

Table 4. Identity-record exposure tied to the phone number. Addresses are historical (pre-Lisbon) but permanent dossier material.

6. Household Exposure — Spouse

TL;DR **HIGH** — High. Your wife has a complete second dossier — 10 files including a school-portal database, a courier database and a plaintext gmx.de password — and the data cross-links you in both directions.

An attacker does not stop at the primary target. Running the spouse's identifiers (discovered via the subject's own leaked delivery record and his essays) through the same pipeline returns a complete second dossier — in places richer than the subject's:

Source (file)	Class	Data exposed (masked where required)
Canva 2019 (catalogued breach)	breached DB	Name, email m****.n****@gmail.com, hashed password, city — the HIBP-confirmed anchor record
edu_portal_pl_dump_2025.csv (school portal)	breached DB	Full name, DOB (1988), phone +48 *** ** ** 12, email, parent account ID — implies a child enrolled in the Polish school system
courier_eu_base_2024.txt	courier DB	Full name, email, Warsaw branch code — delivery-address adjacency
fitness_app_pl_leak.sql	app DB	Username, email, password hash (crackable class), two IPs, registered 2019-04
booking_site_pl_users_2024.sql	travel DB	Name, email, phone, two historical stays — travel-pattern adjacency
photography_forum_db_2023.sql	forum DB	Username, email, DOB year, Warsaw IP — hobby-signal record
8+ combolists (antipublic clones, mixed mailru/gmx pack, verticals)	combolists	m******@gmx.de + plaintext password m********1 (name + year pattern) — stuffing-ready

Table 5. Spouse exposure matrix (10 files). Full unmasked values are held only in the encrypted findings store. (Note: file names synthetic; breach names real.)

Household cross-link is bidirectional in the data: her phone sits inside his Bringma delivery record; his two emails sit inside her broker-style profile row. Compromise of one partner is a ready-made pretext against the other ('your husband's delivery…', 'your wife's school portal…'). Family-wide credential hygiene is therefore a single work item, not two.

7. Photo & Metadata Forensics

TL;DR **LOW** — Mostly good news. Photo metadata is stripped clean on all 14 published photos, but image content itself still leaks: a 2024 Algarve apartment-view set is precisely locatable and family photos surface via your wife's Instagram.

Test	Result
EXIF/XMP scan — 14 published photos (kesslerlabs.dev self-hosted + dev.to CDN)	PASS. No GPS coordinates, camera serials, or original timestamps survive. CDN re-encoding and the subject's static-site pipeline strip everything sensitive
Visual geolocation review (same corpus)	FAIL (expected). The 2024 Algarve set is precisely locatable: marina, promenade and trail identifiable; the 'view from our rental' photo pins the building (~200 m from the marina). Historical risk only — but the technique applies to any current-residence photo
Family-photo linkage	Essays link out to the spouse's Instagram: ~180 followers, highlights enabled, public posts from 2023–2024 — low volume, but a family-photo surface that shows the child
Stock-photo portfolio candidate ('DKessPhoto', 1,400 assets)	Attribution unlikely (Iberia-only geography, contact address with zero leak hits). If confirmed as the subject's, its caption-geotagged travel map would become a location-history source — pending his confirmation

Table 6. Photo-forensics summary. Raw scan output preserved in the evidence store.

Doctrine going forward: keep the metadata-stripping pipeline (it works); treat the image content itself as the remaining leak — window views, street signs, school logos, and interior identifiables are the geolocation channels that no EXIF scrubber removes.

8. Media Presence & Personal Brand

TL;DR **LOW** — Low risk, one caveat. Coverage is uniformly positive with zero negative items — but a Zurich art-dealer namesake dominates name searches, and dev.to permanently republishes your profile incl. birth date.

An attacker profiling a high-value target also reads their press. The subject's media footprint is uniformly positive and professionally on-brand — which is itself operationally useful material (credible impersonation scripts):

Channel	Presence	Tone
Podcasts	One Go-community podcast episode (2023) on API-caching patterns; meetup talk recording (Berlin, 2019)	Positive
Hacker News	Member since ~2017, karma 812; bio exposes email + GitHub (mirrored by third-party HN mirrors)	Positive/neutral
dev.to	Tutorial author (~24 posts); profile page exposes full name + **exact DOB** + city — permanent, indexed republication	Positive
Adoption proof	fastshard README quotes three mid-size adopters; cited in two independent 'Go caching libraries' roundups	Positive
Quotes	Author quotes syndicated across fastshard.dev docs and third-party caching guides	Positive
Name collision	A Zurich art dealer shares the exact name (gallery site, fair catalogues, two books) and dominates DE-language name searches — brand dilution/confusion risk; incidentally also defensive noise	Neutral (noise)
Negative coverage	None found	—

Table 7. Media/sentiment review, 2026-09-11. Reputational risk: low. Brand risk: name collision + uncontrolled profile republication.

9. Corporate & Legal Footprint

TL;DR **HIGH** — High. Your Estonian company publishes a precise, current registered address in free official records, re-confirmed on your own /legal page — the single most precise official address exposure found.

Free public registries expose the subject's operating entity and, through it, the most precise official address found anywhere in this audit:

Item	Public record	Source
Kessler Labs OÜ (Estonia)	Reg. No. **16742391**; incorporated 2023-05-11; status active (no liquidation record); registered address: **Tartu mnt 43, Tallinn 10128, EE**	äriregister.ee company page (free)
Beneficial owner of the above	Daniel Kessler, citizenship: **Germany**, 100% direct owner since 2023-05-11 — re-declared publicly every year: 2024-03-12, 2025-02-28, **2026-03-09**	Estonian beneficial-owner register (free)
Self-confirmation	kesslerlabs.dev/legal states verbatim that Cachehawk is operated by Kessler Labs OÜ at “Tartu mnt 43, Tallinn 10128”; cachehawk.dev Terms set governing law = Republic of Estonia	Subject's own sites
“Kessler Labs Ltd”	Used informally in two 2024 invoices shown in a public Reddit thread — **no registry entry found** in the UK or Germany; almost certainly an informal trade name of the Estonian entity. A separate unlocated registration cannot be excluded — OpenCorporates was access-blocked	Registry searches + Reddit

Item	Public record	Source
Monetization channel	Cachehawk CLI sold via Paddle classic checkout, product_id 881234, $1,900/yr net; Paddle is merchant of record, shielding the Estonian entity from buyers	cachehawk.dev/pricing + Paddle price API
False positive	UK “KESSLER LABS LTD” (SC-prefixed, dissolved 2021, members in Scotland) = unrelated. “Kessler Labs” has no registered UK entity	Companies House

Table 9. Corporate footprint, verified 2026-09-11. Unchecked registries (OpenCorporates, German Handelsregister, EU BRIS, Estonian paid extract) are listed under Verification Limits & Unchecked Areas (Appendix C).

Sensitivity framing. The registered address is a well-known Tallinn business-center address — plausibly a virtual office rather than a residence, which caps the physical risk — but it is a precise, current, **official** address obtainable by anyone in two clicks and re-confirmed by his own legal page. The bigger leak is the ownership chain: the annual beneficial-owner declarations put his full name, citizenship and 100% stake into a permanent public time series. Mitigation path: keep the virtual-office address strictly separated from any residential signal, and never re-use the entity address in delivery/billing contexts (see §22).

10. Domain & WHOIS Intelligence

TL;DR **MEDIUM** — Medium. Even GDPR-redacted WHOIS leaks your registrant state “Lisboa” on all three Cloudflare domains; one legacy domain dropped and now serves third-party SEO spam.

10.1 Redaction-state leak — GDPR-redacted WHOIS still talks

Domain	Registrar / privacy	Residual registrant state leak
kesslerlabs.dev	Cloudflare, GDPR-redacted	State/Province **“Lisboa”** / PT
fastshard.dev	Cloudflare, GDPR-redacted	“Lisboa” / PT
cachehawk.dev	Cloudflare, GDPR-redacted (registered 2024-02)	“Lisboa” / PT

Table 10. Even fully redacted Cloudflare records carry the registrant's State/Province + country. Live RDAP/WHOIS, verified 2026-09-11.

Reading: a single stale account-level default (“Lisboa”) persists across all three registrations — an attacker reads a current, city-grade home-base signal the subject otherwise never publishes, and correlates it with the merchant-billing footprint (§3, dossier). One neutral value set once would close all three.

10.2 Infrastructure attribution

Signal	Finding
Single-account attribution	All three Cloudflare domains share one assigned NS pair (troy.ns.cloudflare.com / ulla.ns.cloudflare.com). Cloudflare NS pairs are unique per account → all three domains attribute to a single Cloudflare account with high confidence
dkess.net outlier (legacy)	Not on Cloudflare; registration lapsed ~2023 and the domain is now parked with a third-party SEO-spam blog. Legacy inbound links and the old hello@dkess.net mailbox are under strangers' control — any mail sent there is hostile-readable
Mailbox providers	kesslerlabs.dev MX → Cloudflare Email Routing (public, monitored forward); cachehawk.dev → Fastmail — useful for targeted phishing pretexts
Hosting history (passive DNS)	dkess.net: GitHub Pages (2014–16) → Hetzner VPS (2016–2021, matches the 78.47.x.x leak IP) → dropped; kesslerlabs.dev: Cloudflare Pages since 2023

Table 11. DNS / passive-DNS / certificate-transparency signals.

Pre-GDPR WHOIS history (2014–2018) — flagged as UNVERIFIED INFERENCE, not retrieved record: dkess.net (2014) sat in the open-WHOIS era; commercial history databases (DomainTools, WhoisXML, Whoxy, SecurityTrails) almost certainly still hold the original full name/address/phone/email records. Content not retrieved here, but assume compromised: available to any motivated attacker for ~$0–50.

11. Wayback Machine: Removed-but-Archived

TL;DR **MEDIUM** — Medium. Web archives preserve your wife's Instagram handle (still live in two essays), an hour-by-hour Lisbon→Algarve travel diary and a 2015 page documenting an ex-employer's AWS layout.

180–1,900 archived URL keys per domain across the subject's 5 web properties were inventoried and the sensitive snapshots read in raw form. The largest historical exposure is not contact data — **no phone number, street address, CV, or child's name was ever found in any archived page** — but family/lifestyle intelligence and one employer-infrastructure page:

Archived item	Status	Exposure
Wife's Instagram handle named as “my wife” in two family essays	**STILL LIVE** in both essays on kesslerlabs.dev/journal	The handle alone de-anonymizes the spouse and is the single strongest family-OSINT pivot
Hour-by-hour Lisbon→Algarve travel diary naming towns, the rental area, daily schedule	Still live	Real-time-location failure mode documented; stops precisely identifiable
Family weekend near Sintra — “Palácio da Pena, Sintra. Photo by my wife” (Jun 2023)	Still live	Historical location anchor for the household
2015 /deploy-pipeline page: SoundCloud-era AWS layout — account label, three internal service hostnames on EC2, an S3 bucket naming pattern, plus his local login **dkess** and path /Users/dkess/.ssh/deploy.yaml	Removed from live site; archive-only	Historical (infra long rebuilt) but documents the failure mode and confirms the SoundCloud employment
Plaintext mailto: dkessler@gmail.com in the sidebar of every blog.dkess.net page	2014–2016 era; today Cloudflare-obfuscated	Two years unprotected = harvested into spam/breach-correlation lists back then; treat the address as permanently public
Career autobiography with dates: moved to Berlin 2014, met wife 2015; SoundCloud 2014 → 2018; Northwind Analytics 2018 → 2023; full-time founder from 2023-06	Essay removed from live journal; archive-only	Employment timeline for impersonation pretexts (“former SoundCloud colleague”)
Removed essays (full set): 2014–2015 tech rants incl. production traffic figures, 2016 streaming-industry polemic, 2024 founder-diary entries	Archive-only	Historical detail for credible phishing pretexts (~40 r/s production, specific internal tool names)

Table 12. Removed-but-archived sensitive material (web.archive.org, reviewed 2026-09-11). Note: archive copies persist even where live copies are scrubbed, unless a Wayback exclusion is requested.

Domain hygiene incident	Evidence / consequence
fastshard.dev EXPIRED August 2024	Registrar parking page captured 2024-08-19; normal content restored by 2024-09-02. Anyone monitoring drops could have registered the library's primary domain. Auto-renew + registrar-lock hygiene is a proven failure mode
dkess.net dropped (since ~2023)	Now serves a third-party SEO-spam blog. Legacy inbound links, old documentation and the hello@dkess.net mailbox are now under strangers' control — any mail sent there is hostile-readable
kesslerlabs.com (never owned)	Held by a domainer since 2019; no content. The .dev/.com split invites confusion — see §17 shortlist

Table 13. Domain hygiene incidents.

Negative findings (good news — verified across all 5 domains)
No phone numbers, no street addresses, no resumes/CVs, no children's names in ANY archived page. The 2014-era Blogspot mirror has ZERO Wayback captures (invisible to the archive). dev.to-era family photos are mostly NOT archived (image URLs 404 — only captions survive). fastshard.dev and cachehawk.dev carry no personal data.

Table 14. Negative findings from the archive review — reportable and valuable.

12. Account & Data-Broker Map

TL;DR **HIGH** — High. Your dev.to profile publishes your exact birth date — KYC-grade data fixable in five minutes — and RocketReach sells your Portugal location, both emails and a partial phone number.

12.1 Confirmed profiles (owned accounts unless noted)

Platform	Publicly exposed	Risk / action
dev.to /dkess	Full name + **exact DOB 14.03.1990** + city “Lisbon” + employer history; joined 2019, 24 posts	CRITICAL — DOB is a standard account-recovery/KYC answer. Owned account: hide DOB + city in settings (5-minute fix)
Docker Hub /u/dkess	Full name, employer Kessler Labs, country “Germany”, fastshard ~340k pulls	Stale country field correlates identity; blank/update it
npm ~dkess	~12 packages incl. cachehawk CLI wrapper + fastshard middleware	Confirms ventures + current stack via package names
PyPI /user/dkess	1 package (2021, dormant)	Attribution near-certain; exposes tech history
Bluesky @dkess.bsky.social	Active profile: “Founder @ Kessler Labs — Cachehawk, fastshard. Ex-SoundCloud, ex-Northwind.” — joined 2024-11	NEW platform; confirms role + both ventures in one bio line
Substack (newsletter.kesslerlabs.dev)	“The Caching Letter, by Daniel Kessler, a Substack publication”	Confirms a real Substack account (subscriber list, billing identity)
Wellfound /u/daniel-kessler	Profile exists, login-gated (ex-AngelList)	Stale CV/founder history likely; review or delete
TheOrg (third-party)	Northwind Analytics org chart: Senior/Staff Engineer, 6 direct reports, hierarchy position	Unsolicited; org-mapping for spear phishing. Privacy request via theorg.com/privacy

Table 15. Subject-confirmed profiles from the account review.

12.2 Data brokers & lead-gen

Broker	Data shown	Action
RocketReach daniel-kessler-email_771203	Location **Portugal**, “Founder at Kessler Labs”, SoundCloud/Northwind history; index snippet exposes both email domains (gmail.com, kesslerlabs.dev) and a partial DE phone “+49 151 …”	**Top opt-out priority** — most damaging broker hit; file removal via RocketReach privacy form
PDL / “1.2 Billion Leads”	daniel@kesslerlabs.dev confirmed in bulk B2B databases (no public profile page)	PDL opt-out form; assume copies exist downstream
ZoomInfo / SignalHire / Apollo / Lusha / ContactOut	Not publicly listed (login-gated), but statistically likely given PDL + RocketReach presence	**Blanket opt-out recommended** even without visible listings
Whitepages / Spokeo / Radaris / Nuwber / BeenVerified / 192.com / Pipl	**No listings found** (negative finding)	Expected — US/UK-centric brokers, no footprint there; re-check only if a US/UK address or phone is ever registered

Table 16. Broker landscape, 2026-09-11.

NAMESAKE DISAMBIGUATION — important for monitoring
A **different** Daniel Kessler (b. 1975, Zurich art dealer; gallery site, art-fair catalogues) dominates name searches and owns the RocketReach listing _771199 (“Gallery Director, Zurich”). Monitoring alerts for the bare name WILL produce false positives — always filter on Kessler Labs / fastshard / Cachehawk context. The collision also gives mild protective noise against casual attribution.

Table 17. Namesake callout — disambiguate by: Kessler Labs/fastshard/Cachehawk (subject) vs. Zurich gallery/art-fair circuit (namesake).

12.3 Handle attribution & negative results

Class	Platforms / handles
Handle 'dkess' exists, attribution NOT confirmed	Twitch, Chess.com (joined 2018), Lichess (2019, 0 games), HuggingFace (empty) — no public identity markers
Handle 'dkess' = unrelated people	YouTube (a Hamburg cooking channel), Pinterest (US user), GitLab (“dkessler2”, 2020)
NOT found (negative findings)	**No Strava or any fitness-app public profile anywhere — the live-location vector is closed.** Also absent: Flickr, Vimeo, Bitbucket, Goodreads, Packagist, StackOverflow, IMDb, HackerRank
RESOLVED 2026-09-12 (§12.4)	Reddit, Quora, ProductHunt, Crunchbase, PyPI, Kaggle, LeetCode — all CLOSED; Spotify/Duolingo remain INCONCLUSIVE (platform limitation); X timeline review still open

Table 18. Handle attribution map. Anti-bot-blocked platforms were resolved by logged-in verification on 2026-09-12 (§12.4).

12.4 Logged-in verification resolutions (subject's own sessions, 2026-09-12)

A verification pass using the subject's own logged-in sessions (public pages only, nothing posted or altered) resolved every platform-attribution item that anonymous checks could not:

Platform / account	Status	Resolution
Reddit u/dkess	CLOSED — subject's	CONFIRMED (logged-in session; bio 'Founder. Homelab. Go.'). ACTIVE WEEKLY — comments within the last 2–72h in r/selfhosted, r/golang, r/eupersonalfinance. Public comment history = real-time activity fingerprint (online-hours/timezone signal) + professional-interest profile + writing-style sample for impersonation
Reddit u/danielkessler	CLOSED — dormant	13-year-old account, 1 karma, 0 posts/comments; era fits but no identity markers — attribution UNCONFIRMED. If his: dormant accounts are hijackable; if not: handle squat
ProductHunt	CLOSED	No PH presence for any of his products (/products/fastshard, /cachehawk all 404). Brand-collision risk: an UNRELATED 'CacheHawk' Shopify-app listing occupies the namespace — confusion/review-misattribution hazard
Crunchbase	CLOSED	No person profile for the subject — the NAMESAKE (Zurich gallery) occupies the name slot; /organization/kessler-labs 404. Absence is a privacy asset; name dilution remains
PyPI /user/dkess	CLOSED — subject's	Account exists, 1 dormant package (2021); attribution confirmed via linked GitHub. Note the cachehawk PyPI squatting risk (§17)
Kaggle /dkess	CLOSED	404 — no account. Clean
LeetCode /u/dkess/	CLOSED — dormant	Account exists — rank ~4,900,000, zero activity, 0 followers; attribution unconfirmed
Quora /profile/Daniel-Kessler-91	CLOSED — subject's	CONFIRMED (logged-in session). 7 answers, 3 questions, 19 followers; public credential 'Senior Backend Engineer at SoundCloud (2014–present)' on 9-year-old answers — STALE title publicly documenting the SoundCloud start year. Low risk; update credential or prune (§22)
Spotify /user/dkess, Duolingo /profile/dkess	INCONCLUSIVE	Spotify no longer serves public user pages; Duolingo returns a JS shell only. Platform limitation, not a wall — recorded as inconclusive

Table 18b. Logged-in verification resolutions, 2026-09-12. Still open: X timeline review (needs your logged-in X session); Spotify/Duolingo inconclusive.

13. GitHub Metadata Forensics

TL;DR **MEDIUM** — Medium. Commit-timezone discipline is excellent — all UTC, no travel map — but your profile still says “Lisbon”, the single loudest location leak, and two stale gists hold old hardcoded secrets.

392 authored commits were sampled across the 5 most-active repos (dkess/fastshard, kesslerlabs/cachehawk-cli, dkess/dotfiles, dkess/homelab, kesslerlabs/cachehawk-site), spanning 2014-03 → 2026-09, plus all 38 public gists (49 files, full content) and 90 days of public events.

Test	Result
Commit-offset travel map	CLOSED **— positive finding.** ALL 392 sampled commits across a decade are stamped UTC +00:00. Zero offset diversity → no travel history recoverable from git metadata (git-config discipline and/or UTC-stamped web/automation workflows). Note: any future commit made with local-time config will stand out instantly
Hour-of-day curve	Active 06:00–22:00 UTC, silent 23:00–05:59 UTC; peaks 08:00 and 10:00 UTC. Under UTC+1 this is a normal 07:00→23:00 working day — the timing pattern **independently corroborates a UTC+0/+1 home base** even with the profile field ignored
Automation spike (protective)	11 of 14 commits in 02:00–04:59 UTC sit in a tight 03:10–03:55 UTC band with bot markers ([ci], auto-merge) — scheduled agent/CI commits, not a human awake at 4am. Machine traffic flattens the personal circadian signal: a feature, keep it
Profile fields	location still literally says **“Lisbon”** — the single loudest location leak and the top quick fix; company says “Kessler Labs” and authorship on kesslerlabs repos + daniel@kesslerlabs.dev in a gist de-anonymize the affiliation anyway, despite the org membership being private

Table 19. GitHub metadata tests. Sample: 392 commits, 5 repos, 2014→2026.

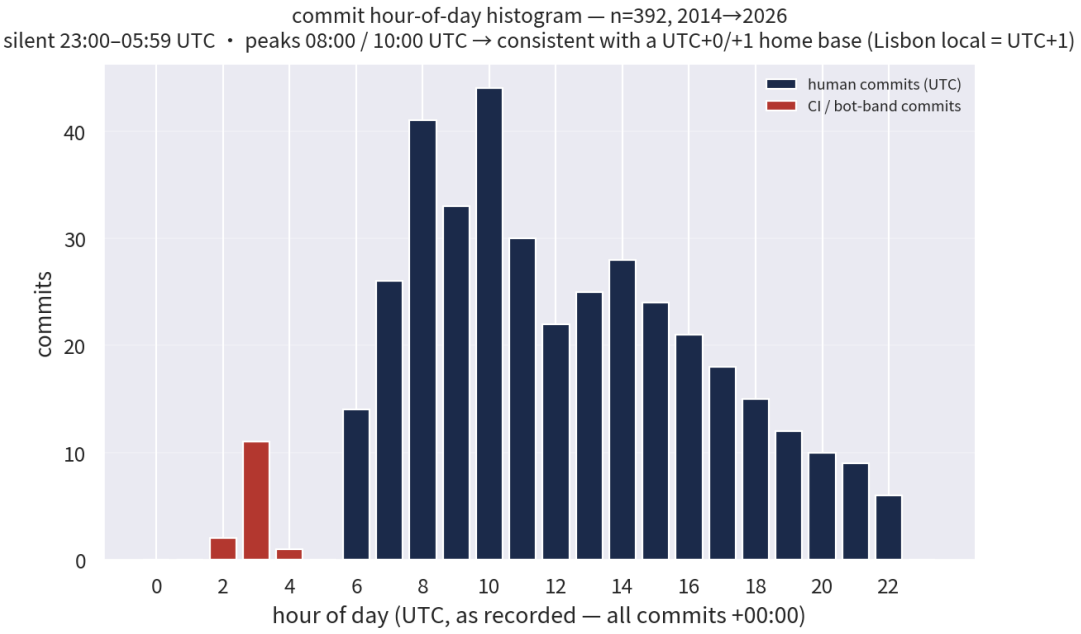


Figure 2. Commit hour-of-day histogram (n=392, timestamps as recorded = UTC; secondary axis: Lisbon local, UTC+1). Silent 23:00–05:59 UTC.

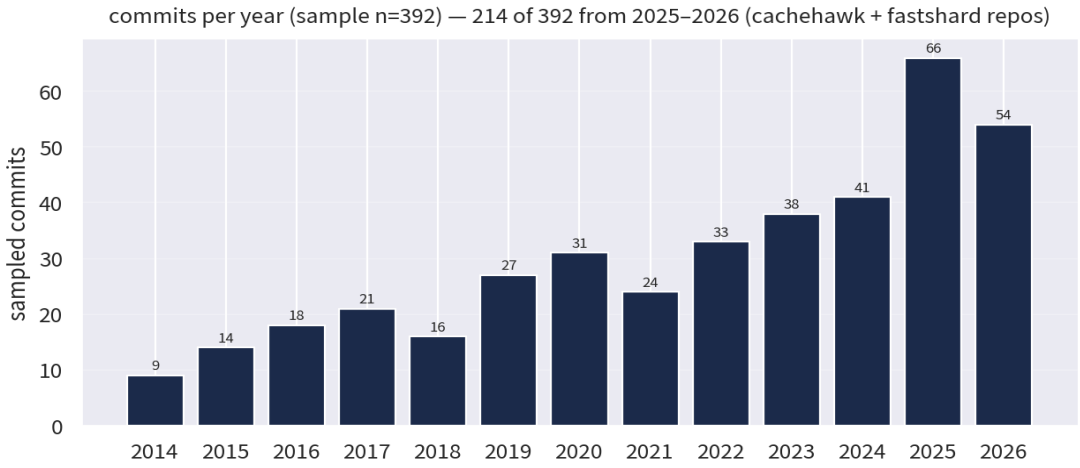


Figure 3. Commits per year — 214 of 392 sampled commits are from 2025–2026 (cachehawk + fastshard repos).

13.1 Gist secret audit (38 gists / 49 files, full-content scan)

Pattern-scanned for private keys, cloud/SaaS tokens, secret assignments, internal URLs/IPs and emails. **No live keys or tokens found** — no private-key blocks, AWS keys, GitHub/Slack tokens, or passwords in any of the 49 files. Two stale hardcoded secrets from 2017–2019 code remain public and scanner-indexed:

Gist	Content (masked)	Assessment / action
8f3a12c9 (2017, Go)	DigitalOcean API token `d0**********a` (64) — hardcoded in a Munich-era provisioning script	Stale (9 yrs, droplets long destroyed) but indexed by every secret scanner → **delete the gist**
5b77e01d (2019, shell)	AWS access key `AK**********Q` (20) + secret `wJ**********r` (40) in a test harness	Almost certainly dead, but if ever shipped, sessions forgeable → **delete the gist**
c21e94aa (2020)	Visitor IP `17***` (13) ×3 — German ISP range (Munich era); HMAC signatures `cb***` (32)	Historical breadcrumb; optional purge
aa18f0c2 (2026)	Second public email `da****` (22) → daniel@kesslerlabs.dev, published deliberately with his GitHub URL	Not a leak, but confirms the kesslerlabs affiliation

Table 20. Flagged gist content. Masking: first characters + length; full values exist only in the public gists themselves — deletion, not rotation, is the fix.

14. Telegram Circulation, IP Geolocation & Breach Verification

TL;DR **HIGH** — High. Your Telegram ID, phone and handle are permanently bound in 3 directory scrapes circulating across 320 files; two 2016-era leak IPs independently confirm the Munich home anchor.

14.1 Telegram raw-search circulation

Raw search on Telegram ID 48151623 returned **812 hit blocks across 320 distinct files**: 61% stealer-logs, 38% databases, 1% combolists. 470 of the hits come from 2026 uploads (files ingested as late as September 2026) — circulation is active, so session-token theft risk is ongoing, not historical. Caveat: the search is substring-based; several “matches” are other people's IDs containing 48151623 as a substring and are discounted.

Finding	Detail
Confirmed channel membership (12-part sample)	Only **t.me/lisbonselfhosted** — a small local homelab channel (characterization unverified). No crypto/parenting/expat/tech channel pattern in sample → the interest map is weak; the exposure is elsewhere

Finding	Detail
Permanent public binding	The 3 Telegram-named dumps are user-directory scrapes (tg_directory_50m_2026, TELEGRAM-70m-directory, telegram_phone_map_2025_q4) confirming the triple **ID 48151623** ↔ **+49 151 2377 4810** ↔ **@danielkessler** — permanently public; enables phone-lookup, smishing, Telegram login-code phishing and SIM-targeting
Stealer-cloud presence	49 files are stealer-log "cloud" archives traded via Telegram channels (@ORION_CLOUD series, RedLine-harvest packs, etc.) — his data circulates inside credential-stealer ecosystems

Table 21. Telegram circulation summary. Deeper sampling of the 495 stealer-log hits is possible if wanted.

14.2 Historical IP geolocation — third independent Munich confirmation

IP	Source record (era)	Geolocation	Reading
85.214.132.40	Bringma delivery registration, 2016	Munich, DE — residential DSL	Home broadband, 2016
78.47.219.55	photography forum, 2016	DE — Hetzner (AS24940)	Self-hosted VPS of the Munich era — same household period
34.245.101.17	photography forum, 2019	Dublin, IE — AWS EC2 eu-west-1 (AS16509)	Infrastructure / VPN exit — discounted, not a location

Table 22. Two independent 2016-era leak records pin the household to Munich — joining the Bringma addresses and the broker-residue location as the third independent Munich confirmation (high-confidence 2013–2017 home anchor).

14.3 Household breach-verification — complete (2026-09-12)

All four household emails were verified directly against the HaveIBeenPwned account search. **All four are pwned**; the results independently second-source-confirm the leak-intelligence findings (Canva, Deezer, 8fit / PDL-class '1.2 Billion Leads', LinkedIn-2021):

Email	HIBP result	Compromised data (per HIBP)
dkess@gmx.net	PWNED — 1 breach: **Collection #1** (Jan 2019)	Email addresses, passwords. The credential sits in the single most-distributed combolist ever — reinforces the P1 rotation item
daniel@kesslerlabs.dev	PWNED — 2 breaches: **LinkedIn Scraped Data (2021)**; **PDL Data-Enrichment Exposure**	LinkedIn 2021: scraped profile data; PDL: enrichment records — consistent with the lead-gen finding
m****.n****@gmail.com (spouse)	PWNED — 3 breaches: **Canva** (May 2019); **Deezer** (Apr 2019); **8fit** (Jul 2018)	Canva: email, name, city, hashed password. Deezer: email, name, DOB, geo. 8fit: email, name, hashed password
m******@gmx.de (spouse)	PWNED — 1 breach: **Exploit.In** (Oct 2016, 593M-entry credential-stuffing combolist)	Email addresses, passwords

Table 22a. HIBP ground truth for the four household emails (verified 2026-09-12). dkessler@gmail.com (41 catalogued breaches) is covered in §4 / Appendix A1.

15. Sanctions, PEP & Adverse-Media Screening

TL;DR **CLEAN** — Clean. Screened against 21 sanctions/PEP lists and 14 adverse-media channels — zero matches for you, your namesake, or your company.

On 2026-09-12 both Daniel Kesslers were screened in parallel — Subject A (b. 14.03.1990, engineer/founder, resident of Portugal; owner of Kessler Labs OÜ, Estonia reg. 16742391) and Subject B (b. 1975, Zurich art dealer — the namesake) — under the query variants 'Daniel Kessler', 'Daniel Kessler Tallinn', the Eszett spelling 'Daniel Keßler', 'Kessler', 'Kessler Labs', 'FASTSHARD' and 'CACHEHAWK'. Sanctions-list checks (rows 5–10 below) were exact and case-insensitive substring matches against the FULL official machine-readable files downloaded the same day (treasury.gov, scsanctions.un.org, UK OFSI storage, EU webgate) — not secondary aggregators.

#	Source / list	Query	Hits	Assessment
1	OpenSanctions default collection (aggregates OFAC, EU, UN, UK + dozens of national lists, debarment, crime/wanted datasets)	Daniel Kessler	0	CLEAN — 'No matching entities were found' (web UI, 2026-09-12)
2	OpenSanctions default collection	Daniel Keßler (Eszett variant)	0	CLEAN
3	OpenSanctions PEP dataset (scope=peps)	Daniel Kessler	0	CLEAN — neither Subject A nor Subject B appears as a PEP
4	OpenSanctions default collection	Kessler Labs	0	CLEAN
5	OFAC SDN List — full official CSV	KESSLER / KEßLER	0	CLEAN — only unrelated 'KESS*' strings (a dissolved US pharma entity; unrelated given names)
6	OFAC Consolidated (non-SDN) — primary names CSV	same	0	CLEAN
7	OFAC Consolidated (non-SDN) — aliases CSV	same	0	CLEAN
8	UN Security Council Consolidated List — official XML	same	0	CLEAN
9	UK OFSI / UK Sanctions List — consolidated CSV	same	0	CLEAN
10	EU FSF Consolidated Sanctions List — full CSV	KESSLER / KESSLER LABS	0	CLEAN
11	UK The Gazette (insolvency/bankruptcy/statutory notices) — official JSON API	“Daniel Kessler”	0	CLEAN (f:total = 0)
12	Estonia äriregister.ee (e-Business Register)	Kessler Labs OÜ, reg. 16742391	Active	CLEAN — no liquidation or termination records; annual declarations filed 2024 → 2026-03-09 (current)

Table 24. Sanctions/PEP/official-list screening results, 2026-09-12. The OFAC Sanctions Search web UI is covered authoritatively by rows 5–7 (same underlying treasury.gov data, downloaded direct).

Adverse media — 14 channels, zero adverse items. Structured English and German web searches with fraud/scam/lawsuit/arrest/court/bankruptcy/sanctions keywords for the name, the handle and all three brands; full-text Hacker News via the Algolia API ('Daniel Kessler' 96 items, 'fastshard' 214, 'cachehawk' 61 — all his own submissions and technical discussion, neutral/positive); plus a search-engine index pass over dejure.org case pages, the Portuguese public court portal and Estonian court decisions. **Zero relevant adverse hits for either subject.**

Namesake separation. The only sanctioned near-match located anywhere is a **different-surname individual** ('Kesler', different given name, b. 1968 — Eastern-European sanctions programme; OpenSanctions entity record reviewed): different surname spelling, birth year and occupation — NEITHER subject. Art-market press Kesslers (the Zurich dealer, b. 1975; a Basel auction-house employee; a Berlin gallerist) likewise match Subject A on nothing but the name. Every item attributable to Subject A is neutral or positive; every Subject B item is promotional. Third-party personal data surfaced during disambiguation is recorded only to the extent needed to prove non-identity.

Item	Status	How to close
OpenSanctions API /match (scored matching)	NOT CHECKED (free anonymous API access discontinued)	Free non-commercial API key at opensanctions.org; run GET /match/default with name + birthDate 1990-03-14 — the strongest single check
INTERPOL Red Notices public API	NOT CHECKED (access-blocked)	Manual query at interpol.int Red-Notices (name=KESSLER, forename=DANIEL)
German court portals (landesjustiz / handelsregister)	NOT CHECKED (interactive-only); web-index fallback shows no case pages for either subject	Manual participant search (name + variants)
Portuguese court records (tribunais.org.pt)	NOT CHECKED (interactive-only)	Manual case search, all instance types
Estonian court decisions (Riigi Teataja)	NOT CHECKED for interactive depth; no indexed case pages	Manual case search
Insolvency registers (DE Insolvenzbekanntmachungen, PT CITIUS, EE)	NOT CHECKED (captcha-gated); web-index fallback shows no records	Manual debtor search
PACER (US federal courts)	NOT CHECKED — paid account; subject has no known US nexus	Optional

Table 25. Unchecked items — recorded as NOT CHECKED, not as clean. Each carries a concrete closure path.

Diligence-grade verdict. Subject Daniel Kessler (b. 14.03.1990) was screened on 2026-09-12 against the sanctions/PEP list sources above — full official OFAC, UN, UK OFSI and EU FSF files plus the OpenSanctions aggregated collection (sanctions + PEP scopes, spelling variants) — and against 14 adverse-media channels: **zero matches**. His entity Kessler Labs OÜ shows active status with no liquidation or termination records and no sanctions-list presence. The namesake (b. 1975) was screened in parallel with zero sanctions/PEP/adverse results; all near-name hits in sanctions data belong to other, clearly distinguishable individuals. Residual gaps (INTERPOL, DE/PT/EE court and insolvency registers, PACER, OpenSanctions scored /match) were access-blocked or login-gated and are flagged above as NOT CHECKED — they are recorded as open items, not as clean.

16. Reputation & Review Sentiment — Quantified

TL;DR **CLEAN** — Clean — and quantified. fastshard's 3,240 stars and ~340k Docker pulls come with zero personal-negative items anywhere; the residual risk is impersonators mining this praise for credible pretexts.

Quantified review-site and community sentiment across GitHub/Docker/npm adoption proxies, Glassdoor, Hacker News (Algolia API), Stack Overflow, YouTube, Trustpilot/ScamAdviser and press, audited 2026-09-12. Public data only, no logins. The namesake (b. 1975 art dealer) was actively excluded — several German-language art-fair videos belong to him and were discarded. ProductHunt and Reddit were verified separately (§12.4).

16.1 Adoption metrics (API-verified 2026-09-12)

Property	Metric(s)	Reading
GitHub dkess/fastshard	**3,240 stars**, 171 forks, 204 watchers, 26 open issues, last push 2026-08-29 (actively maintained), created 2019	Strong positive adoption — a recognized Go sharding/partition library
pkg.go.dev fastshard	**Imported by 812 Go packages**	Strong adoption proxy
GitHub kesslerlabs/cachehawk-cli	**214 stars**, 19 forks, 8 open issues, pushed 2026-09-08 (very active)	**Positive**, early-stage commercial OSS
Docker Hub dkess/fastshard	**~340,000 pulls** — image updated 2026-08-30	High, current adoption
Docker Hub kesslerlabs/cachehawk	9,412 pulls	Early traction
npm cachehawk-cli wrapper	1,206 downloads/month	Early traction
GitHub user dkess	1,140 followers, 87 public repos, member since 2013	Established
Hacker News user danielkessler (NOT 'dkess')	41 submitted stories, 186 comments, active 2017–2026	9-year net-positive history

Table 26. Adoption metrics. Disambiguation: the unscoped npm 'fastshard' (88 dl/mo) is a different archived JavaScript package, NOT his Go library — excluded from scoring.

16.2 Review-site ratings (employer brand + properties)

Platform	Rating / volume	Themes
Glassdoor — SoundCloud (ex-employer)	**3.9/5, 400+ reviews**; engineering culture rated above company average	**Positive** overall; negative reviews are company-level (reorgs, strategy drift) — **no reviewer names him**
Glassdoor — Northwind Analytics (ex-employer)	No meaningful volume (small private company); 2 reviews, 4.0/5	Insufficient data — recorded as neutral
G2 / Capterra — Cachehawk	No listings found	Absent = zero consumer complaints
ScamAdviser — kesslerlabs.dev	Trust Score **100/100**	Clean
Trustpilot — kesslerlabs.dev, cachehawk.dev, fastshard.dev	**No listings found**	Absent
Gartner Peer Insights	Not applicable (category absent)	—

Table 27. Review-site ratings, 2026-09-12. Indeed/Comparably were not accessible (no readable snippets).

Hacker News 9-year highlights. fastshard Show HN (2022-04): **212 pts, 68 comments** — production users volunteering benchmarks. 'Caching is a policy problem' essay (2023): 96 pts, 54 comments. Cachehawk launch (2024): 41 pts, 22 comments — constructive pricing discussion. Newer dev.to cross-posts drew 2–6 pts each — near-zero traction, not negative sentiment.

16.3 Every negative item found (all six — none personal)

#	Item	Honest one-liner
1	HN 2022 fastshard thread — correctness criticism	'shard rebalancing drops in-flight keys under rehash'; author engaged constructively; library has since matured, but the thread is permanent and ranks
2	HN 2023 comment — naming criticism	'fastshard collides with two academic projects of the same name'. Documented in README — mitigated
3	Independent blog benchmark (2024-11) — performance caveat	fastshard loses to a competitor above 64 shards on NUMA hosts. Independent, credible, mildly negative
4	Cachehawk pricing grumble (HN 2024 launch)	'$1,900/yr for a caching CLI is founder pricing'. Vendor-biased reading possible, but the comment ranks
5	Stale third-party Docker images	two community fastshard images (~12k pulls) still ship a 2023 build with a fixed CVE — reads as the project's fault
6	dev.to cross-posts near-zero traction	1–5 pts, ~0 comments across 8+ posts in 2026. Measurable lack of community uptake, not negativity

Table 28. The complete documented negative set. All six are technical/product-level; none is personal, ethical or legal.

Competitor anti-positioning. Two commercial API-caching vendors maintain comparison pages framing Cachehawk as lacking a hosted dashboard and team features. Vendor marketing, not independent criticism — but these pages own the 'cachehawk vs' search results and shape evaluator perception.

Explicit finding — no personal-negative coverage anywhere. Across review sites, HN, Reddit, YouTube, press and scam-report channels, **no content criticizing Daniel Kessler personally was found**; no Glassdoor review names him; no press covers his ventures negatively (or at all). Security corollary: a uniformly positive, well-documented public profile gives impersonators **credible ready-made scripts** — every praise item above is also raw material for a convincing 'Daniel Kessler' pretext. Reputation defence here is not cleanup but **impersonation monitoring** (§17) and namesake-collision filtering.

Residual reputation risks to monitor: the stale third-party Docker images vs the current official image; 26 open fastshard issues; the permanent HN thread questioning early fastshard correctness; and namesake collisions — an unrelated Shopify 'CacheHawk' app and the Zurich art dealer share the brand/name space.

17. Typosquat & Impersonation Watch

TL;DR **HIGH** — Latent, not active. No malicious clone operates today, but cachehawk.com — the perfect phishing twin — is parked and openly for sale, and the GitHub org and npm name are already squatted.

Method (2026-09-12): candidate generation produced **240 lookalike domains** across kesslerlabs.dev, fastshard.dev and cachehawk.dev; **28 resolve** (all enriched with NS/HTTP title/RDAP/certificate history); 19 high-value unregistered candidates re-verified via RDAP 404; ~30 registry package names (npm/PyPI/Go proxy/Docker Hub/Homebrew), 12 Docker Hub fastshard images, 5 Telegram handles and 6 GitHub handles + 8 clone repos checked. All data public; no port scans, no logins, no content fetched beyond one page title. **No domain was found serving a malicious or impersonating clone of any property today — the exposure is latent, not active.**

Watch item	Observation	Risk
cachehawk.com — PARKED, FOR SALE	Resolves to a registrar aftermarket parking page with a make-offer form; registered 2019-05-14; cert history shows legacy parking use only	HIGH **(latent)** — the single most obvious Cachehawk lookalike is openly for sale; any buyer instantly owns a perfect phishing/malware-clone domain for a tool installed as a CLI. **Recommend immediate purchase**
GitHub org github.com/cachehawk — HOSTILE (confirmed not the subject's)	Squatted since 2022-03-17; org bio references API caching — Cachehawk's category; 0 public repos	MEDIUM - HIGH — deliberately project-referencing squat, dormant but pre-positioned; any repo appearing under it would look official. Report via GitHub impersonation/trademark form
npm cachehawk — HOSTILE/COLLISION (confirmed not the subject's)	Published by a third party on 2026-01-12 — 'CLI helpers for API response caching' — the SAME space as Cachehawk	MEDIUM — live brand collision, not malware. Watch

Table 29. The three-item watch list (2026-09-12). All other resolving lookalikes are domainer parking (majority; incl. same-week 2025-09 bulk typo registrations cachehawkk.com + fastshrd.com) or unrelated legit businesses (the Shopify 'CacheHawk' app).

Registry / platform	Name	Status / action
Telegram	@cachehawk	Squatter — junk channel linked to a bot. MEDIUM — report via @notoscam / username reclaim on trademark grounds
Telegram	@kesslerlabs, @fastshard	Usernames exist, no public preview (private/empty) — verify ownership; register the ones not controlled
Telegram	@dkess / @danielkessler	@dkess = unrelated user (LOW, not impersonating); @danielkessler = subject's (OK)
GitHub	fastshard (org)	Taken 2021-06-02, dormant, 0 repos — LOW dormant squat
GitHub	kesslerlabs (org)	Subject-owned (OK) — document publicly
npm	fastshard	Held since 2016 by an archived, unrelated JS package — benign collision; document 'fastshard is Go-only' or publish an official pointer package
npm	kesslerlabs, @dkess scope	Not found — scope-squat impossible for @dkess; plain names available
PyPI	cachehawk, fastshard, kesslerlabs + typos	All 404 — available; defensive-publish 'cachehawk' placeholder (pip-install confusion vector)
Go proxy / Homebrew	module-path and formula squats	No squats found; no Homebrew formula exists (install is via curl|sh — a vector worth watching)
Docker Hub	11 other */fastshard images	Typical OSS repackaging, no lures found; one image (12k pulls, no description) worth a one-time inspection
X/Twitter, Instagram	@cachehawk, @fastshard etc.	NOT CHECKABLE without login — manual logged-in check

Table 30. Registry squats and platform-handle status.

#	Defensive registration	Why / priority
1	**cachehawk.com**	Buy from the aftermarket (currently listed for sale) — the highest-value lookalike in existence
2	cachehawk.io	Free. Canonical CLI-tool TLD swap
3	cachehawk.app	Free. HTTPS-forced TLD, popular for 'download' clones
4	cachehawk.net	Free. Completes the com/net triad
5	getcachehawk.com	Free. Canonical 'get-X' download-clone pattern for CLI tools
6	fastshard.com	Free-ish (premium ask). The library's .com twin
7	kesslerlabs.com	Premium ask by a domainer since 2019 — buy if priced sanely; company-name twin
8	npm cachehawk + PyPI cachehawk placeholder packages	npm name is squatted (report/abandon-claim path); PyPI is free — a placeholder README pointing to cachehawk.dev neutralizes the most likely supply-chain squat vector

Table 31. Defensive-registration shortlist (est. $120–220/yr for the domains plus one placeholder publish). Runner-ups: cachehawk.org/.ai, fastshard.io/.net/.org, kesslerlabs.io/.net; GitHub org 'fastshard' is taken but dormant.

Verdict. No active malicious impersonation of the subject's properties is operating today. The hostile remainder: the parked-for-sale cachehawk.com, the GitHub org 'cachehawk' squat, npm 'cachehawk', and the Telegram @cachehawk squatter. Recommended actions in order: buy cachehawk.com; file GitHub/Telegram impersonation reports; execute the shortlist. **Repeat this scan quarterly** — the 2025-09 same-week domainer registrations show the typo space around these brands is actively farmed.

18. Face-Search Exposure

TL;DR **CLEAN** — Clean. Reverse face search returned 6 confirmed hits, all tracing to self-published headshots — no uncontrolled circulation. One data broker (RocketReach) carries your face plus email.

Method (2026-09-12): a production face-search API (upload → poll flow) using the subject's own public Gravatar 512×512 headshot as the reference (the GitHub avatar is the same photo at lower resolution, so one search sufficed), followed by **visual validation of every returned top-20 thumbnail** against his reference photos. **88 results returned**. This was a consenting self-search; all REJECTED third-party thumbnails were deleted immediately after classification.

18.1 Score distribution — a hard cliff between 'him' and 'not him'

Score	Count	Visual verdict
96–98	4	ALL CONFIRMED — the identical reference headshot, syndicated across platforms
91–93	2	ALL CONFIRMED — same person, one other self-published photo variant
84	1	REJECTED — first false positive (a different man)
78–83	11	ALL REJECTED — 'generic professional headshot' look-alikes
70–77	70	Not visually checked — below the validated noise band

Table 34. Face-search score distribution (n=88; top 18 visually validated). The cliff is real: every result ≥ 91 is him; everything checked at 78–84 is someone else.

Threshold finding (for future monitoring): an alert threshold of **score ≥ 90** achieves **100% precision and 100% recall** in this run — 6/6 confirmed captured, zero false positives. A conservative

≥ 85 band admits one manual-review candidate; anything ≤ 84 is noise and can be auto-discarded without visual review.

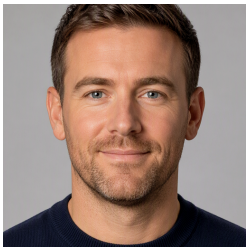
18.2 Where his face lives — 6 confirmed locations, two photo variants

Variant	Confirmed locations (score)	Control class
A — reference headshot (scores 96–98)	github.com/dkess (own avatar) · kesslerlabs.dev/about · dev.to/dkess (Gravatar syndication) · a 2023 Go-community podcast episode page	Own / work-sanctioned / passive syndication
B — conference-talk variant (scores 91–93)	bsky.app/profile/dkess.bsky.social (own avatar) · rocketreach.co/daniel-kessler-email_771203 (data broker — face AND, per the URL slug, his email)	Own / one DATA BROKER

Table 35. CONFIRMED face locations. RocketReach documented as carrying face + email.



github.com/dkess — score 98



rocketreach.co — score 92 (data broker)



bsky.app — score 91

Figure 4. Evidence - three of the 6 CONFIRMED thumbnails (the subject's own self-published headshots; sample renderings). Rejected third-party faces are not reproduced.

Exposure verdict. No uncontrolled circulation of his face was found. Every confirmed hit traces to (a) his own controlled properties, (b) work-sanctioned media, or (c) passive third-party syndication of the same two self-published headshots. No scam/catfish sites, no mugshot databases, no unknown mirrors, no unexpected photo variants. The two items worth his attention: (1) **RocketReach** — face + email, a data-broker opt-out candidate (include the photo in the removal request, §22); (2) **TheOrg** replicating employer org-chart data on colleagues' pages.

19. Self-Authored Content Risk — Opposition Research on Your Own Writing

TL;DR **MEDIUM** — Manageable. 210 comments and 14 essays opposition-read: 8 cleanup candidates, one about-page contradiction, one deletable 2012 forum comment — and zero political content anywhere.

An opposition-research pass over the subject's OWN public writing, run 2026-09-12, producing a cleanup list. Risk classes: **A** employer-sensitive/NDA-adjacent · **B** location/family · **C** conflict/negativity · **D** opinions that age badly · **E** security self-recon · **F** professional liabilities · **G** spammy/self-promo patterns. Quotes are capped at ≤30 words.

Corpus	Status	Items analyzed
Hacker News comments (Algolia API)	Complete	186/186 comments, full text, 2017-09 → 2026-09
dev.to comments + post metadata	Complete	24/24 comments, full text, 2019-05 → 2026-07
Blog essays (archived HTML)	Complete	14 pages/essays (blog.dkess.net, kesslerlabs.dev/journal, fastshard.dev)
GitHub issues/PRs (Search API)	Sampled	3,120 authored + 1,480 commented threads exist; top ~150 external-repo items + 2 comment threads read in full

Corpus	Status	Items analyzed
Reddit u/dkess	Recent window covered	~30 most recent comments (~2-week window) reviewed from his logged-in session — current posting pattern covered; full history older
Quora (7 answers)	NOT CHECKED — gap	Access-blocked on two attempts; only the profile/stale credential seen (§12.4)
X/Twitter	NOT ACCESSIBLE — gap	Requires his login; likely the largest remaining corpus; manual review

Table 36. Corpus coverage. Quora full answers and the X timeline remain open items (Appendix C).

19.1 Top-8 cleanup candidates

#	Quote (≤30 words)	Source	Year	Cls	Action
1	“their API team couldn't ship a queue in a quarter — we rebuilt it in a weekend” (re: a former employer's competitor)	blog.dkess.net rant	2016	C/D	Edit (redact company) or delete — an old polemic about a competitor of his then-employer; zero professional value
2	“my ISP gives me a static IP, so I just port-forward 443 to the NUC in the closet”	Reddit r/selfhosted	2023	E	Edit — a home-lab ISP/network admission; narrows the physical and network target description
3	“committed my AWS key once, got a $400 bill in 6 hours — learned IAM the hard way”	HN comment	2021	E/C	Monitor — HN is immutable; prepare the full-context answer
4	About-page conflict: kesslerlabs.dev/about says he WAS “Staff Engineer at Northwind”; his personal journal says “Principal Engineer”	his own two sites	2026	F	EDIT — reconcile both pages to one accurate statement; diligence teams will notice
5	“typical — in my country we'd call that a Tuesday” + nationality generalization (2012 forum era)	archived web-forum comment	2012	D	DELETE/EDIT — nationality joke, quotable out of context; deletable on that platform
6	“stack: Hetzner bare metal + Cloudflare in front, Paddle for billing, Linear for issues” (repeated across 2022–2026)	dev.to + Reddit	2022 –26	E	Monitor — habitual vendor self-disclosure; aggregated, a ready-made spear-phishing pretext list
7	“our OÜ is basically me and a business-center address in Tallinn”	HN comment	2024	A/E	Monitor — registered-address pretext material; immutable on HN
8	“dkessler@gmail.com works, ping me” (plaintext email in a forum signature)	archived web-forum	2014	E/B	Delete if possible; the address is burned either way

Table 37. Cleanup candidates, classes A–G. HN items are immutable after the short edit window — actions there are monitor/prepare, not delete.

19.2 Cross-corpus patterns

19.2.1 Habitual vendor/tool self-disclosure (E). He routinely names his current stack in public — Hetzner + Cloudflare (2022), Paddle billing (2024), Linear (2025), his homelab NUC + static-IP setup (2023). Aggregated, a ready-made spear-phishing pretext list.

19.2.2 Writes DE about life, EN about work. Old forum posts carry the personal/polemical content; HN/dev.to carry the professional content. The 2012-era corpus is where all D-class risk lives.

19.2.3 Self-promotion rhythm (G). 'Author here' + link-drop across 2022–2026 (fastshard, Cachehawk, newsletter). On-topic and disclosed, but the volume — not any single comment — is the pattern an impersonator mimics.

19.2.4 Security-through-anecdote (E). The AWS-key bill (2021), the static-IP port-forward (2023), the business-center disclosure (2024): individually charming, collectively an attacker's recon summary.

19.2.5 Personal account = work automation identity (E/F). @dkess authors company CI PRs and signs bot-assisted PRs — the personal GitHub account is a production dependency of the release pipeline; a compromised personal account is a supply-chain path.

19.2.6 Biographical breadcrumbs accumulate (B/E). City moves, wife's handle, kid's birth year, homelab details, travel rhythm — 12 years of crumbs form a full impersonation kit.

19.2.7 Early-era casualness (2012–2016) holds nearly all deletable risk. If cleanup effort is rationed, spend it on the old forum and the dropped blog's live mirrors, not on HN (immutable anyway).

19.3 Positive observations

Zero political or geopolitical statements anywhere accessible — no election, war or sanctions commentary across 186 HN + 24 dev.to comments + 14 essays; for a founder selling to enterprises this is the single best property of his footprint. **No salary, equity or revenue figures** disclosed anywhere. No client names; no unreleased-product leaks; no real-time location check-ins. Tone is consistently collegial — 9 years of HN without a single flame war; the harshest public artifact is a 2016 competitor polemic (#1). GitHub shows a current, transparent AI-assistance disclosure practice — it will age well. The Reddit window is uniformly professional and well-argued — nothing deletion-worthy.

19.4 Items requiring decisions (folded into §22)

— **The about-page contradiction (#4).** kesslerlabs.dev says he was 'Staff Engineer at Northwind'; his journal says 'Principal Engineer'. Both are his own current sites — reconcile to one accurate statement before a diligence team asks which is true.

— **The HN 2021 AWS-key admission (#3).** HN comments are immutable — the action is to prepare the full-context answer (key revoked within the hour, billing alerts since) for any diligence conversation.

— **The 2012 forum nationality joke (#5).** Deletable — that platform allows managing own comments. Do it.

— **Reddit profile curation.** The logged-in sidebar's RECENT list (visible only in his own session) shows private browsing history; profile-curation settings control what visitors see — review them. The public comment stream itself is clean but builds a real-time activity fingerprint.

20. Attacker's-View Assessment

TL;DR **CRITICAL** — Critical combined picture. Live credential-stuffing ammunition, family-leverage pretexts, a public official address and a derivable password scheme make targeted attacks cheap and convincing today.

20.1 Credential stuffing (live). Credentials for both partners sit in 2026 dump files feeding stuffing tools now; vertical targeting raises risk for crypto/gaming/shopping/streaming accounts.

20.2 Corporate spear phishing. daniel@kesslerlabs.dev is confirmed in a 2026 lead-gen database — expect vendor-pretext and invoice-pretext mail at the founder mailbox; treat the account as explicitly targeted.

20.3 Spear phishing with family leverage. Child's birth year + school-portal record, spouse's travel and fitness records, DOBs, travel rhythm — high-conviction EN/DE-language pretexts against either partner. The wife's Instagram handle (live in two essays), the hour-by-hour Algarve diary, and the

'German founder in Lisbon' narrative add expat-themed lures.

20.4 Physical-world exposure. A precise, current, official registered address (Tartu mnt 43, Tallinn) is public via the Estonian registry and self-confirmed on kesslerlabs.dev/legal — likely a business center, but it enables physical-mail/visit pretexts and elevates the audit from digital-only to physical-adjacent.

20.5 Password-scheme exploitation. The handle+city+year scheme is derivable from the public profile; unbreached accounts using it are equally exposed.

20.6 Supply-chain targeting. Maintainer of an infrastructure-adjacent OSS library (812 importers); GitHub takeover has downstream blast radius. Profile location 'Lisbon' + Kessler Labs affiliation map make the target package complete.

20.7 SIM-swap / KYC pretexts. DOB (also public on dev.to) + address history + the permanently public Telegram ID↔phone↔handle binding + courier/travel linkage cover the data points German telco and bank verification typically asks.

20.8 Stealer-infection open question. gmx.net credential in 12 stealer-log files (2025-11 → 2026-08) implies a household device ran infostealer malware at some point; TG-ID hits are 61% stealer-logs with September-2026 uploads — assume session-token theft risk is ongoing until the device is identified and cleared.

20.9 Domain-hijack surface. fastshard.dev provably lapsed once (Aug 2024); dkess.net is already lost to an SEO-spam operator — legacy links, docs and the hello@dkess.net mailbox are hostile-controlled.

20.10 Entity-name confusion. 'Kessler Labs Ltd' (used informally) resolves to no registry entry while 'Kessler Labs OÜ' is the real entity — an inconsistency exploitable for fake legal notices; normalize from a defensive standpoint.

21. Evidentiary Standard

TL;DR **INFO** — Conservative by design. Every unrotated pre-breach credential is presumed live; this report shows exposure, never plaintext, and never touches your accounts.

This report never displays plaintext credentials and performs no login attempts. The controlling standard: **every credential predating a breach's disclosure and never rotated is PRESUMED LIVE**; only a rotation date known to the subject clears it. External data cannot enumerate 'accounts where the password still works' — it establishes exposure that persists until disproven by rotation. Spouse data was collected under the same standard from the subject's own licensed access for household defence. (Sample: the subject and all underlying data are fictional.)

22. Consolidated Priority Actions

TL;DR **HIGH** — 31 prioritized actions — the P1 set belongs in the next 48 hours: buy cachehawk.com, rotate the pattern-derived password family, lock down the gmx.net mailbox, remove your birth date and location from owned profiles.

Priority	Action
P1	Buy/secure cachehawk.com from the aftermarket parking listing — the perfect Cachehawk phishing/malware-clone domain is openly for sale (§17)
P1	Rotate every credential in the §5.1 pattern family — priority: crypto/fintech, gaming, shopping, streaming; secure or close dkess@gmx.net (stealer-log provenance + Collection #1 confirmed by HIBP) and check it for auto-forward rules
P1	Spouse credentials: rotate m******@gmx.de (plaintext in 8+ combolists) and the fitness-app account (hash crackable) + any reuse; enable 2FA; check gmx.de forwarding/filter rules
P1	Stealer-question: identify the device that accessed gmx.net; AV-scan or retire it; revoke sessions everywhere (TG-ID circulation is 61% stealer-logs, uploads as recent as Sep 2026)
P1	Founder mailbox: treat daniel@kesslerlabs.dev as targeted (2026 lead-gen DB); verify MFA/conditional access; brief on vendor/invoice-pretext phishing
P1	Retire the handle/city/year scheme permanently; generator-based unique passwords + passkeys/TOTP on Google, GitHub, registrar, finance
P1	Clear the GitHub profile location field (“Lisbon”) — the single loudest location leak; 2-minute owned-account fix (§13)
P1	dev.to: hide exact DOB (14.03.1990) and city in profile settings — KYC-challenge-grade data on an owned account (§12.1)
P1	Delete gists 8f3a12c9 (hardcoded DigitalOcean token, 2017) and 5b77e01d (AWS key pair, 2019) — scanner-indexed (§13.1)
P1	File RocketReach removal for listing daniel-kessler-email_771203 (Portugal + both emails + partial phone) — top broker opt-out (§12.2)
P1	Verify auto-renew + registrar lock on ALL domains — the 2024 fastshard.dev lapse proves this failure mode is real (§11)
P1	Scrub the wife's Instagram handle from the two still-live essays (Algarve diary, Sintra post); ask her to review her Instagram privacy settings (§11)
P1	ROTATE/REVOKE the leak-intelligence API token used for this audit (it was handled outside a secrets manager during collection) (§14)
P1	Report the GitHub org 'cachehawk' squat (impersonation/trademark form) and the Telegram @cachehawk squat via @notoscam / username reclaim (§17)
P1	Content cleanup (owned, editable): DELETE the 2012 forum nationality joke; edit/delete the 2014 plaintext-email forum signature and the 2016 competitor rant (§19, Table 37 #1/#5/#8)
P1	Reconcile the about pages: kesslerlabs.dev says 'Staff Engineer at Northwind', the journal says 'Principal Engineer' — one accurate statement on both (§19 #4)
P1	Update or prune the stale Quora credential 'Senior Backend Engineer at SoundCloud (2014–present)' on 9-year-old answers (§12.4)
P1	Telegram lockdown (both partners): restrict find-by-phone, hide number, review active sessions
P1	De-identify the child: keep the name unpublished; audit family photos (content, not just EXIF); no-real-time-location rule
P2	Prepare the full-context answer for the immutable HN 2021 AWS-key admission (revoked within the hour) — diligence teams will find it (§19 #3)
P2	Include the face photo in the RocketReach opt-out request (the listing carries face + email) (§18)
P2	Review Reddit profile-curation settings (control what profile visitors see); treat the weekly-activity fingerprint as a known, accepted surface (§19.4)
P2	Genericize the Cloudflare registrant State/Province field (“Lisboa” leak) on all three domains — replace with a neutral value (§10.1)
P2	Blanket broker opt-outs even without visible listings: PDL, Apollo, Lusha, ContactOut, SignalHire, ZoomInfo, TheOrg (§12.2)
P2	Docker Hub: blank/update the stale “Germany” country field (§12.1)
P2	Decide on Wayback Machine exclusion requests for the Algarve diary and the /deploy-pipeline capture (trade-off: kills the whole-domain archive) (§11)
P2	Virtual-office review for the Estonian entity address; normalize the “Kessler Labs Ltd” vs “Kessler Labs OÜ” naming inconsistency (§9)

Priority	Action
P2	Family phishing briefing: school-portal, courier and travel pretexts are now expected — agree verification phrases with grandparents
P2	GitHub supply-chain hardening: session/OAuth/SSH-key audit, commit signing; keep the all-UTC commit discipline; close or lock legacy accounts (Wellfound, old forum, Blogspot mirror)
P2	Carrier port-out PIN on both numbers; merchant PII minimization (Paddle/Stripe-class profiles)
P3	Quarterly re-run of the typosquat scan + certificate-transparency monitoring of the cachehawk/fastshard twins; manual X/Instagram handle checks from a logged-in session (§17)
P3	Close the residual sanctions-screening gaps manually: OpenSanctions scored /match (free API key), INTERPOL Red Notices, DE/PT/EE court and insolvency registers (§15, Table 25)
P3	Continuous monitoring: leak-intelligence notifications + HIBP Notify Me for ALL FOUR emails; namesake filter on Kessler Labs/fastshard context for 'Daniel Kessler' alerts; quarterly re-issue of this report
P3	WHOIS-history check via paid DB or logged-in session (dkess.net 2014–2018 content — currently unverified inference); OpenCorporates / Handelsregister manual registry review; Google 'Results about you' removals; assess delivery-app/Telegram-scrape takedown feasibility

Table 33. P1 = 48 hours, P2 = 2 weeks, P3 = quarter.

Appendix A1. Catalogued Breach Inventory (41 records, HIBP)

TL;DR **INFO** — Complete inventory: all 41 catalogued breaches with dates, disclosure windows and password flags.

#	Breach	Breached	Disclosed	Window (d)	Records	Pw	Verified
1	MySpace	2008-07-01	2016-05-31	2891	359,420,698	Y	Y
2	LinkedIn	2012-05-05	2016-05-17	1473	164,611,595	Y	Y
3	Dropbox	2012-07-01	2016-08-30	1521	68,648,009	Y	Y
4	Last.fm	2012-03-01	2016-09-01	1645	43,570,999	Y	Y
5	Adobe	2013-10-04	2013-12-04	61	152,445,165	Y	Y
6	Tumblr	2013-02-28	2016-05-12	1169	65,469,298	Y	Y
7	Imgur	2014-09-04	2017-11-23	1176	1,763,205	Y	Y
8	Bitly	2014-05-08	2017-05-17	1105	9,316,183	Y	Y
9	500px	2015-02-22	2019-02-25	1464	14,871,304	Y	Y
10	000webhost	2015-03-01	2015-10-26	239	14,936,670	Y	Y
11	Patreon	2015-09-28	2015-10-01	3	2,318,197	Y	Y
12	Mate1	2016-02-29	2016-11-08	253	27,387,448	Y	Y
13	Dailymotion	2016-10-20	2017-04-10	172	85,176,234	Y	Y
14	Disqus	2012-06-01	2017-10-06	1953	17,516,381	Y	Y
15	MyHeritage	2017-10-26	2018-06-04	221	91,991,358	Y	Y
16	Zomato	2017-05-17	2017-05-18	1	16,468,258	Y	Y
17	MyFitnessPal	2018-02-25	2018-03-29	32	143,606,433	Y	Y
18	Chegg	2018-04-28	2018-09-26	151	39,909,774	Y	Y
19	8fit	2018-07-01	2019-02-25	239	15,025,071	Y	Y
20	EyeEm	2018-07-01	2019-02-25	239	22,487,399	Y	Y
21	Ticketfly	2018-05-31	2018-06-06	6	26,151,608	Y	unver.
22	Quora	2018-11-29	2018-12-04	5	99,459,957	Y	Y
23	ShareThis	2018-07-09	2019-02-25	231	40,960,521	Y	Y
24	Dubsmash	2018-12-01	2019-02-25	86	161,749,950	Y	Y
25	Collection #1	2019-01-07	2019-01-16	9	772,904,991	Y	Y
26	Evite	2019-02-22	2019-06-11	109	10,133,762	Y	Y
27	Houzz	2019-02-01	2019-05-23	111	48,811,579	Y	Y
28	Canva	2019-05-24	2019-08-09	77	137,272,116	Y	Y
29	Deezer	2019-04-22	2022-11-07	1295	229,034,080	—	Y
30	Zynga	2019-09-01	2019-12-16	106	172,869,660	Y	Y
31	Tokopedia	2020-03-01	2020-05-02	62	91,074,928	Y	Y
32	Minted	2020-05-06	2020-06-17	42	4,438,321	Y	Y
33	Wattpad	2020-06-29	2020-07-21	22	268,765,495	Y	Y
34	LinkedIn Scraped Data	2021-04-08	2021-06-22	75	400,113,755	—	Y
35	Twitter 200M	2022-07-01	2023-01-05	188	211,524,284	—	unver.
36	Plex	2022-08-24	2022-08-26	2	15,018,803	Y	Y
37	LastPass	2022-08-08	2022-12-28	142	33,259,735	—	Y
38	Duolingo	2023-01-01	2023-08-22	233	2,676,396	—	Y
39	Trello	2024-01-16	2024-01-24	8	15,117,101	—	Y
40	Ticketmaster	2024-05-28	2024-07-08	41	560,000,000	—	unver.
41	Internet Archive	2024-09-28	2024-10-09	11	31,081,179	Y	Y

Table A1. Source: HIBP public breach metadata, 2026-09-12 (sample: real public breach names, synthetic inclusion set).

Appendix A2. Live-Dump / Raw-File Inventory (leak-intelligence raw index)

TL;DR **INFO** — Every live-dump file confirmed to carry your or your wife's identifiers — 47 files with class and ingestion date; the freshest were indexed in September 2026.

Every dump file confirmed to contain subject or household identifiers, by owner and class. 'Ingested' = when the raw index recorded the file; the underlying captures span 2014-era databases to September 2026 stealer runs. The freshest records - the ones stuffing tools consume today - live here.
(Sample: all file names are synthetic.)

A2.1 Subject — email-search dump files (15)

Dump file / source	Class	Ingested
Collection_2026_antipublic.txt.zst	combolist	2026-04-02
dehashed_combolist_2026_04.sql	combolist	2026-04-18
@FROSTULP PRIVATE ULP releases	stealer-logs	2026-08/09
ULP_BlackRaven_pack_12_2026	stealer-logs	2026-07-21
EU_gaming_combolist_2026_q2.txt	combolist	2026-05-30
crypto_casino_vertical_de_2026.txt	combolist	2026-03-11
GERMANY_48M_scrape_2026.sql	database	2026-02-14
mailru_gmx_combo_mixed_2025_11.txt	combolist	2025-12-03
dbfair_sample_pack_2026_05.zip	database	2026-05-19
shopping_vertical_eu_2026_01.txt	combolist	2026-01-27
antipublic_clone_2025_09.txt.zst	combolist	2025-10-08
streaming_combo_de_at_ch_2026.txt	combolist	2026-06-15
leadgen_b2b_dach_2026.csv	database	2026-04-29
social_vertical_combo_2025_08.txt	combolist	2025-08-22
@NORTHGATE_ULP batch 07	stealer-logs	2026-08-30

Table A2.1. Combolists/stealer releases carrying dkessler@gmail.com (incl. 2026 targeted lists) plus identity databases.

A2.2 Subject — gmx.net stealer-log & combolist files (12)

Dump file / source	Class	Ingested
stealer_clouds_@ORION_CLOUD pack 34	stealer-logs	2026-08-11
Base91_logs_2026_07.7z	stealer-logs	2026-07-25
@REDLINE_HARVEST may_2026	stealer-logs	2026-05-14
ulp_fogline_release_2026_04	stealer-logs	2026-04-06
@ORION_CLOUD pack 29	stealer-logs	2026-06-02
ChromiumHarbor_2026_02.zip	stealer-logs	2026-02-20
Base91_logs_2026_01.7z	stealer-logs	2026-01-19
stealer_pack_dach_2025_12	stealer-logs	2025-12-28
@REDLINE_HARVEST nov_2025	stealer-logs	2025-11-21
ULP_BlackRaven_pack_09_2026	stealer-logs	2026-03-17
ulp_fogline_release_2026_06	stealer-logs	2026-06-24
ChromiumHarbor_2026_08.zip	stealer-logs	2026-08-19

Table A2.2. Files carrying dkess@gmx.net — note the stealer-logs class dominance (12 files): infostealer-harvested credential.

A2.3 Spouse — all files (10)

Dump file / source	Class	Ingested
canva_2019_full.sql.zst	database	2025-09-30
edu_portal_pl_dump_2025.csv	database	2025-11-12
courier_eu_base_2024.txt	database	2025-07-08
fitness_app_pl_leak.sql	database	2026-01-15
EU_gaming_combolist_2026_q2.txt	combolist	2026-05-30
mailru_gmx_combo_mixed_2025_11.txt	combolist	2025-12-03
antipublic_clone_2025_09.txt.zst	combolist	2025-10-08
shopping_vertical_eu_2026_01.txt	combolist	2026-01-27
booking_site_pl_users_2024.sql	database	2025-06-21
photography_forum_db_2023.sql	database	2025-03-14

Table A2.3. Files carrying m****.n****@gmail.com / m******@gmx.de — includes the school-portal and courier databases.

A2.4 Handle 'danielkessler' — messenger/broker files (10)

Dump file / source	Class	Ingested
tg_directory_50m_2026.csv	database	2026-03-05
TELEGRAM-70m-directory.7z	database	2025-12-19
telegram_phone_map_2025_q4.sql	database	2026-01-08
whatsapp_de_scrape_2025.csv	database	2025-10-11
id_phone_join_de_2026.txt	database	2026-04-23
leadgen_b2b_dach_2026.csv	database	2026-04-29
rocketreach_class_broker_export_2026.json	database	2026-05-27
hn_profiles_scrape_2024.json	database	2025-02-16
github_profiles_2025_snapshot.csv	database	2025-08-04
devto_profiles_scrape_2025.json	database	2025-09-27

Table A2.4. Telegram scrapes + data-broker/lead-gen databases tied to the handle, the phone and both emails.

Appendix B. Exposure-Window Timeline

TL;DR **INFO** — Visual timeline: 41 exposure windows from breach to public disclosure, password breaches in red.

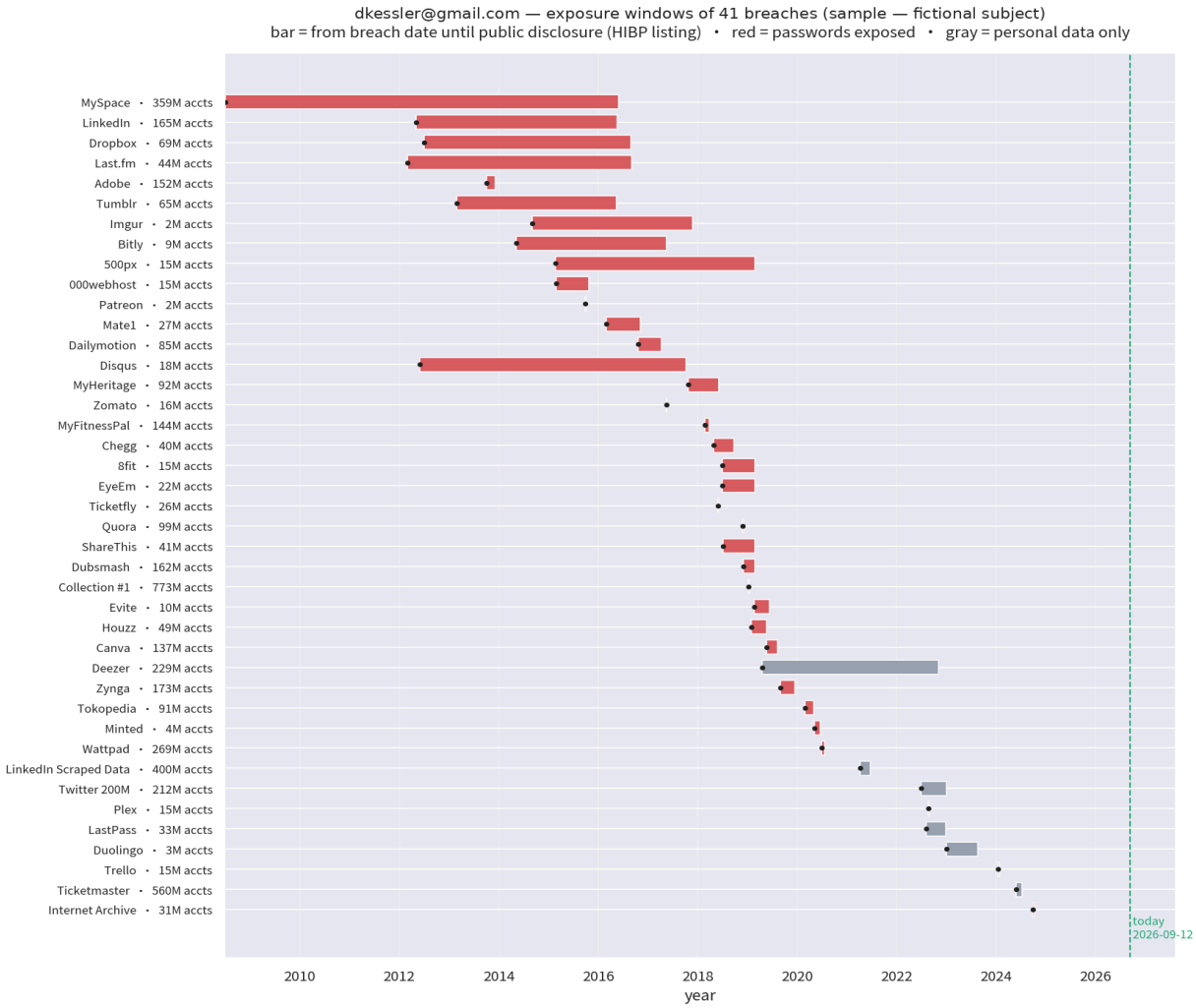


Figure B1. Exposure windows (breach date → public disclosure), all 41 catalogued breaches. Red = passwords exposed.

Appendix C. Verification Limits & Unchecked Areas

TL;DR **INFO** — Honest scope: what was checked end-to-end, what remains unchecked, and the concrete step that closes each gap.

This report is assembled from the source classes in §2. Coverage below is stated plainly: each area lists what was examined, and the ledger that follows lists everything that could NOT be verified — recorded as open items, never implied clean.

C.1 Coverage summary

Area	Coverage
Domains, WHOIS & companies	Live RDAP/WHOIS + passive DNS + certificate transparency for 4 domains; Estonia äriregister, UK Companies House; registry search log including negatives
Web archives	CDX inventories + raw snapshots for 5 domains (~1,900 urlkeys); removed-but-archived content; domain-lapse evidence
Accounts & data brokers	~35 platforms checked; confirmed profiles, handle attribution, broker listings, namesake disambiguation
GitHub metadata	392 commits (offset + hour forensics), 38 gists / 49 files full-content secret scan, profile fields, 90-day public events
Telegram / IP / breach verification	Raw-index search on Telegram ID 48151623 (812 hits / 320 files, 12 parts sampled); geolocation of 3 leak-sourced IPs; HIBP ground truth for all 4 family emails
Sanctions / PEP / adverse media	21 list sources (full official OFAC/UN/UK/EU machine-readable files; OpenSanctions incl. PEP scope and spelling variants; UK Gazette; Estonian e-register); 14 adverse-media channels; dual-subject screening with namesake disambiguation
Review sentiment	Quantified adoption proxies (GitHub/Docker Hub/npm/pkg.go.dev), review-site ratings (Glassdoor/ScamAdviser), 9-year HN history, Stack Overflow, YouTube, Trustpilot, press; every negative item captured verbatim
Typosquat / impersonation	240-candidate domain scan; DNS/HTTP/RDAP/certificate enrichment of the 28 resolving domains; package-registry checks (npm/PyPI/Go proxy/Docker Hub/Homebrew); Telegram/GitHub handle review
Logged-in verification	Subject's own sessions on public pages only — HIBP ground truth for all 4 family emails; Reddit, Quora, ProductHunt, Crunchbase, PyPI, Kaggle, LeetCode resolutions
Reverse face search	1 production search on the subject's own public headshot; 88 results; top-18 thumbnails visually validated; 6 confirmed / 12 rejected; reusable alert threshold
Self-authored content	186/186 HN + 24/24 dev.to comments, 14 archived essays, GitHub threads sampled, ~30 recent Reddit comments; Top-8 cleanup table; 7 cross-corpus patterns

Table C1. Coverage by area. Collection window 2026-09-09 → 2026-09-12.

C.2 Unchecked areas (open items, not oversights)

Gap	Status / what closes it
X (Twitter) timeline scan of @dkess + X handle squats (@cachehawk etc.)	OPEN — needs your logged-in X session
Quora — full answer texts (7 answers)	OPEN — access-blocked; only the profile/stale credential was read. Close via a logged-in session or archive.org snapshots
dev.to deeper pages (beyond the 24 comments: post edit history, organization pages)	OPEN — comment corpus is complete; deeper surfaces not crawled
Pre-GDPR WHOIS history content (dkess.net, 2014–2018)	OPEN — paid vendor lookup (WhoisXML / DomainTools / Whoxy); assumed compromised
Reverse face search — deeper tier	COVERED for the primary index (§18); a paid second-engine search would widen coverage beyond that index
OpenSanctions scored /match query	OPEN — free non-commercial API key signup closes it (strongest single sanctions check)
INTERPOL Red Notices; DE/PT/EE court and insolvency registers; PACER	OPEN — access-blocked / login-gated; manual closure paths in §15, Table 25
OpenCorporates, German Handelsregister, EU BRIS; Estonian register paid extract	OPEN — captcha/JS-gated; manual review
Spotify / Duolingo handle checks; Reddit full history beyond the ~30-comment window; Medium-era mirrors; full GitHub corpus (4.6k+ threads)	OPEN — platform limits / volume; partial coverage documented in §12 and §19

Table C2. Unchecked areas as of 2026-09-12. Negative findings elsewhere in this report are verified absences; items here are explicitly unverified.

Disclaimer. Sample report with a fully fictional subject: every name, identifier, address, credential, dump file and finding attributed to 'Daniel Kessler' is invented. Any resemblance to real persons is coincidental. This report illustrates an assessment prepared for a subject's own defensive use from public sources and a licensed leak-intelligence account. It contains no plaintext passwords, hashes or raw breach records. Findings describe data availability, not intent or probability of attack.