Private Key Leaks in the Wild

Insights from Certificate Transparency

Philippe BONEFF - **Gaetan FERRY** - David TAO - **Guillaume VALADON**

$ whoami

Guillaume

Cybersecurity Researcher

editor-in-chief of the **MISC magazine**

Scapy maintainer

previously at **Quarkslab,** ANSSI…

Gaetan

Cybersecurity Researcher

former researcher **@Sonar**

Synacktiv red teamer for 7 years

01

Private Key Leaks and Certificate Transparency

From unknown keys to identities

Leaks Everywhere You Look

Public secrets leaks an **underestimated problem**

29 millions

secrets leaked on GitHub in 2025

⬆️ 34% increase from 2024

430,000

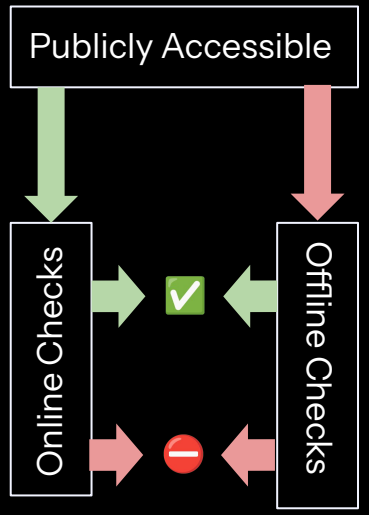
private keys included

From Private Key Leaks to Critical Threats

mathematical objects
several use cases: TLS, GPG, SSH, software signatures...

X.509 certificates assign an identity to the public part
as well as other metadata: issuer, validity, usages..

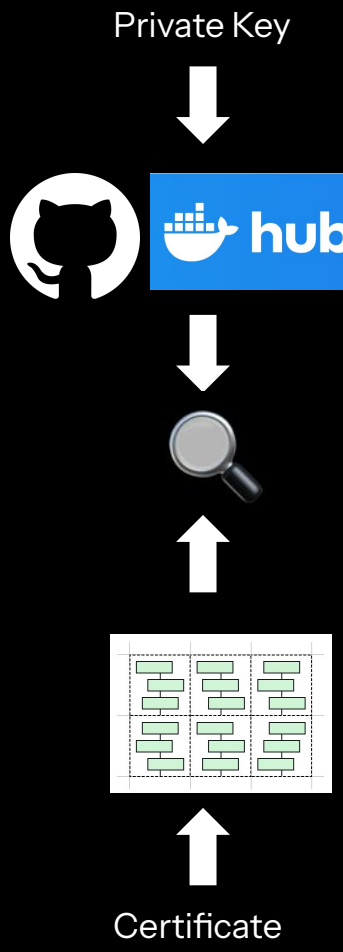
with TLS, a private key leak is critical
attackers can impersonate websites, manipulate data...



Certificate Transparency

a public historical database of issued certificates
in use since 2015 by the main CAs

CT is a game changer for ownership attribution
a list of public key & identities
ready to be mapped to leaked private keys



Certificate Transparency Limitations

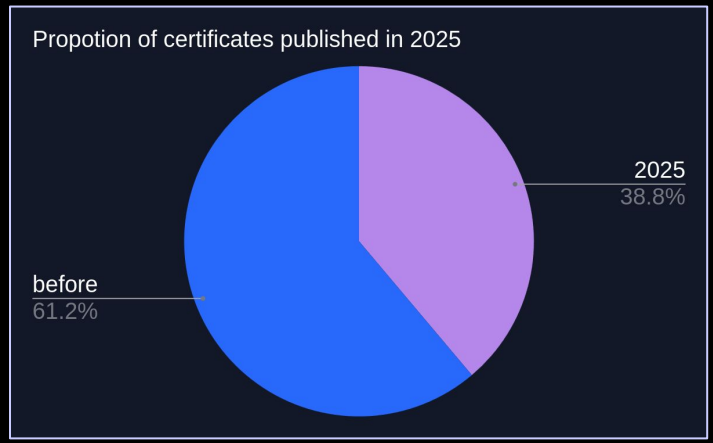
currently too big and too slow for us

38TB of certs for 2025 only
rate limiting on operators' side

in July 2025, old logs were expected to be put offline

partnered with Google

shortcut to retrieve all certificates of interest at once



02

Research Results

Charts, numbers & insights

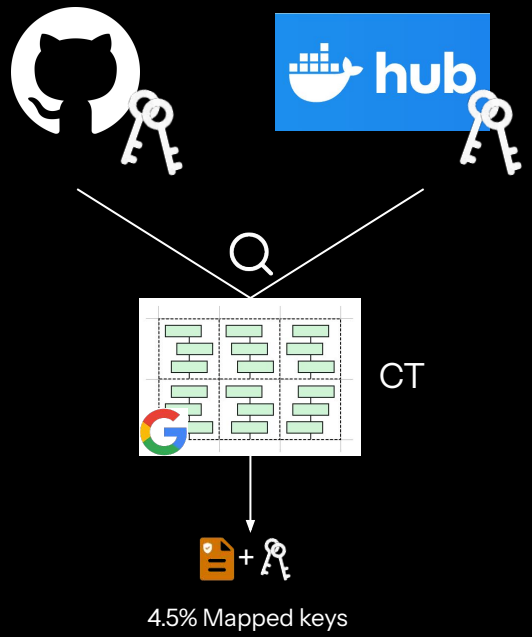
Origin of Private Keys Leaks

945,560 unique private keys
extracted in July 2025, dated back to 2021

42,690 keys attributed thanks to CT Logs
77% from GitHub - 23% from DockerHub

strong dataset bias
keys are not only used for TLS, but SSH, JWT...

139,767 unique certificates
corresponding to 36,978 subjects



Certificates Validity

2,622 valid certificates in September 2025

35% used by publicly reachable services

revocation is barely used

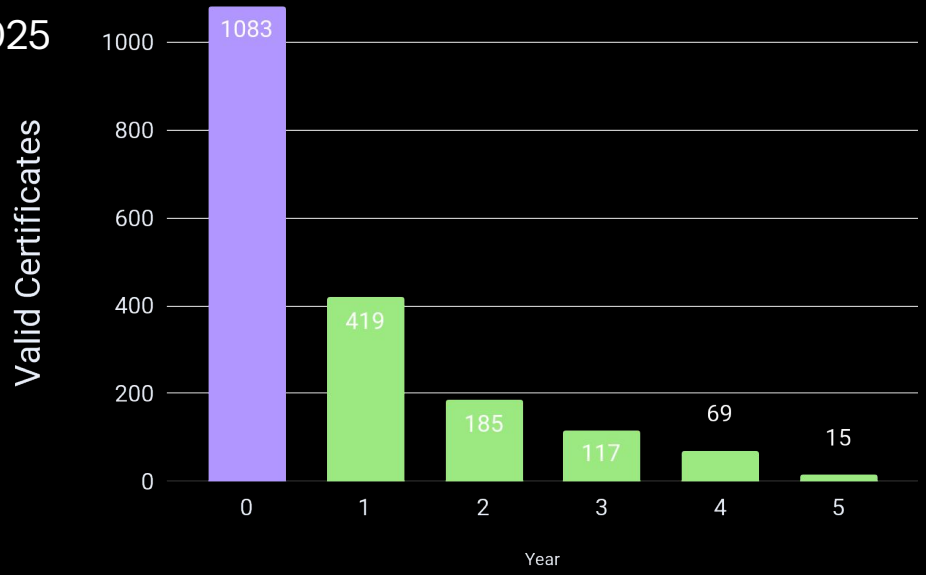
CRL: 24 invalid certificates; 1 with *key_compromise*

OCSP: 56 invalid certificates; 2 with *keyCompromise*

Durations of Exposures on GitHub

GitHub metadata allows to measure exposures
time between first public exposure and certificate expiration

recent vs. long-term exposure
43% of valid certificates' keys leaked before 2025
while 20.44% have been exposed for 2+ years



Validity at Initial Exposure

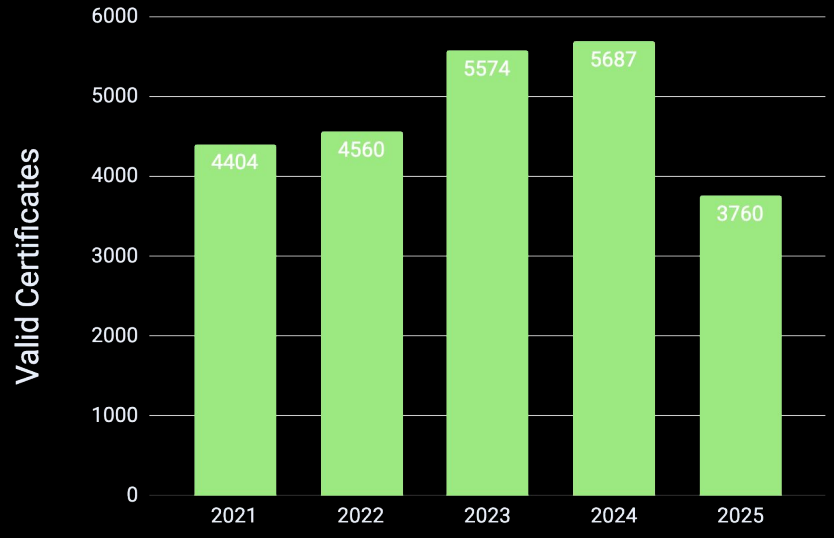
simulating validity at leak time

acknowledging that revocation rarely used

compare the leak date against the certificate's validity period

thousands of valid certificates exposed every year

17.16% of the 139,767 certificates discovered in CT



03
Disclosure Stories

Hard facts & lessons learnt

Identifying & Contacting Owners

bias to fix root causes instead of revoking
we want to fix vulnerabilities
owners need to known the bigger picture

don't break production
at GitGuardian, we know that revoking breaks production

various attributions techniques
X.509 Organizations, security.txt, Whois, MX, LLM...

600 organizations identified
1,300 certificates

4,300 emails sent
9 Bug Bounty programs

various types
19 governmental entities
several Fortune 500
1 Certificate Authority

Interesting Answers

overall poor response rate
54 answers only / 9%

low response rate for high confidence attribution
36% for companies
10% for governmental entities

shocking misunderstanding of the critical role private keys
PoC of impact requested, confusion between keys & certificates, or validity and usage

Interesting Answers

Final Assessment

The private RSA key associated with digest [REDACTED] and fingerprint [REDACTED] is no longer active on any live service. **The endpoint now serves a different certificate** and keypair (ZeroSSL ECC, valid Jan 2026) and only performs a 301 redirect to the corporate homepage.

Based on the presented evidence, this incident represents a historical exposure rather than an active security threat. **The previously exposed key is not in use, and there is no exploitable service behind the hostname.**

Contacting Certificate Authorities

contacted 9 CAs
2,193 certificates

almost immediate revocation
aligned with Certification Policy and Certification Practice Statement

not standard procedure to share findings
direct contact with proof of ownership
dedicated service (web portal or API) with a proof of ownership

no direct contact with owner
some asked to talk to use and learn about the leaks origin

Certificates	CA Name
1,264	Sectigo
366	GoDaddy
256	GlobalSign
153	Digicert
54	GoGetSSL
52	InCommon
22	SSL Corporation
22	Starfield Tech.
4	Harica
2,193	**Total**

04
Missing Pieces

How issuers and users can improve against key leaks

Users' misunderstanding needs technical resilience

complement revocation with one-time private keys
limit leak impact for users

For users: systematic private key renewal
generate a new private key as cert-bot does

For issuers: forbid key re-use at CA level
enforcing the key rotation at the CA level

20% of private keys leaked more than 2 years ago

Improving leaked keys visibility

Private keys leak, we see it, the information does not bubble up

- Leaked keys are reused
- Some leaked keys start to be used long after
- No easy way to track leaked keys

Compromised private keys logs as a way to allow keys observability

- Similar to CT: store leaked keys information in an auditable log

Proactive prevention at issuance

- Enable CAs to check for leaked keys, and blocking re-use
- Also works for cross CA private key blacklist

TLS & Certificate Transparency Evolution

OCSP deprecation
operational cost, privacy issues, cache duration…

CRLite
compact database of revoked certificates

Static CT
simplified operation and consumption of CT

Logs Archives
clone CT Logs, and store then in the Internet Archive

18.5% revoked

3% still valid
84 certificates

CRLite result on January 2026

Take-Away Messages

hard-facts

1. 2,622 valid certificates in september 2025
2. 20.44% have been exposed for 2+ years
3. low response rates to disclosures

several gaps and opportunities for improvements in the ecosystem

1. keeping the same private key exacerbates the threat of leaked keys
2. compromised Private Keys logs as a solution to the problem of private key leaks

Google's colleagues enabled this research, and we strongly encourage researchers with similar use cases to get in touch with us.

Thank you

Question time 🔥

Philippe BONEFF - Gaëtan FERRY - David TAO - Guillaume VALADON

Revocation observability

Understanding revocation usage is limited by a lack of observability

- Key for *.amlarc.microsoft.com leaked years ago
- Was the key revoked? Was the company aware of the leak?

The CT-archive project archives certificates in logs *
Let's do the same for CRLs

- Far smaller than CT logs
- Should not require much efforts

* Many thanks to Filippo Valsorda and Geomys