RISET & STUDI KASUS - TEGALSEC

SUBDOMAIN TAKEOVER AT SCALE

Ancaman Sistemik pada Ekosistem SaaS

WHOAMI

VAN LYUBOV

CCSE | CAP | CNSP | CMPEN | CAPEN | EHE | NDE

https://blog.tegalsec.org/author/dalpan//

- *Satpam di Punggawa Siber (punggawa.com)*
- *Tukang yapping di Tegalsec (tegalsec.org)*
- *Tukang bacot ke triager yang gejelas manage bug bounty program*

AGENDA

- PENGENALAN SAAS & ATTACK SURFACE
- APA ITU SUBDOMAIN TAKEOVER
- MEKANISME TEKNIS (FLOW SCANNING & DORKING)
- STUDI KASUS NYATA (TEGALSEC RESEARCH)
- TOOLS & METODOLOGI
- STRATEGI MITIGASI
- DEMO SINGKAT (OPSIONAL) + Q&A

MENGENAL SAAS (SOFTWARE AS A SERVICE)

SaaS adalah model layanan di mana perangkat lunak disediakan dan dikelola oleh penyedia layanan, serta kamu dapat mengaksesnya melalui internet menggunakan browser web. Tidak perlu lagi repot-repot menginstal atau merawat perangkat lunak di komputer kamu! Semua pembaruan dan pemeliharaan ditangani oleh penyedia layanan.

MENGAPA SAAS RENTAN?

- Banyak layanan SaaS menawarkan fitur custom domain.
- Pengguna pasang CNAME untuk menunjuk ke layanan vendor.
- Bila resource di vendor dihapus/tidak terpakai → CNAME tetap ada.
- Orphaned record = peluang takeover.

“Fitur custom domain yang memudahkan brand identity justru sering menjadi titik lemah.”

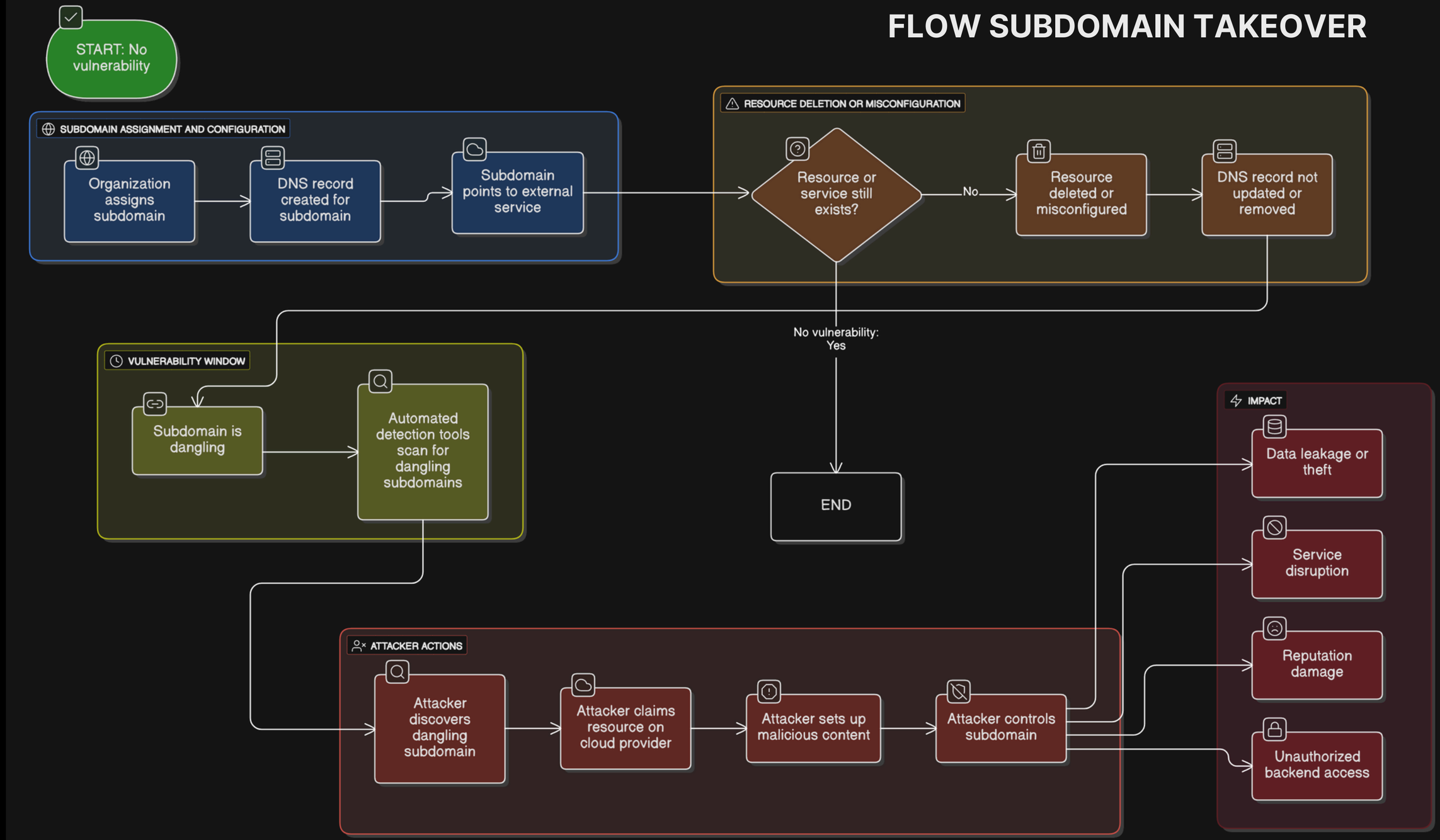
APA ITU SUBDOMAIN TAKEOVER?

Subdomain takeover terjadi ketika subdomain masih memiliki DNS record yang menunjuk ke layanan pihak ketiga, tetapi resource tersebut sudah tidak aktif - sehingga attacker bisa mengklaim ulang dan mengontrol subdomain itu sepenuhnya

JENIS-JENIS SUBDOMAIN TAKEOVER

- Orphaned CNAME: resource vendor dihapus tapi DNS tetap.
- Vendor misconfiguration: verifikasi domain lemah (mis. TXT verification bypass).
- SaaS chaining: vendor berantai (mis. Hashnode ↔ Vercel).
- Wildcard/Expired resources: akun atau project expired tanpa cleanup DNS.

FLOW SUBDOMAIN TAKEOVER



DAMPAK & KENAPA INI SISTEMIK

- Phishing (pelanggan/pekerja melamar kerja palsu)
- Reputational damage (brand abuse)
- Supply-chain contagion (satu vendor mempengaruhi banyak klien)
- Potensi eksfiltrasi data via API/docs palsu

“One abandoned DNS record can break a chain of trust.”
— Van Lyubov

“Fitur custom domain yang memudahkan brand identity justru sering menjadi titik lemah.”

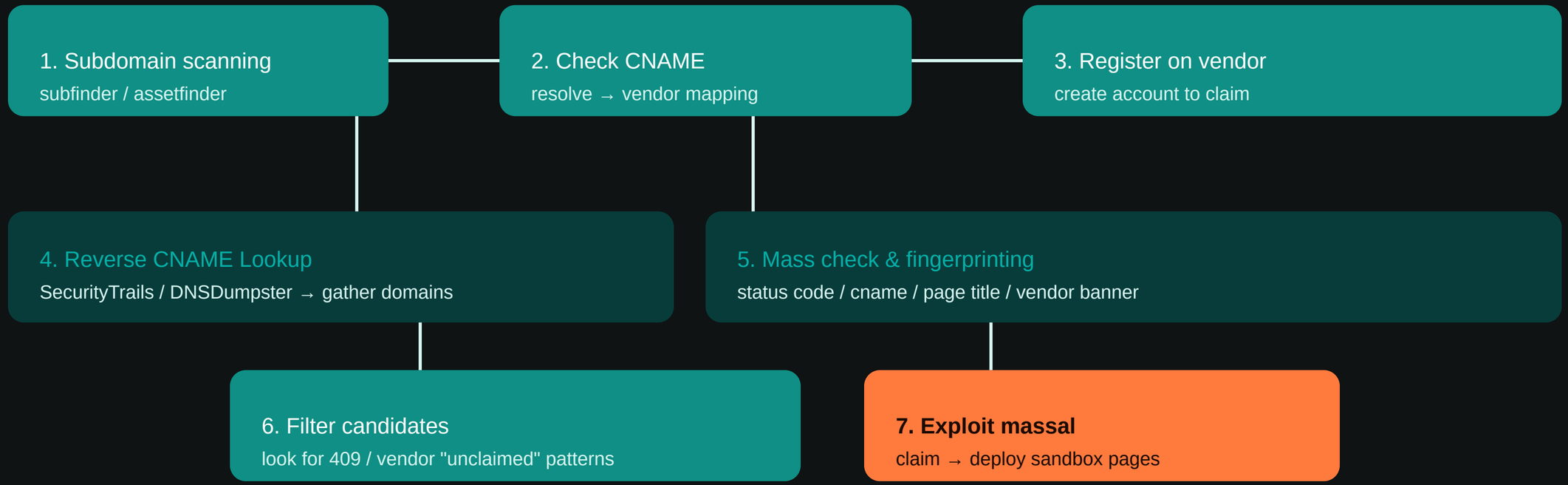
KENAPA SUPPLY CHAIN MEMPERBURUK RISIKO

Faktor	Penjelasan singkat	Contoh dampak / konsekuensi
Fragmentasi vendor	Dari dokumentasi -> LMS -> blogging -> CRM, tiap departemen bisa pilih tool sendiri.	Security team sering tidak tahu semua custom domain yang aktif.
Low-cost entry	Banyak SaaS mengizinkan klaim custom domain gratis atau mudah tanpa verifikasi.	Attacker menunggu domain terlantar lalu klaim tenant di provider.
Persistence	Rekam DNS (CNAME) sering dibiarkan bertahun-tahun setelah project dihentikan.	CNAME tetap ada -> titik takeover tersedia meski project sudah mati.
Chained impact	Takeover satu subdomain dapat digunakan untuk menyebarkan payload ke aset lain (embed JS, redirect, social engineering).	blog.example.com kena takeover -> pasang JS yang menarget dashboard.example.com.

TEGALSEC - RESEARCH

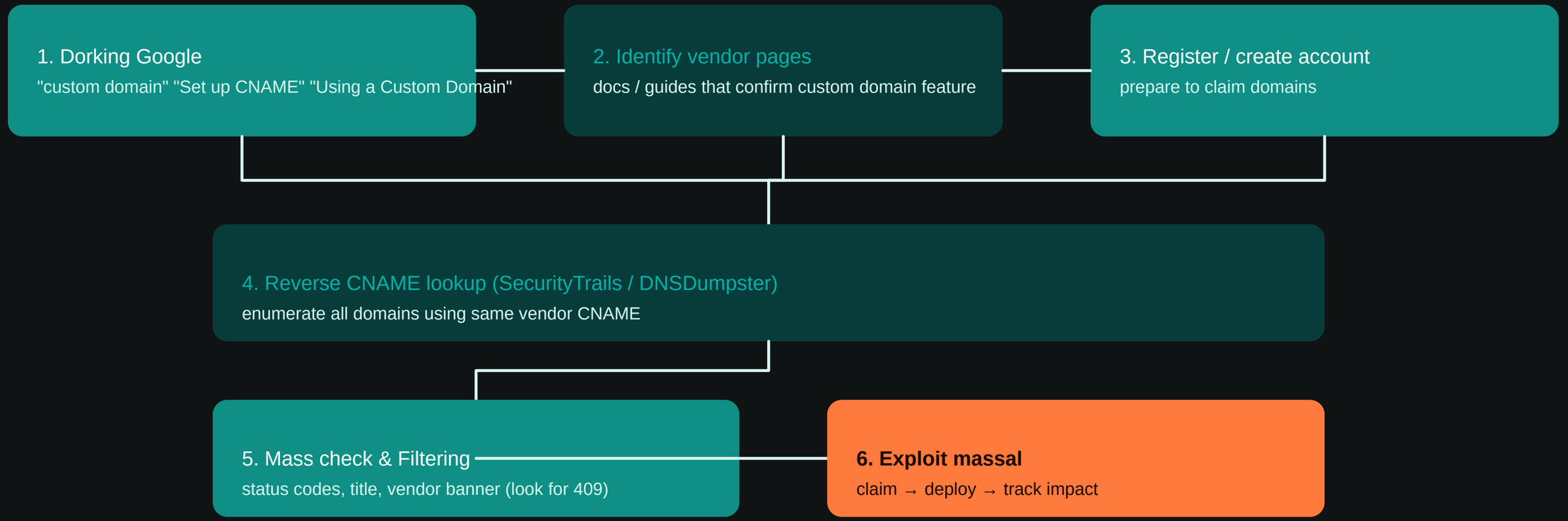
MENCARI SERVICE RENTAN

Flow Pertama — Scanning & Exploitation



Tip: Automasi setiap step — hasil terbaik dicapai dengan kombinasi reverse-CNAME + fingerprint templates.

Flow Kedua — Dorking → Reverse CNAME



Note: Dorking helps discover less-known vendors — combine with reverse CNAME to expand reach.

INDIKATOR & FINGERPRINT YANG UMUM

- HTTP status: 404, 301/302, 409 (vendor-specific)
- Page title / body: pesan “help center closed”, “project not found”, “Error 1001” “DNS resolution error” , atau banner vendor
- CNAME pattern: cname.vendor.com, cname.service.net

Kombinasi di atas → kandidat rentan

STUDI KASUS: NICEBOARD

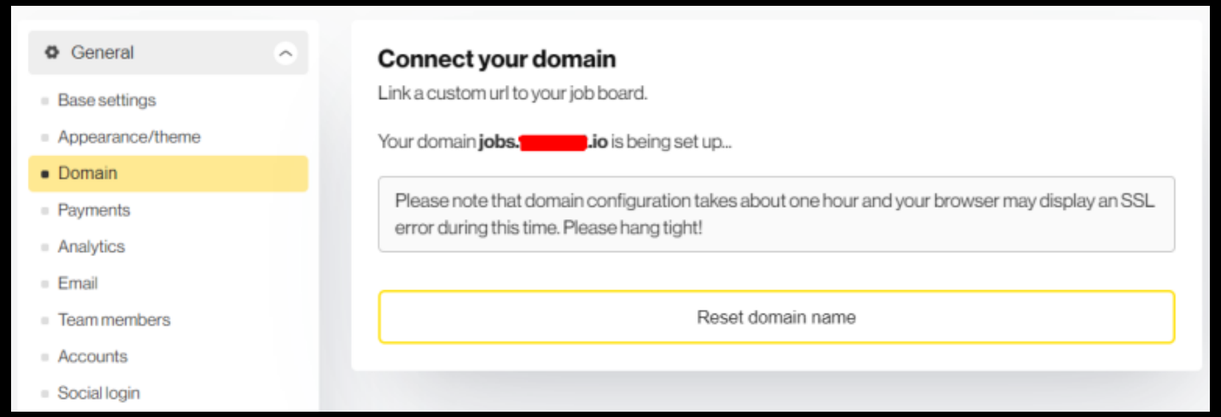
Niceboard.co adalah platform SaaS populer untuk memungkinkan organisasi, yayasan, dan komunitas untuk membangun dan mengelola pekerjaan ataupun menawarkan pekerjaan mereka dengan mudah.

- Platform: Niceboard - job board SaaS yang memungkinkan custom domain via app.niceboard.co.
- Root cause: Subdomain yang mengarah ke app.niceboard.co namun resource akun pengguna di Niceboard dihapus/unused -> terjadi dangling CNAME.

POC NICEBOARD: LANGKAH EKSPLOITASI

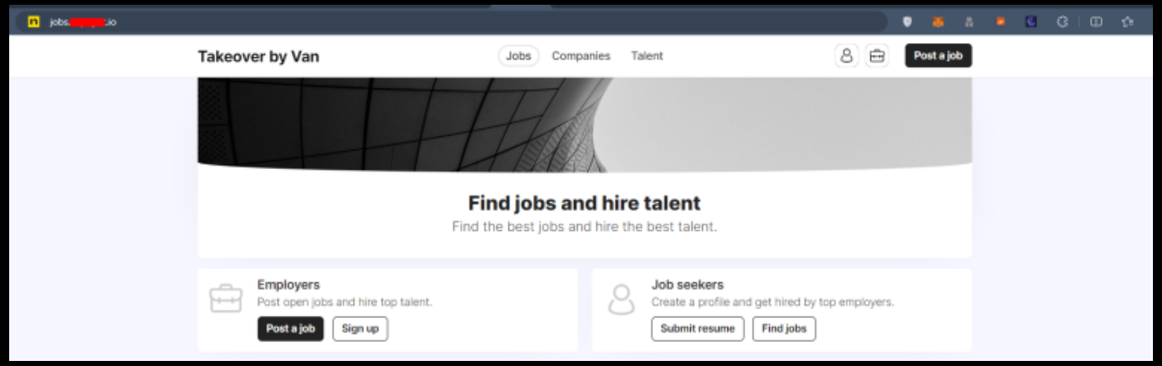
- Identifikasi subdomain yang mengarah ke app.niceboard.co.
- Akses subdomain — lihat respons (mis. “No such account” atau redirect).

```
┌──(van㉿DESKTOP-RBABAE1)-[~]
└─$ curl --insecure -I https://jobs.[redacted].io
HTTP/2 301
server: nginx
date: Thu, 28 Nov 2024 12:00:22 GMT
content-type: text/html
content-length: 162
location: https://100teletravail.fr/
```



Buat akun baru di Niceboard, tambahkan custom domain yang sama (claim).

Deploy halaman/asset di Niceboard untuk membuktikan kontrol subdomain.



IMPLIKASI DARI CASE NICEBOARD

- Banyak organisasi bisa saja memiliki career page / job board yang orphaned → target sosial-engineering & phishing pelamar.
- Niceboard case menggambarkan bagaimana layanan HR/Job-board yang terlihat “non-technical” tetap berisiko besar.

STUDI KASUS: INTERCOM

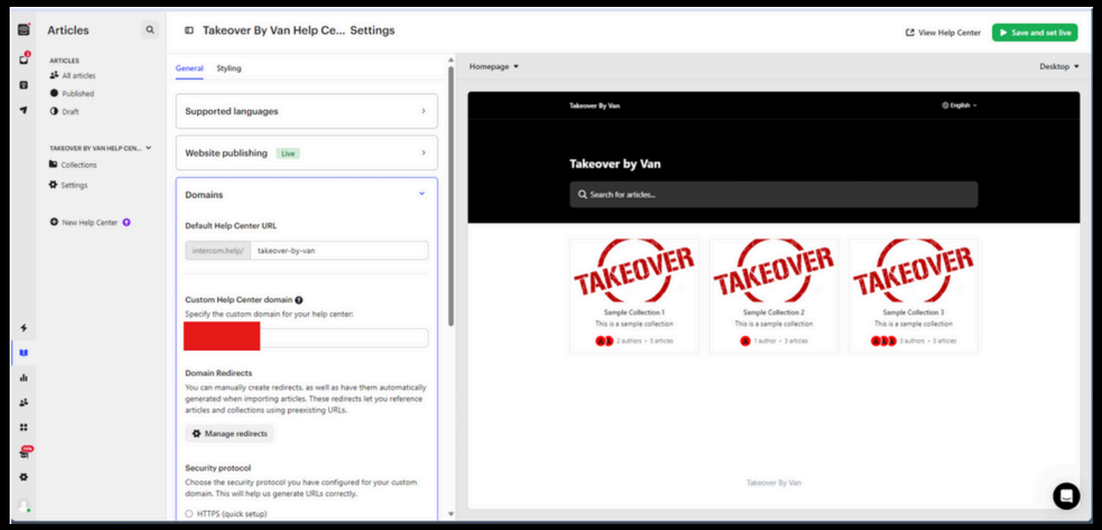
Intercom adalah platform SaaS populer untuk live chat, customer support, dan help center yang banyak digunakan oleh perusahaan untuk menampung artikel bantuan dan percakapan dengan pelanggan.
Platform ini mendukung custom domain seperti:

help.domain.com → misal : *custom.intercom.help*

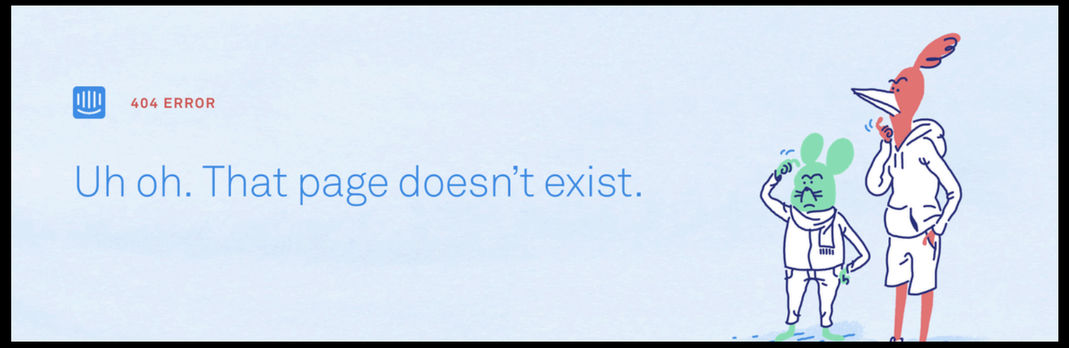
- Saat organisasi menghapus atau menonaktifkan workspace Intercom-nya, domain custom (help.domain.com) tidak otomatis dihapus dari DNS.
- CNAME masih menunjuk ke custom.intercom.help, tetapi workspace-nya sudah tidak aktif.
- Kondisi ini menciptakan dangling CNAME.

POC INTERCOM : LANGKAH EKSPLOITASI

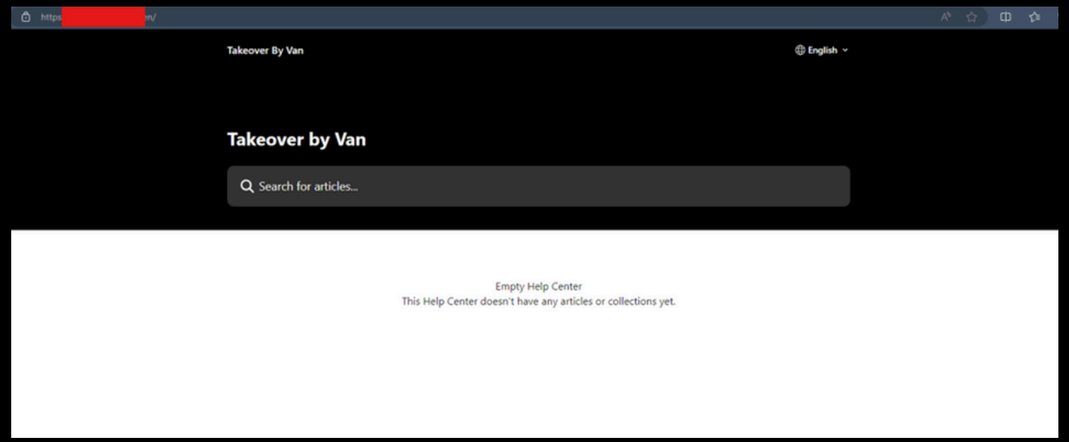
- Identifikasi subdomain yang mengarah ke custom.intercom.help.
- Akses subdomain — lihat respons (mis. “404 Error”).



Deploy halaman/asset di Intercom untuk membuktikan kontrol subdomain.



Buat akun baru di Intercom, tambahkan custom domain yang rentan (claim).



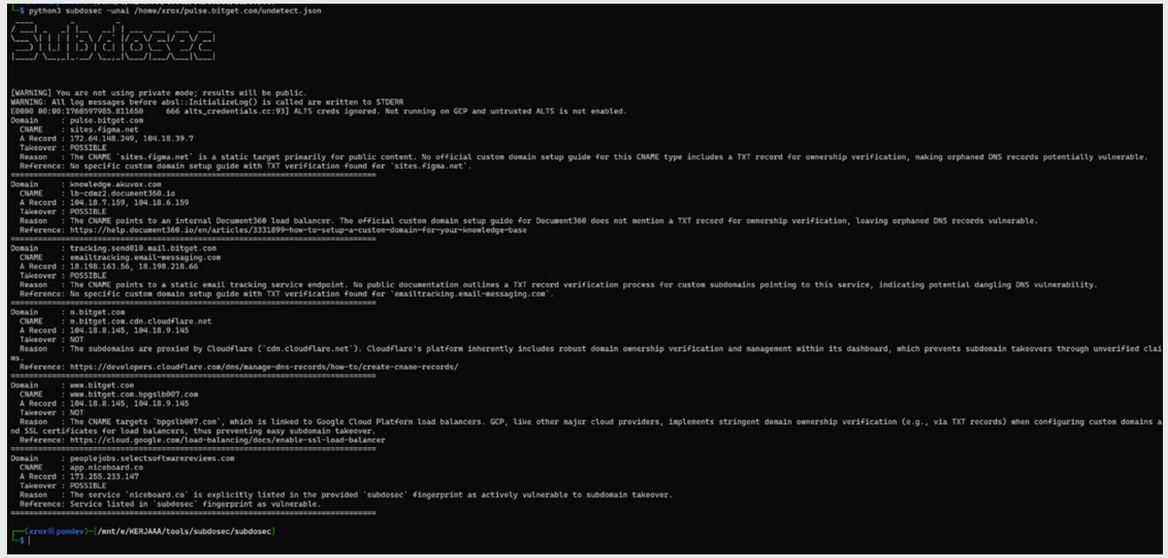
IMPLIKASI DARI CASE INTERCOM

Phishing realistis:
Attacker bisa membuat help center palsu di help.domain.com dengan SSL valid, sulit dibedakan dari asli.

Eksploitasi kepercayaan:
User mengira situs resmi, lalu mengirim data pribadi atau kredensial ke attacker.

Reputasi & brand damage:
Pengguna menilai perusahaan diretas, menurunkan kepercayaan publik dan reputasi digital.

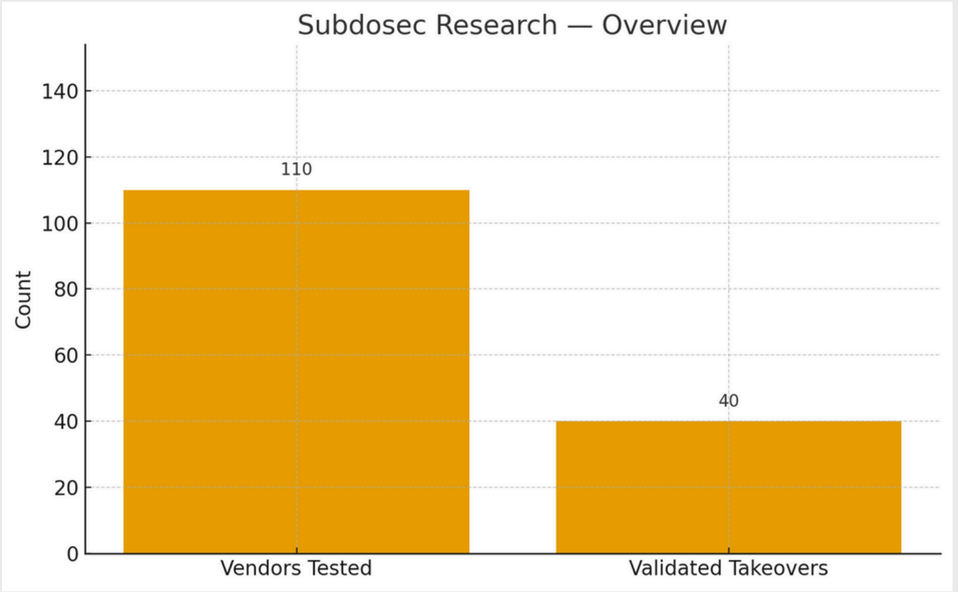
Subdosec



- Subdosec adalah sebuah tool riset keamanan yang dikembangkan oleh Tegalsec Research untuk melakukan otomatisasi deteksi misconfiguration SaaS dan proyek public monitoring & fingerprint database untuk subdomain takeover dalam skala besar (at scale) berbasi AI.
- Nama “Subdosec” berasal dari singkatan:
  Sub (subdomain) + do (discovery) + sec (security).

RESEARCH - OVERVIEW

- 100+ SaaS vendor diuji (2024–2025)
- 40+ takeover tervalidasi (Mintlify, Stoplight, Hashnode, Teamtailor, Niceboard, Zendesk, DLL)
- Fokus: risiko supply-chain antar SaaS
- Tujuan: menciptakan dataset “SaaS Misconfiguration Observatory”



SUBDOSEC VS CAN-I-TAKE-OVER-XYZ

Aspek	Subdosec (Tegalsec)	Can-I-Take-Over-XYZ (EdOverflow)
Tujuan	Otomatisasi riset & observasi misconfig SaaS serta subdomain takeover berskala besar.	Dokumentasi komunitas tentang layanan yang bisa di-takeover.
Pendekatan	Eksperimen langsung & otomasi scanning terhadap 100+ vendor SaaS (2024–2025), mencatat fingerprint, status HTTP, CNAME, dan kondisi klaim.	Crowdsourced, berbasis kontribusi issue & PR GitHub; setiap entri diverifikasi manual/CI oleh maintainer.
Fokus	Supply-chain antar-SaaS dan misconfiguration masif (multi-tenant risk, TXT verification, orphaned CNAME).	Fingerprint statis - fokus pada pesan error, DNS pattern, dan status “Vulnerable/Not Vulnerable”.
Keterbatasan	Tidak semua hasil bisa dipublikasikan (karena disclosure & NDA).	Tidak fokus pada mitigasi sistemik, sebagian data sudah usang.
Etika & Disclosure	Responsible disclosure > koordinasi dengan vendor, penandaan status “Fixed/Still Open”.	Disclaimer di README: “Don’t exploit, only for testing/education.”

MITIGASI

- **DNS Hygiene & Asset Inventory**
  Audit berkala DNS records.
  Gunakan tooling (Subdosec, httpx, subfinder) untuk check orphaned domains.
- **Vendor Contract & Security Clause**
  Tambahkan klausul custom domain deprovisioning dalam kontrak SaaS.
  Vendor wajib auto-reject orphaned domains setelah grace period.
- **Security Automation**
  Integrasikan automation scanner
  Alert jika ada domain yang resolve ke SaaS tapi tidak terclaim.
- **Defense-in-Depth**
  Content-Security-Policy (CSP) -> mencegah domain takeover jadi pivot XSS.
  Monitoring logs -> alert jika traffic tiba-tiba mengarah ke “retired” subdomain.

“Security isn’t about locking everything — it’s about knowing what’s left open.”
— Van Lyubov

THANKYOU