Tea app data leaks

Jak (ne)zacházet s daty

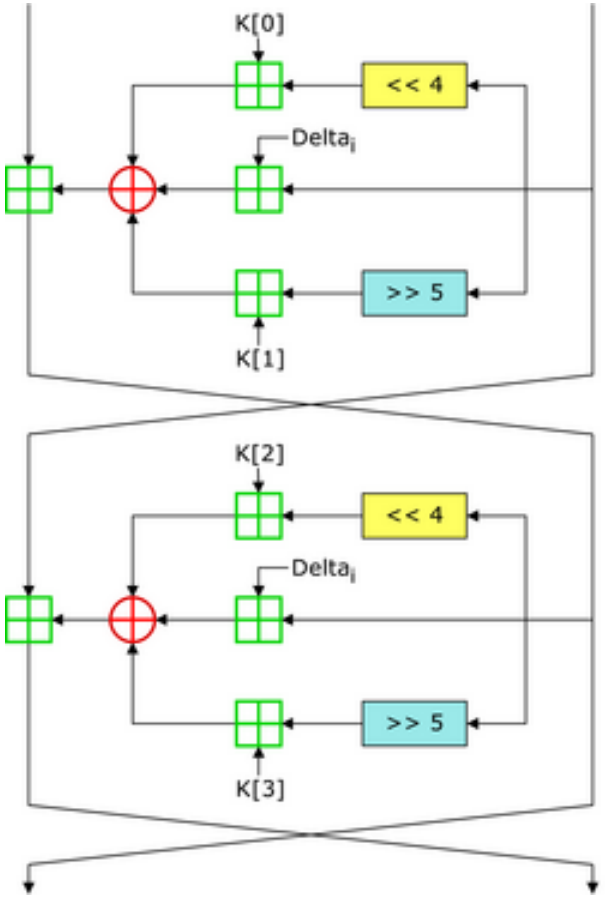
Tomáš Barták – Batacek.eu – LinuxDays 2025

Who am I?

- Student 3. ročníku SSŠVT
- 17 let
- O technologie se zajímám už více než 5 let
- Můj první kód byl v Pythonu, který jsem vytvořil během online hodin :D
- Umím hlavně Python a C#
- Vyzkoušel jsem spoustu dalších jazyků
- Zajímám se primárně o kyberbezpečnost
- Pracuji u společnosti AgentFly Technologies, která vyvíjí vojenské drony

www.batacek.eu

Co je Tea?



Co je Tea app?


USE TEA TO
find verified green flag men
run background checks
identify potential catfish
verify he's not a sex offender
check for a criminal history
tea
Sean
Follow
Golden retriever energy! This man is a total sweetheart - honest and respectful...
Share
Background Check
Conrad Arthur
CONVICTIONS
None found - he's safe!
MARITAL STATUS
Never married
CIVIL COURT RECORDS
Reverse Image Search
POSSIBLE MATCHES
HINGE
INSTAGRAM
Sex Offender Map
Carlos
Daly City
Carlos Jackson Ford
1445 Samuel St
Charlotte NC 28203
OFFENSE
13A-6-63 - Sexual Assault on Minor
VIEW DETAILS
Criminal Record Search
JAKE CALDWELL
CRIMINAL HISTORY
Nonexistent - proceed!
PAST INCARCERATIONS
He's never been to jail
INDICTMENTS

Časová osa

Jaro 2023

- Vznik aplikace

Únor 2024

- Zrušení nahrávání selfie a ID

2024/2025

- První data leak

25.07.2025 6:44 (15:44)

- Odhalení prvního data leaku

Časová osa

- Odhalení prvního data leaku
- Druhý data leak
- Odhalení druhého data leaku
- Odhalení třetího (nepotvrzeného) data leaku

Architektura

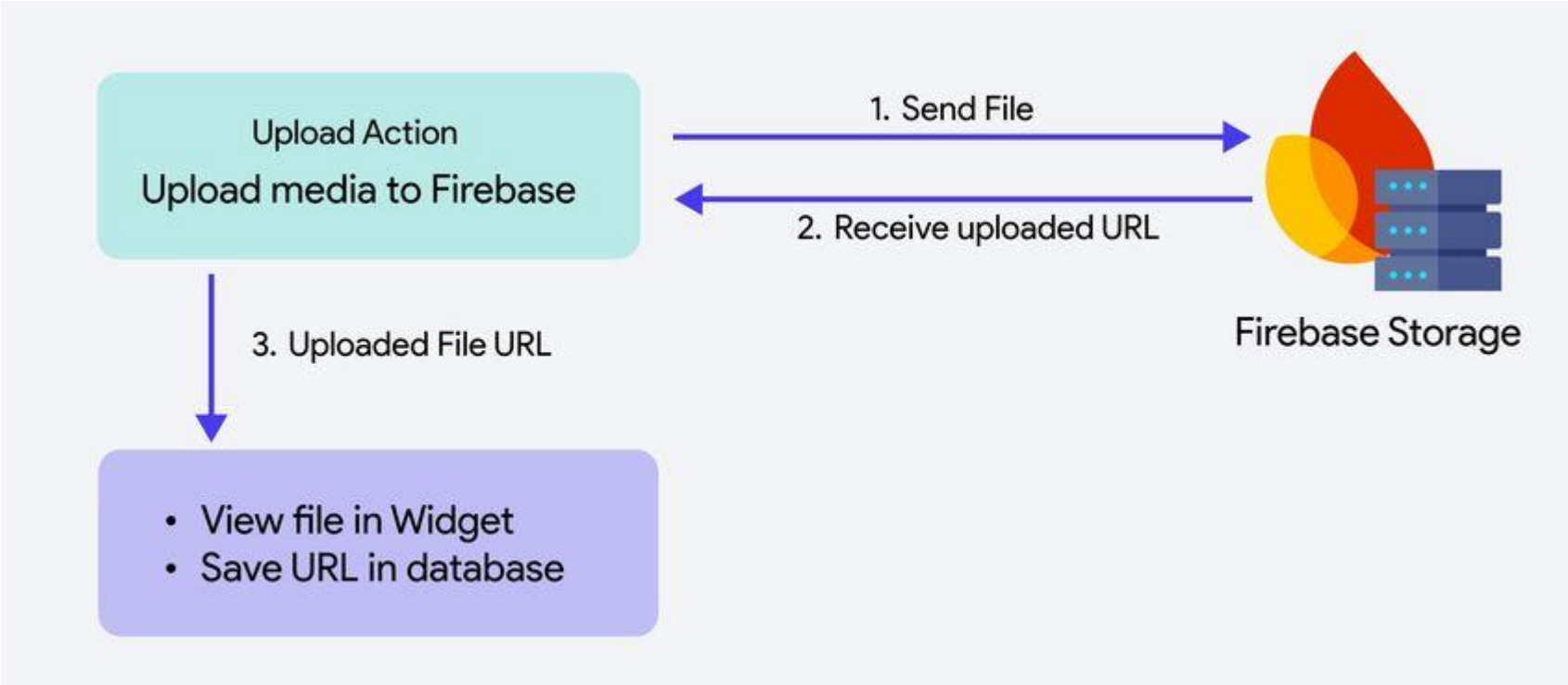
- Firebase public bucket bez autentizace a autorizace
- Žádné šifrování
- Z obrázků nebyla odstraňována metadata
- Firestore pro chaty
- Nejspíše neměli žádný monitoring
- Nejspíše nedělali žádné penetrační testování
- Pro web používají Webflow.com

Bezpečnostní chyby

- 1) Špatná konfigurace cloudového uložiště
- 2) Špatné zacházení s daty
- 3) Špatná správa API klíčů, tokenů a sessions
- 4) Chybějící monitoring
- 5) Žádné penetrační testování

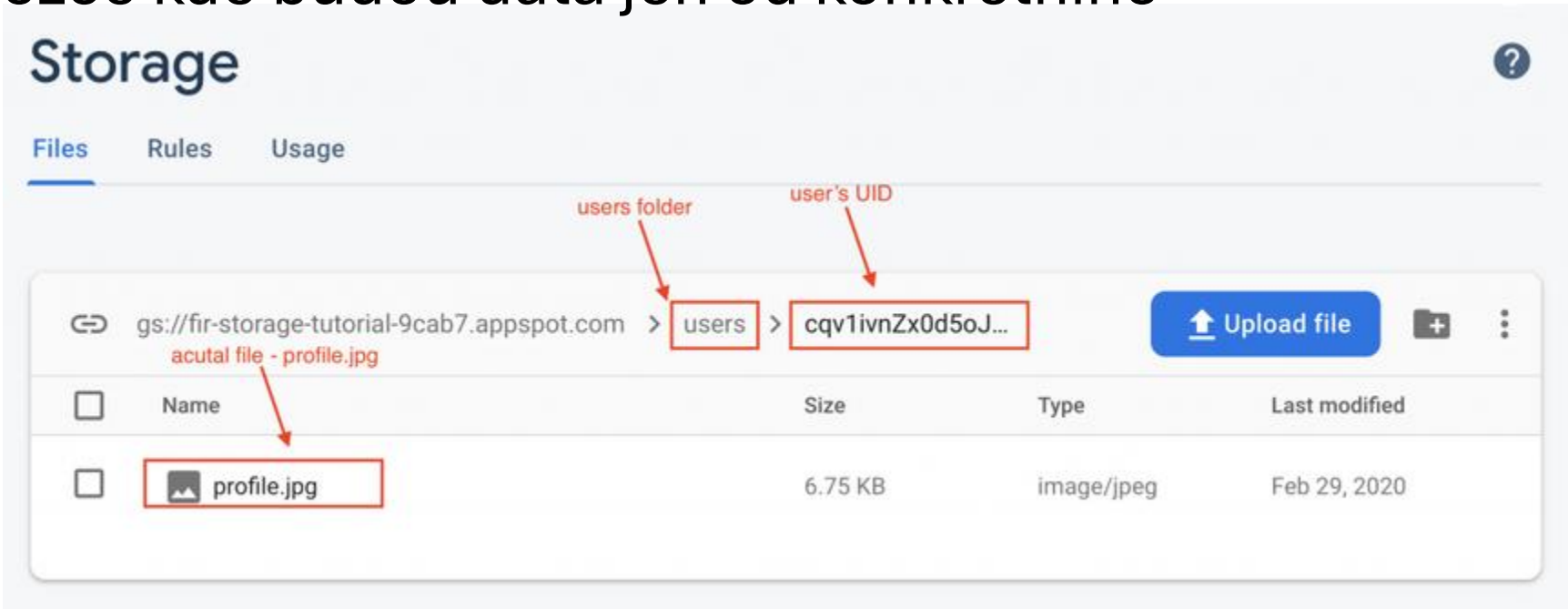
1) Špatná konfigurace Firebase

- Všechna data byla uložena ve veřejném úložišti
- Útočníkům stačilo znát URL
- Používali default (legacy/public) bucket místo private bucket



Správná konfigurace Firebase

- Použít private bucket
- Používat URL, které budou platné jen krátkou dobu
- Pro nahrávání dokladů, selfie atd. zakázat čtení
- Dát přístup jen k složce kde budou data jen od konkrétního uživatele



2) Špatné zacházení s daty

- Data nebyla šifrovaná
- Chaty nepoužívali E2EE
- Společná složka pro všechny uživatele místo složky pro každého uživatele
- Zbytečné uchovávání dat, která nejsou potřeba
- Žádná anonymizace

3) Špatná správa API klíčů a tokenů

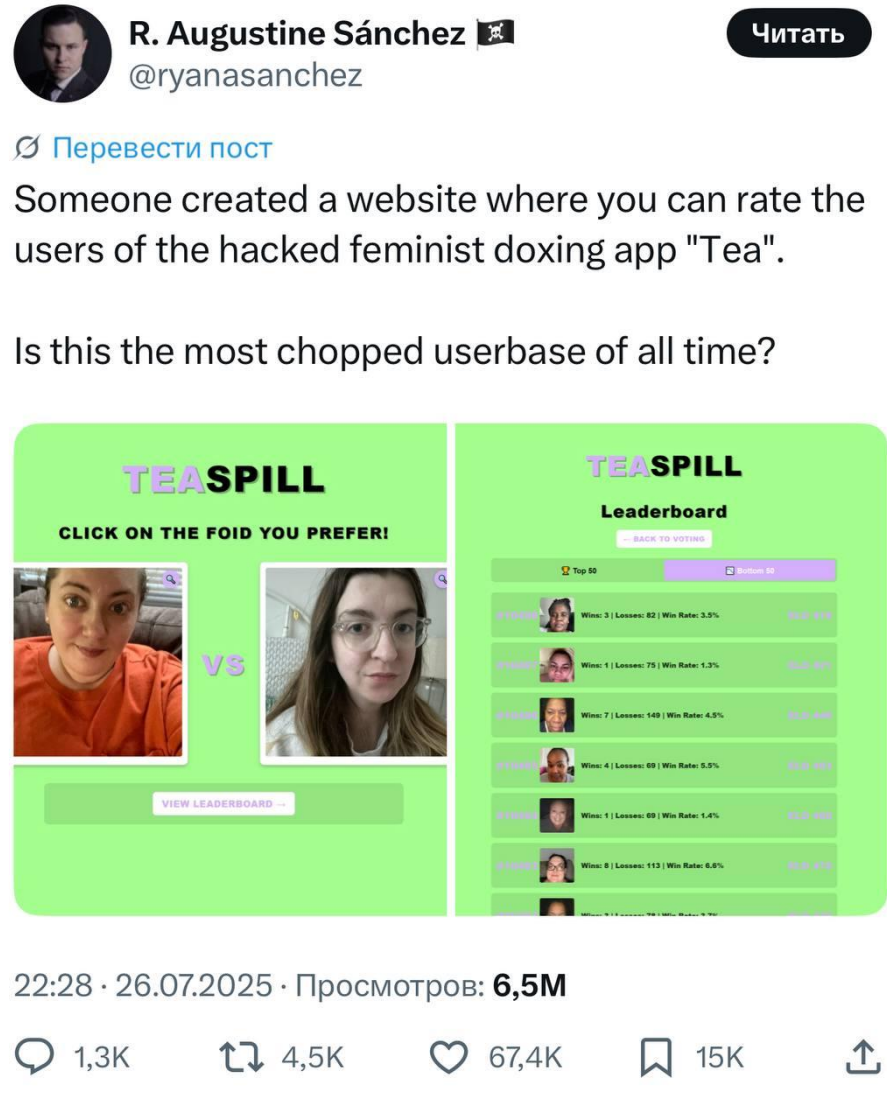
- Hardcoded v apk
  - Bez šifrování
- Žádná rotace
- Klíče měli nepotřebná oprávnění
- Sessions/tokeny neměly expiraci
- Po zjištění úniku byli klíče deaktivovány až po nějaké době

4/5) Monitoring a absence penetračních testů

- Monitoring nebyl nebo byl špatně nakonfigurován
- Nebyly prováděny žádné pen. testy nebo byly velmi slabé
  - Jednalo se o začátečnické chyby, které by měly být snadno detekovatelné

Důsledky úniků

- Únik 72 000 obrázků
  - Z toho 13 000 ověřovací selfie a doklady
- Únik >1 mil. soukromých zpráv
- Při třetím úniku nejspíše unikla osobní data
- Vznikl web TEASPILL pro hodnocení žen
- Vznikla mapa s bydlišti žen
  - Bylo získáno z dokladů, ale také z metadat fotek



Důsledky úniku

- Vývojáři se (možná) poučili
- Lidi si (možná) uvědomili, jak některé společnosti zachází s jejich daty
- Hackeři zjistili, že učit se je ztráta času, stačí jen najít neschopnou společnost

Zdroje

- https://www.404media.co/how-teas-founder-convinced-millions-of-women-to-spill-their-secrets-then-exposed-them-to-the-world/
- https://www.404media.co/podcast-the-tea-hack-just-keeps-getting-worse/
- https://www.404media.co/women-dating-safety-app-tea-breached-users-ids-posted-to-4chan/
- https://www.404media.co/a-second-tea-breach-reveals-users-dms-about-abortions-and-cheating/
- https://www.404media.co/tea-app-turns-off-dms-after-exposing-messages-about-abortions-cheating/
- https://www.404media.co/tea-user-files-class-action-after-womens-safety-app-exposes-data/

Děkuji za pozornost

www.batacek.eu

Tomáš Barták – Batacek.eu – LinuxDays 2025