

Le minacce informatiche prendono di mira le app per la fertilità: nuova arma di ricatto



Le principali violazioni dei dati e vulnerabilità delle API nel 2024-2025 espongono i dati intimi sulla salute riproduttiva di milioni di utenti ai criminali informatici, creando rischi senza precedenti per ricatti ed estorsioni. La combinazione di informazioni personali altamente sensibili, pratiche di sicurezza deboli e attori malevoli sofisticati ha creato una tempesta perfetta per lo sfruttamento nell'industria del monitoraggio della fertilità.

L'incidente più significativo si è verificato nell'ottobre 2024 quando il ricercatore di sicurezza Ovi Liber ha scoperto una vulnerabilità critica dell'API nell'app di monitoraggio della fertilità Glow che ha esposto i dati personali di 25 milioni di utenti, inclusi nomi, età, informazioni sulla posizione e immagini caricate. Questa violazione, causata da un'API per sviluppatori pubblicamente accessibile priva di autenticazione appropriata, esemplifica i fallimenti sistemici della sicurezza che affliggono il settore della tecnologia per la salute riproduttiva. Eva Galperin dell'Electronic Frontier Foundation l'ha definita "una questione piuttosto importante", evidenziando come queste vulnerabilità creino opportunità per attori malevoli di raccogliere dati intimi per scopi di ricatto.

App per la fertilità e sicurezza

informatica: attacchi globali in crescita

Il periodo 2024-2025 ha assistito a un'escalation di attacchi informatici mirati a organizzazioni per la salute riproduttiva in tutto il mondo. La clinica della fertilità Genea in Australia ha subito una violazione devastante quando il gruppo ransomware Termite ha rubato 700GB di dati sanitari sensibili, incluse informazioni personali confidenziali, anamnesi mediche, diagnosi, trattamenti e risultati patologici. I dati rubati sono stati successivamente pubblicati sul *dark web*, dimostrando come le informazioni relative alla fertilità vengano utilizzate come arma dai criminali informatici.

Il professor Dali Kaafar del Cybersecurity Hub della Macquarie University ha fornito testimonianza esperta sulla violazione di Genea, spiegando come i criminali sfruttano le vulnerabilità dei dati sulla fertilità: "Se effettivamente percepiscono una qualche forma di vulnerabilità con la loro vittima, per esempio, la vittima sta cercando di nascondere qualche tipo di informazione dal [suo] datore di lavoro o dalle loro famiglie, probabilmente cercheranno di sfruttare ciò in forma di ricatto". Questa analisi esperta sottolinea il potenziale intrinseco di ricatto nelle violazioni dei dati sulla salute riproduttiva.

Il settore sanitario è diventato sempre più attraente per i criminali informatici, con il rapporto 2024 dell'FBI sui crimini informatici che identifica la sanità come il settore di infrastrutture critiche più preso di mira. Le organizzazioni sanitarie hanno affrontato 444 incidenti segnalati, inclusi 238 attacchi ransomware e 206 violazioni di dati, molti dei quali coinvolgono informazioni sensibili sulla salute riproduttiva.

Sicurezza delle API e vulnerabilità delle app per la fertilità

La ricerca completa sulla sicurezza rivela che il 61% delle app di monitoraggio della fertilità contiene vulnerabilità classificate nei rischi di sicurezza OWASP Top 10. Studi accademici delle università di Newcastle, Royal Holloway e ETH Zurigo hanno identificato difetti critici inclusi traffico Bluetooth non crittografato, meccanismi di autenticazione insicuri e vulnerabilità agli attacchi *man-in-the-middle* in dispositivi e app popolari per il monitoraggio della fertilità.

L'app WhatToExpected ha dimostrato fallimenti di sicurezza particolarmente preoccupanti, con ricercatori che hanno scoperto un endpoint API non autenticato vulnerabile ad attacchi di forza bruta su codici di reset password a 6 cifre. Questa vulnerabilità ha consentito il completo controllo dell'account ed esposto nomi, indirizzi, indirizzi IP, età e dati sulla salute riproduttiva degli utenti. L'API ha anche inavvertitamente esposto indirizzi email di amministratori di forum sensibili, inclusi quelli che gestiscono discussioni sui diritti all'aborto.

La sicurezza delle API rappresenta il vettore di attacco più comune, con le app per la fertilità che espongono regolarmente API per sviluppatori senza controlli di autenticazione o autorizzazione appropriati. L'incidente di Glow esemplifica questo modello, dove un'API pubblicamente accessibile ha permesso a chiunque di raccogliere sistematicamente dati utente inclusi identificatori unici che potrebbero facilitare attacchi mirati.

Le app per la fertilità popolari dimostrano inadeguatezze di sicurezza diffuse. Clue, nonostante la sua base europea e le dichiarazioni sulla privacy, condivide dati estesi con reti pubblicitarie. Ovia Health, di proprietà dell'azienda

farmaceutica Labcorp, fornisce dati sanitari de-identificati ai datori di lavoro che acquistano l'app come benefici per i dipendenti. L'app Flo, che ha risolto con la Federal Trade Commission per 200 milioni di dollari nel 2021, continua ad affrontare scrutinio sulle pratiche di condivisione dei dati nonostante l'implementazione di miglioramenti della privacy.

Casi di ricatto documentati limitati mascherano un potenziale di minaccia significativo

Mentre sono avvenute violazioni estese di cliniche della fertilità, i casi documentati di ricatto reale utilizzando dati sulla salute riproduttiva rimangono relativamente rari nei registri pubblici. Tuttavia, gli esperti di sicurezza informatica avvertono costantemente che questo divario probabilmente riflette una sottostima piuttosto che l'assenza di sfruttamento. La natura sensibile dei dati sulla salute riproduttiva rende le vittime riluttanti a segnalare incidenti, mentre gli accordi di non divulgazione negli accordi spesso impediscono la divulgazione pubblica.

L'ambiente legale post-Roe v. Wade ha drammaticamente elevato questi rischi. Ventisei stati americani hanno vietato o probabilmente vieteranno l'aborto, creando nuove opportunità di sorveglianza dove i dati di monitoraggio del ciclo potrebbero essere utilizzati per azioni legali. I sostenitori della privacy notano che "ciò che era dati benigni prima è ora potenzialmente prova criminale", trasformando le app per la fertilità in potenziali strumenti per l'applicazione della legge.

L'esperto di privacy italiano Guido Scorza, membro dell'Autorità italiana per la privacy, descrive le app di monitoraggio della fertilità come "autentici colapasta" in termini di protezione della privacy. L'Autorità italiana per

la privacy ha aperto indagini su app sanitarie che processano dati sensibili senza adeguate garanzie, enfatizzando la necessità di consenso esplicito e misure appropriate di protezione dei dati.

L'analisi esperta delle minacce informatiche rivela attori di minaccia sofisticati

I professionisti della sicurezza informatica identificano multipli attori di minaccia specificamente interessati ai dati sulla fertilità e salute riproduttiva. I gruppi ransomware di lingua russa rappresentano la minaccia principale, utilizzando tecniche sofisticate di ingegneria sociale per prendere di mira le organizzazioni sanitarie. Il gruppo Scattered Spider ha espanso i suoi obiettivi per includere i settori sanitario e assicurativo, impiegando ingegneria sociale avanzata per compromettere i *help desk* IT.

Il gruppo ransomware Kairos ha preso di mira un centro sanitario femminile australiano, estraendo 77GB di dati dei pazienti. Questi attacchi dimostrano come gli attori di minaccia prendano specificamente di mira le strutture per la salute riproduttiva a causa della natura sensibile dei dati e della disponibilità delle organizzazioni a pagare riscatti per prevenire l'esposizione.

La dottoressa Maryam Mehrnezhad della Royal Holloway University London, una ricercatrice leader nella sicurezza FemTech, enfatizza che "multipli attori di minaccia sono interessati ai dati FemTech come informazioni sulla fertilità e sul sesso". La sua ricerca informa direttamente organismi regolatori incluso l'Information Commissioner's Office del Regno Unito sulle minacce emergenti nel settore della tecnologia per la salute riproduttiva.

Il contesto italiano evidenzia preoccupazioni sulla privacy europea

Il forte quadro di protezione della privacy italiano crea vulnerabilità e protezioni uniche per gli utenti delle app per la fertilità. L'Agenzia nazionale per la sicurezza informatica italiana ha enfatizzato la protezione dei dati sanitari critici, mentre l'influenza culturale cattolica del paese rende le informazioni sulla salute riproduttiva particolarmente sensibili. Le donne italiane utilizzano sempre più app di monitoraggio della fertilità a causa del basso tasso di natalità del paese, ma la consapevolezza dei rischi per la privacy rimane limitata.

L'Autorità italiana per la privacy è stata particolarmente attiva nelle azioni di enforcement, con un'implementazione del GDPR più rigorosa di molti paesi UE. Le autorità italiane esprimono preoccupazioni specifiche sui trasferimenti di dati verso paesi non UE, particolarmente Cina e Stati Uniti, dove i dati delle app per la fertilità potrebbero essere accessibili da governi o corporazioni straniere.

L'organizzazione italiana di sicurezza informatica Clusit identifica la sanità come il secondo settore più preso di mira, rappresentando il 12,2% di tutti gli attacchi informatici in Italia. L'iniziativa Women for Security, supportata da Clusit, ha prodotto analisi specifiche sulla sicurezza informatica in sanità, incluse le applicazioni per la salute riproduttiva, enfatizzando la necessità di prospettive femminili nell'affrontare vulnerabilità specifiche di genere.

Emergono misure preventive mentre l'industria risponde

Il panorama delle minacce alla sicurezza informatica ha spinto varie risposte protettive da sviluppatori di app, regolatori e utenti. Clue ha fatto impegni pubblici a non condividere dati utente con autorità statunitensi, sfruttando la sua posizione berlinese e le protezioni europee della privacy. Il video virale dell'azienda su TikTok che dichiara di non voler conformarsi alle citazioni americane dimostra la crescente consapevolezza dei rischi geopolitici per la privacy.

Flo Health ha introdotto la "Modalità anonima" per privacy potenziata, permettendo agli utenti di accedere all'app senza fornire informazioni identificative. Tuttavia, gli esperti di sicurezza notano che la vera anonimizzazione rimane tecnicamente sfidante quando le app richiedono dati sanitari estesi per funzionare efficacemente.

Sta emergendo legislazione federale e statale per affrontare queste minacce. Il "My Body, My Data" Act, supportato dall'Electronic Frontier Foundation, restringerebbe la raccolta e condivisione di dati sulla salute riproduttiva fornendo diritti privati di azione per violazioni della privacy. La California ha approvato legislazione sui santuari di dati che protegge le informazioni sulla salute riproduttiva dall'applicazione della legge di altri stati.

Raccomandazioni tecniche per sicurezza potenziata

Gli esperti di sicurezza informatica raccomandano l'implementazione immediata di crittografia *end-to-end* per tutti i dati sulla salute riproduttiva, archiviazione locale dei dati piuttosto che sistemi basati su *cloud*, e autenticazione multi-fattore obbligatoria. Audit di sicurezza

regolari e test di penetrazione dovrebbero diventare pratica standard per gli sviluppatori di app per la fertilità.

Gli utenti dovrebbero dare priorità alle app con politiche sulla privacy forti, archiviazione locale dei dati e giurisdizioni europee o altre favorevoli alla privacy. Etichette nutrizionali per la privacy per le app sanitarie aiuterebbero gli utenti a prendere decisioni informate sui rischi di condivisione dei dati. Per individui ad alto rischio, gli esperti raccomandano metodi alternativi di monitoraggio analogico per evitare completamente la sorveglianza digitale.

L'industria richiede condivisione coordinata di *threat intelligence* tra organizzazioni sanitarie, partenariati pubblico-privati per la sicurezza informatica e cooperazione internazionale sulla protezione dei dati sulla salute riproduttiva. I quadri regolatori necessitano aggiornamenti per affrontare rischi specifici del FemTech e pratiche obbligatorie di minimizzazione dei dati.

Conclusione

La convergenza di dati intimi preziosi, vulnerabilità sistemiche della sicurezza e attori di minaccia sofisticati crea un ambiente di rischio senza precedenti per gli utenti delle app di monitoraggio della fertilità. Mentre i casi di ricatto documentati rimangono limitati nei registri pubblici, l'infrastruttura per lo sfruttamento chiaramente esiste, e il consenso degli esperti avverte di minacce crescenti. L'ambiente legale post-Roe v. Wade ha ulteriormente elevato questi rischi, rendendo i dati sulla salute riproduttiva particolarmente vulnerabili ad abusi per scopi di sorveglianza e criminalizzazione.

Gli utenti italiani affrontano vulnerabilità particolari a causa delle sensibilità culturali attorno alla salute riproduttiva combinate con l'adozione crescente di app. Le

forti protezioni della privacy del paese forniscono qualche difesa, ma attori di minaccia globali e trasferimenti internazionali di dati creano rischi continui. La combinazione di lacune regolamentari, vulnerabilità tecniche e motivazioni politiche suggerisce che la sicurezza delle app di monitoraggio della fertilità rimarrà una preoccupazione critica che richiede attenzione immediata da parte di decisori politici, aziende tecnologiche e gli utenti stessi.

Fonti:

ArXiv Research Paper – Privacy and Security of Women’s Reproductive Health Apps

TechCrunch – Glow Fertility App Vulnerability

BleepingComputer – Genea Fertility Breach

Cyber Daily – Genea Fertility Ransomware Attack

Federal Trade Commission – Flo Health Settlement

Australian Privacy Foundation – Fertility Apps Data Misuse

California Attorney General – Glow Inc. Settlement

Yesil Science – Privacy Concerns in Period Tracking Apps

FBI Sextortion Resources

Digital Forensics Corp – 2025 Sextortion Report

SC Media – Glow Fertility Forum Vulnerability

The Nightly – Genea Fertility Cyber Attack

Bright Defense – Recent Data Breaches 2025

Linux Security – Internet Blackmail 2025

ReliaQuest – Ransomware Q3 2024 Report

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/app-per-la-fertilita/>