Facebook Demanded User Email Passwords

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/na1tTE-gi_Y/facebook-demanded-user-email-passwords

---

Facebook, dati di mezzo miliardo di utenti trovati su un server (accessibile a tutti) di Amazon

Ennesimo allarme sicurezza correlato alle attività del social network di **Mark Zuckerberg.**

Una vasta raccolta di dati di utenti Facebook è stata esposta al pubblico fino a poco tempo fa su un server di Amazon. A scoprirlo i ricercatori di **UpGuard,** società di cybersecurity, grazie al ritrovamento di un database contenente i dati Facebook di 540 milioni di persone.

Questi dati, che includevano informazioni sensibili come amici degli utenti, Mi piace, musica, foto, eventi, interessi e check-in, sarebbero stati arichiviati da **Cultura Cultiva**, una società messicana di media.

Inoltre sempre i ricercatori hanno dichiarato che un'altra app chiamata 'A**t the pool'** abbia memorizzato password di Facebook non protette per 22.000 utenti.

UpGuard ha dichiarato di aver provveduto a informare Facebook e Amazon lo scorso gennaio. I dati, però, sono rimasti accessibili fino ad oggi e non è ancora stato chiarito da quanto tempo risultavano online.

Cosa è successo

Secondo **UpGuard**, gli sviluppatori di app hanno esposto i dati degli utenti sui server pubblici. In questo caso, una società di media con sede in Messico chiamata **Cultura Colectiva** ha archiviato dati di 540 milioni di utenti degli utenti di Facebook. Questi dati, accessibili e scaricabili da chiunque, includevano ID di Facebook e nomi di account, nonché commenti e reazioni.

La società di sicurezza ha confermato inoltre un altro backup separato da un'app integrata di Facebook intitolato **"At the Pool"** è stato anche scoperto esposto a Internet tramite un bucket Amazon S3.

Come sottolinea il team di UpGuard Cyber □□Risk: "*Questo stesso tipo di raccolta, in forma altrettanto concentrata, è stato motivo di preoccupazione nel recente passato, dati i potenziali usi di tali dati*".

Quanto è grave

Data la sensibilità di queste informazioni esposte, è piuttosto serio. "At the Pool" conteneva le password non crittografate di 22.000 utenti di Facebook. Ciò nonostante il fatto che al Pool sia cessata l'attività nel 2014. "*Questo dovrebbe offrire poca consolazione agli utenti finali dell'app i cui nomi, password, indirizzi e-mail, ID di Facebook e altri dettagli sono stati esposti apertamente per un periodo di tempo sconosciuto*", afferma il post di UpGuard.

Intervistato dal CNBC **Chris Vickery**, direttore della ricerca sui rischi informatici di UpGuard, ha dichiarato: "*Il ritrovamento di questo database evidenzia un problema intrinseco alla raccolta di dati di massa. I dati sembravano essere stati raccolti attraverso l'integrazione di Facebook in quanto il social network consente agli sviluppatori di terze parti di integrare app e siti Web con la sua piattaforma per consentire funzionalità come l'accesso al servizio tramite Facebook.*

> *New: Facebook user info still being found via third-party-developer data leaks. UpGuard report:* https://t.co/xk3bBRqvqv *Bloomberg coverage:* https://t.co/uFYmSHG6hG
>
> *— Chris Vickery (@VickerySec)* 3 aprile 2019

"*Facebook non ha alcun modo di garantire la memorizzazione sicura dei dati dei propri utenti finali se questi consentiranno agli sviluppatori di app di raccoglierli in massa*", ha concluso Vickery.

Le dichiarazioni di Cultura Colectiva

Tutti i dati sono disponibili pubblicamente e sono quelli che Facebook condivide con noi. Utilizziamo tali informazioni per migliorare l'esperienza dell'utente sul nostro sito web, così come per generare nuovi contenuti che siano attraenti e ispirino il nostro pubblico, ha dichiarato il team Cultura Colectiva in un comunicato. "*Il team di UpGuard Cyber Risk ha rivelato che alcuni dei nostri database contenenti informazioni pubblicamente disponibili sono stati esposti, inclusi 540 milioni di interazioni come Mi piace, commenti e reazioni. Tuttavia, non hanno incluso informazioni riservate o confidenziali, come e-mail o password, dal momento che non abbiamo accesso a questo tipo di dati, quindi la privacy e la*

sicurezza dei nostri utenti non erano a rischio. Ci impegniamo a rispettare sempre le regole di Facebook e anche a proteggere i dati e la privacy dei nostri utenti".

La replica di Facebook

In una dichiarazione a Business Insider, la portavoce di Facebook **Katy Dormer** ha dichiarato: "*Le politiche di Facebook proibiscono di archiviare le informazioni di Facebook in un database pubblico. Una volta allertato il problema, abbiamo collaborato con* ***Amazon*** *per rimuovere i database*".

Le responsabilità di Facebook

Sicuramente **Cultura Colectiva**, **Amazon** e **Facebook,** hanno molte responsabilità ma differenti tra loro.

I primi ad essere chiamati in causa sono quelli di Cultura Colectiva poiché – a prescindere dall'opportunità dell'operazione – hanno lasciato i dati stessi alla mercé di chiunque e senza intervenire tempestivamente a seguito della segnalazione dei ricercatori UpGuard.

Facebook adesso dovrà dimostrare di aver fatto quanto possibile per evitare che un eccessivo numero di dati potesse essere raccolto.

Anni di menefreghismo su come gli sviluppatori di app possano accedere ai dati degli utenti (vedi Cambridge Analytica) hanno portato a una massiccia proliferazione delle informazioni sensibili delle utenti, spesso senza la loro conoscenza o consenso informato.

Anche se – sulla scia dei recenti scandali – Facebook ha reso più restrittivi i dati accessibili agli sviluppatori di app, i danni ormai sono già stati fatti.

https://www.key4biz.it/facebook-dati-di-mezzo-miliardo-di-uten

ti-trovati-su-un-server-accessibile-a-tutti-di-amazon/252748/

AWS S3 Buckets Exposed Millions of Facebook Records

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/rCtabma11G4/aws-s3-buckets-exposed-millions-facebook-records

---

Facebook’s Call for Global Internet Regulation Sparks Debate

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/l9YzsQNIE4A/facebooks-call-global-internet-regulation-sparks-debate

---

Hacking di stato italiano: il

progetto Exodus spia anche i cittadini

Apr 01, 2019 Giancarlo Calzetta Attacchi, In evidenza, Malware, News, Privacy, RSS, Scenario 0

Qualche centinaio di utenti italiani sono stati inseriti per errore in un sistema per la sorveglianza di sospetti criminali sotto indagine. L'errore poteva essere facilmente evitato, ma scoperchia una situazione disastrosa nella gestione delle intercettazioni elettroniche.

Quando si parla di hacking di stato, c'è sempre il pericolo che le cose **sfuggano al controllo** di chi dovrebbe usarle lecitamente e gli esempi non sono certo mancati in passato. Per questo non sorprende più di tanto scoprire che anche le forze dell'ordine italiane non hanno gestito in maniera impeccabile il loro sistema di intercettazione elettronica.

Come ci ha confermato qualche tempo fa un colonnello dei Carabinieri, al giorno d'oggi **una parte importantissima delle indagini viene condotta sui dispositivi elettronici dei sospettati** e le intercettazioni avvengono per lo più mettendo sotto sorveglianza lo smartphone degli indagati tramite l'uso di "captatori informatici" meglio conosciuti come spyware di Stato.

Secondo quanto riportato da un report dell'organizzazione no profit Security No Borders e dal sito Motherboard che per primo ne ha riportato i contenuti, uno dei sistemi usati dalle Forze dell'Ordine ha probabilmente spiato per errore alcune centinaia di utenti italiani che hanno scaricato delle app liberamente disponibili sul Play Store di Google.

Da quanto si legge nel rapporto, e sfruttando l'ottimo approfondimento di Alessandro Longo su La Repubblica, capiamo che Exodus è il sistema usato da molte procure per compiere intercettazioni a tutto tondo sui dispositivi Android dei sospettati: dalle attività su Facebook alle chat di Whatsapp, tutto poteva essere dirottato sui server dei gestori del servizio, incluse conversazioni telefoniche, rubrica dei contatti e ogni altro dettaglio. Non è chiaro se lo spyware fosse in grado di intercettare anche password inserite precedentemente alla sua installazione, mentre è lecito aspettarsi che il suo modulo di keylogging potesse intercettare quelle inserite in seguito.

Come veniva inoculato lo spyware e perché dei normali cittadini sono stati spiati

Secondo quanto riporta il pezzo su *La Repubblica*, Exodus viene usato dalle procure solo dietro autorizzazione a procedere di un giudice. A quel punto, sull'indagato vengono usate delle tecniche di ingegneria sociale per indurlo a scaricare **il malware, che era presente in una ventina di versioni sullo store ufficiale di Google** (a quanto pare a insaputa del grande G). Lo spyware era camuffato da app per migliorare le prestazioni dello smartphone, aggregatore di sconti e offerte o gestore della SIM. Non dimentichiamo che le aziende di telefonia italiane sono tenute a collaborare con le Forze dell'Ordine e quindi alcune comunicazioni arrivavano direttamente dall'operatore in modo da risultare più convincenti. Una volta installata, la prima app fungeva da dropper "condizionato", inviando a server di comando e **controllo il numero di IMEI e attendendo l'eventuale payload** da installare. Purtroppo, a quanto pare, il controllo degli IMEI non era attivo e quindi **chiunque scaricasse l'app da Google Play diventava vittima** di intercettazione.

Un fenomeno tutto italiano, i numeri dell’infezione e la reazione di Google

Lo spyware a cui ci riferiamo è esclusivo del nostro Paese. Ovviamente, moltissime delle forze dell’ordine del mondo hanno a disposizione strumenti simili, ma **Exodus è stato sviluppato in Italia** da un’azienda italiana, la **eSurv** di Catanzaro, e tutti i download sono stati effettuati nel nostro Paese. Addirittura, una delle chiavi crittografiche usate all’interno del codice è “Rino Gattuso”, a confermare l’orgoglio campanilistico degli sviluppatori.

I ricercatori di **Security Without Borders** hanno contattato Google per segnalare quanto avevano scoperto e **Big G ha provveduto a eliminare dallo store oltre 20 varianti** dello spyware, aggiornando le sue misure di sicurezza per riconoscere futuri software simili. Purtroppo, non è disponibile un dato certo sul numero di download effettuati, ma i ricercatori hanno stimato che **in tutto si tratti al massimo di poco più di un migliaio**.

Ovviamente, tra questi ci sono gli indagati delle procure e quindi è impossibile sapere quanti normali cittadini siano

caduti per errore in questo sistema, ammettendo anche l'improbabile caso che potrebbero non essercene stati. Di sicuro, i ricercatori che hanno fatto la scoperta hanno installato la prima app e ricevuto il payload, senza che **nessuno si preoccupasse di disinfettare poi il dispositivo da remoto**.

E qui si intravede il vero problema.

Una gestione troppo allegra delle intercettazioni

I captatori informatici, o spyware, sono strumenti molto potenti ed estremamente invadenti. Per questo andrebbero usati con molte precauzioni. In primo luogo, è **impensabile che la app non venga sottoposta a un regolare controllo di sicurezza** da parte di personale competente delle Forze dell'Ordine. Un semplice test da parte di qualcuno che sapeva come funziona il sistema avrebbe scoperto immediatamente la falla e impedito che cittadini non coinvolti diventassero potenziali oggetti di intercettazione.

In secondo luogo, **è impensabile che il server di comando e controllo non sia sotto il diretto controllo di personale delle Forze dell'Ordine**. Tutti i riferimenti trovati dai ricercatori sembrano puntare a domini controllati direttamente da eServ. Come può lo Stato esser certo di come vengono gestiti i dati, estremamente sensibili, che lo spyware raccoglie?

Infine, ci si aspetterebbe che **i dati raccolti siano continuamente monitorati per riscontrare inesattezze e anomalie**, ma questo non è ovviamente accaduto dal momento il dispositivo infetto dei ricercatori è rimasto tale per diversi giorni (e probabilmente lo è ancora).

In altre parole, sembra che sebbene la gestione delle intercettazioni segua un iter corretto prima che queste

avvengano, dopo l'ok **tutto accade in maniera sregolata o comunque poco appropriata**, probabilmente per una mancanza di cultura all'interno dell'organismo statale che regola queste attività.

Ci sembra urgente trovare un modo per **mettere in sicurezza questo importante strumento investigativo**, delegandone il controllo a personale competente all'interno della struttura delle Forze dell'Ordine.

Please follow and like us:

Falle critiche in VMware. Aggiornare di corsa!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/01/hacking-di-stato-italiano-il-progetto-exodus-spia-anche-i-cittadini/

Giuseppe Busia (Autorità Garante Privacy): 'Regole

comuni tra Italia e Cina sui dati’

Con l’avvento delle smart cities come regolare il trasferimento dei dati tra i Paesi, in particolare tra l’Italia e la Cina? Abbiamo posto questa domanda a **Giuseppe Busia**, Segretario generale dell’Autorità Garante per la protezione dei dati personali.

La videointervista è stata realizzata in occasione dell’incontro a Roma dal titolo *“Smart Cities and Digital Transformation Dialogue. Italy and China – How to Make Cities Better Connected and More Intelligent”,* promosso da **ChinaEU** e **Link University** e organizzato da **Supercom** durante la visita del presidente cinese **Xi Jinping** in Italia.

https://www.key4biz.it/giuseppe-busia-autorita-garante-privacy-regole-comuni-tra-italia-e-cina-sui-dati/252074/

Impronte digitali nella Pa, via libera dalle Commissioni della Camera. Ma spunta l’obbligo anche nelle scuole

Fa progressi alla Camera l’esame in seconda lettura del Disegno di Legge con norme per la concretezza delle azioni nella Pubblica amministrazione e la prevenzione

dell’assenteismo, già approvato dal Senato a dicembre. Dalle commissioni Affari costituzionali e Lavoro è arrivato, ieri, il via libera all’articolo 2, che prevede, oltre al badge, l’introduzione di sistemi di verifica biometrica dell’identità (la scelta sarà solo per le impronte digitali e non anche il controllo dell’iride come erroneamente riportato ieri e oggi da molti giornali) e, contestualmente, anche la videosorveglianza per i furbetti del cartellino nelle Pa.
“Primo passo verso l’introduzione del controllo biometrico: con le impronte digitali stop alle truffe degli assenteisti”, ha commentato su Twitter la ministra della Pa **Giulia Bongiorno**.

> *#Pa #DdlConcretezza Oggi primo passo verso introduzione controllo biometrico: con le impronte digitali stop alle truffe degli assenteisti*
>
> *— Giulia Bongiorno (@gbongiorno66) March 28, 2019*

Tra le novità, approvate dalla Commissioni della Camera, l’estensione delle impronte digitali e della videosorveglianza anche per gli accessi e le uscite nelle scuole. E quest’ultima norma ha scatenato una bagarre nella Commissione Cultura, tanto da costringere il presidente **Luigi Gallo** prima a sospendere la seduta poi a rinviarne la convocazione alla settimana prossima. Facendo ritardare di conseguenza anche l’approdo in Aula del testo previsto per il primo aprile.

“Quello che è successo in Commissione Cultura”, ha detto **Gabriele Toccafondi** (gruppo Misto-Civica Popolare-Ap), *“è solo un antipasto di quello che avverrà in Aula*”.

Marco Bussetti, ministro Istruzione: ‘Sono tutti contro la

norma, non passerà’

“Sono favorevole ai controlli digitali all’ingresso delle scuole, ma non per questioni di controllo sull’assenteismo, piuttosto per ragioni di sicurezza. Un ministero deve sapere chi c’è all’interno di un edificio di 1.200 persone. Credo, però, che alla fine l’articolo 2 del decreto non passerà: sono tutti contro”.

L’ha affermato il ministro dell’Istruzione **Marco Bussetti**, in un’intervista a ‘*La Repubblica*‘. La sensazione è che in Aula l’obbligo venga cancellato per le scuole, invece sarà valido per il resto della Pubblica amministrazione. In questo modo, con le impronte digitali e, contestualmente, anche la videosorveglianza in tutte le Pa, centrali e locali, non si terrà conto dei rilievi del Garante Privacy: *“Misura eccessiva, occorre migliorare il Ddl”,* ha detto **Antonello Soro** in audizione, ma il parere del Garante sarà obbligatorio prima dell’approvazione dei decreti attuativi. Il ministro **Giulia Bongiorno** ha trovato questa soluzione a uno dei dubbi sollevati dal Garante: *“Il sistema che adotteremo trasforma l’impronta in caratteri alfanumerici, così il dato non sarà trasferito integralmente all’amministrazione, ma solo una parte”.*

https://www.key4biz.it/impronte-digitali-nella-pa-via-libera-dalle-commissioni-della-camera-ma-spunta-lobbligo-anche-nelle-scuole/251978/

GDPR Day a San Marino, Soro ‘Incoraggiare il diritto alla portabilità dei dati per contrastare gli oligopoli digitali’

“*Obblighi di correttezza, trasparenza e principio della limitazione della finalità previsti dalla normativa privacy possono promuovere condizioni per ristabilire la correttezza dei rapporti commerciali. Occorre perciò una maggiore consapevolezza della nuova geografia dei poteri. L’Europa non può diventare una colonia nell’imperialismo digitale, ma deve chiedere che tutti giochino alla pari*“.

E’ quanto ha affermato **Antonello Soro**, presidente dell’Autorità Garante per la Protezione dei Dati Personali intervenendo al convegno ‘**GDPR Day**‘, l’evento che simboleggia l’allineamento della Repubblica del Monte Titano ai princìpi del Regolamento UE 2016/679.

La giornata di lavori infatti, si tiene a poche settimane dalla ratifica della legge **171**, che allinea la Repubblica ai principi del GDPR europeo.

> *Antonello Soro Italian SA: Awareness on new geopolitical balance of powers and interests is key. Europe cannot be relegated as a colony of digital imperialism: all actors should be equal #GarantePrivacy pic.twitter.com/FKvagmaaFV*
>
> *— baldo meo (@meobaldo) 29 marzo 2019*

Nel suo intervento il Garante privacy ha auspicato “*un riconoscimento universale della protezione dei dati perché*

proteggere i dati personali significa proteggere la libertà individuale di ognuno”.

Inoltre, ha aggiunto il Garante, *il diritto alla portabilità dei dati va incoraggiato per contrastare gli oligopoli digitali.*

La disciplina di protezione dati rivela un’inattesa attitudine proconcorrenziale di fronte ai fallimenti del mercato digitale

> *#GDPRDAY #SanMarino Antonello Soro: i Dpo sono i principali alleati del #GarantePrivacy*
>
> *— baldo meo (@meobaldo) 29 marzo 2019*

Infine il Garante ha anche parlato del sistema dello sportello unico come importante innovazione.*“Il sistema dello sportello unico è importante innovazione. Ma la prevista facoltà di designazione per le multinazionali, del proprio stabilimento principale rischia di favorire quel forum shopping che il Regolamento intendeva evitare,* ha concluso il Garante.

Il convegno ha visto partecipare oltre al Garante di San Marino **Nicola Fabiano**, anche il presidente dell’Authority italiana **Antonello Soro**, e il Garante europeo **Giovanni Buttarelli.**

https://www.key4biz.it/gdpr-day-a-san-marino-soro-incoraggiare-il-diritto-alla-portabilita-dei-dati-per-contrastare-gli-oligopoli-digitali/251890/

GDPR. Banche, sanità, Spid e telemarketing nel mirino del Garante Privacy

Istituti di credito, sanità, sistema statistico nazionale (Sistan), Spid, telemarketing, carte di fedeltà, grandi banche dati pubbliche.

Sono questi i settori sui quali nei prossimi mesi punterà la sua lente il Garante per la protezione dei dati personali contenuti nel piano ispettivo per il primo semestre 2019 approvato nelle scorse settimane.

L'attività ispettiva, svolta anche in collaborazione con il **Nucleo speciale privacy** della Guardia di finanza, riguarderà innanzitutto i trattamenti di dati effettuati dalle banche, con particolare riferimento ai flussi legati all'anagrafe dei conti; i trattamenti di dati effettuati dalle Asl e poi trasferiti a terzi per il loro utilizzo a fini di ricerca; la gestione delle carte di fidelizzazione da parte delle aziende; il rilascio dell´identità digitale ai cittadini italiani (**Spid**); il Sistema Integrato di **Microdati** (Sim) dell'Istat.

I controlli si concentreranno anche sull'adozione delle misure di sicurezza da parte di pubbliche amministrazioni e di imprese che trattano dati sensibili, il rispetto delle norme sull'informativa e il consenso, la durata della conservazione dei dati da parte di soggetti pubblici e privati. L'attività ispettiva verrà svolta anche in riferimento a segnalazioni e reclami con particolare attenzione alle violazioni più gravi.

Intanto il bilancio 2018 dell'attività ispettiva dell'Autorità conferma l'incremento dell'attività sanzionatoria già

registrato lo scorso anno.

Nel corso del 2018 sono state adottate 175 ordinanze-ingiunzione, a fronte delle 109 del 2017 ed è stato rilevato un notevole aumento delle somme riscosse pari a 8.161.806 euro, a fronte dei 3.776.694 euro registrati nel 2017 (con una variazione positiva del +116%).

Da registrare inoltre un incremento del 20% delle violazioni amministrative contestate: 707 nel 2018 rispetto alle 589 contestazioni del 2017.

Le contestazioni hanno riguardato la violazione di disposizioni del Codice per illeciti commessi prima della data di applicazione del Regolamento (UE) 2016/679.

Sono invece diminuite le segnalazioni all´autorità giudiziaria: 27 nel 2018 rispetto alle 41 del 2017.

Gli accertamenti, svolti nel 2018 anche con il contributo delle Unità Speciali della Guardia di finanza, Nucleo speciale privacy, hanno riguardato numerosi e delicati settori, sia nell´ambito pubblico che privato. Per quanto riguarda il settore privato le ispezioni si sono rivolte principalmente ai trattamenti effettuati: dagli istituti di credito, da società per attività di rating sul rischio e sulla solvibilità delle imprese, dalle aziende sanitarie locali e poi trasferiti a terzi per il loro utilizzo a fini di ricerca, da società che svolgono attività di telemarketing, da società che offrono servizi di "money transfer". Oggetto di particolare accertamento anche i trattamenti di dati svolti da società assicuratrici attraverso l'installazione di "scatole nere" a bordo degli autoveicoli e da società che offrono servizi medico-sanitari tramite app.

Per quanto riguarda il settore pubblico l´attività di verifica si è concentrata su enti pubblici, soprattutto Comuni e Regioni, che svolgono trattamenti di dati personali mediante app per smartphone e tablet, con particolare attenzione

all’eventuale profilazione e geolocalizzazione degli utenti; sulle grandi banche dati; sul sistema della fiscalità, con speciale riguardo alle misure di sicurezza e al sistema degli audit; sul sistema informativo dell’Istat e sullo Spid.

https://www.key4biz.it/gdpr-banche-sanita-spid-e-telemarketing-nel-mirino-del-garante-privacy/251118/

Second Critical Crypto Flaw Found in Swiss E-Voting System

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bezZ_CP1xG8/second-critical-crypto-flaw-found-swiss-e-voting-system