Ladri del futuro

NEL MIRINO *Da inizio 2018 sono 3,2 milioni le app dannose per Android. L'attività degli hacker si rivolge ormai solo ai telefonini: "Postare la foto delle vacanze permette di capire che la propria casa è libera"*

Identità, home banking: smartphone sotto attacco

» VIRGINIA DELLA SALA

È stata una settimana pesante, in Italia, per il trattamento dei dati personali e della privacy: il garante ha chiuso l'istruttoria nei confronti di Facebook per Cambridge Analytica e, soprattutto, ha messo nel mirino una funzione che il social network aveva attivato per i suoi utenti durante le elezioni del 4 marzo 2018. Si intitolava "Candidati" e permetteva di consultare sulla base del proprio indirizzo i candidati nei dintorni e il loro programma elettorale. Inoltre, mostrava un messaggio che ricordava agli utenti che era giorno di elezione, li esortava a condividere con gli altri di aver votato e di spiegare perché fosse importante farlo in un'ottica di "incoraggiamento della partecipazione civica". Una iniziativa realizzata in collaborazione con il ministero degli Interni e con la presidenza del Consiglio che, però, secondo il garante, ha "collezionato" dati potenzialmente "idonei a rivelare le opinioni politiche" degli utenti italiani e quindi considerati sensibili. "Tali - scrive il garante - possono ritenersi, in particolare, le condivisioni degli utenti relative all'essersi recati o meno alle urne e le ulteriori, eventuali dichiarazioni a favore del voto (entrambe rimaste visibili sulla piattaforma, ancorché non monitorate da Facebook". Il garante considera "rilevanti" anche i dati sulla consultazione dei profili dei candidati, in prossimità delle elezioni "benché idonei a fornire indicazioni meno univoche in ordine alle opinioni politiche". Facebook, infatti, ha dichiarato di aver conservato traccia degli accessi ai profili dei candidati per 90 giorni ma solo per "generare metriche aggregate", per capire cioè come sia stato usato lo strumento e se fosse stato efficiente, senza però - sempre secondo il garante - aver debitamente informato gli utenti. "Alla luce di tali considerazioni, il trattamento di dati personali (anche sensibili, in quanto astrattamente idonei a rivelare le opinioni politiche dell'interessato) risulta illegittimo".

ELEZIONI DEL 4 MARZO 2018

La Privacy contro Facebook: "Collezionava dati utili per capire l'orientamento politico in modo illegittimo"

METÀ DEGLI UTENTI NON SI PROTEGGE

L'esperto: "Rubando un semplice estratto conto si può ottenere una carta di credito o un finanziamento"

La scheda

SPIATI
L'obiettivo degli hacker non è più il pc, ma lo smartphone. Secondo gli analisti di G Data, da inizio 2018, sono 3,2 milioni le app dannose per il sistema operativo Android

BANCHE ON-LINE
Trend Micro ha rivelato la vendita, su Play Store, di due applicazioni in grado di sottrarre i dati dell'home banking degli utenti: con un codice malevolo potevano conoscere credenziali e password

I DATI. É solo l'ultimo esempio delle informazioni sensibili che lasciamo online, soprattutto con lo smartphone e le applicazioni. Secondo una indagine Eurostat, diffusa durante il Data Privacy Day, l'anno scorso il 75% dei cittadini dell'Unione europea tra i 16 e i 74 anni ha utilizzato uno smartphone ma il 28% non ha mai limitato o negato l'accesso ai propri dati. Nella classifica dei paesi i cui cittadini si sono protetti di più, la Francia è al primo posto, seguita da Germania, Paesi Bassi e Lussemburgo. L'Italia si è posizionata a metà classifica, con il 30% dei consumatori che non ha mai rifiutato l'accesso alle proprie informazioni personali. Stando alle statistiche, il 7% di chi possiede uno smartphone non è a conoscenza della possibilità di farlo. Inoltre, meno della metà (circa il 43%) dei proprietari di un telefono ha riferito di avere un programma per la sicurezza installato automaticamente o fornito dal sistema operativo, mentre un ulteriore 15% ha sottoscritto un sistema di protezione dati o ne ha usato uno installato da qualcun altro. Uno sbaglio. G Data ha pubblicato l'Android Malware Report relativo al terzo trimestre 2018, che monitora le debolezze delle applicazioni Android: dall'inizio del 2018 gli analisti di G Data hanno rilevato ben 3,2 milioni di app dannose per Android, con un incremento del 40 per cento rispetto allo stesso periodo dello scorso anno. Un'ultima analisi di Trend Micro ha rivelato la vendita, su Play Store, di due applicazioni in grado di sottrarre i dati dell'home banking degli utenti: con un codice malevolo potevano conoscere credenziali e password, ma anche effettuare screenshot dello schermo e registrare audio ambientali, monitorare la posizione e sapere quando lo smartphone era in uso o meno.

485%
Quanto è cresciuto, nel terzo trimestre '18, l'uso di tecniche e di manipolazione delle informazioni per trarre in inganno gli internauti

30%
Degli utenti quanti in Italia non ha mai rifiutato l'accesso alle proprie informazioni Mentre le app dannose sono aumentate del 40%

LE ESPOSIZIONI. Per capire a quanti livelli sono esposti oggi gli utenti, contattiamo Francesco Cipollone, che è consulente su cybersecurity e digital data protection e il direttore degli eventi per la cloud security alliance in Gran Bretagna, nonché membro di ISC2. "Quando si naviga online, ogni utente lascia delle impronte digitali che possono essere categorizzate come 'attive' o 'passive'". In pratica sono passive quelle inconsapevoli: "Quelle dei siti web che raccolgono informazioni su quante volte lo hai visitato in passato. - spiega Cipollone -. Non si sceglie di consegnarle, semplicemente vengono raccolte quando il dispositivo è connesso ai siti web".

Ci sono poi le impronte "attive", che si lasciano quando si effettuano determinate scelte. "I post che si pubblicano sui social media ne sono una forma" spiega Cipollone. E se per accedere alle prime in modo fraudolento ci sarebbe bisogno che le aziende digitali le cedessero a terzi o subissero attacchi alla sicurezza, le impronte attive sono sempre più esposte invece alla cosiddetta 'ingegneria sociale'. "Postare la foto delle proprie vacanza - ad esempio - non solo permette di far sapere dove si è ma anche che la propria casa è vuota". Inoltre, fornire informazioni su se stessi può servire ai cybercriminali per profilare nel dettaglio l'utente e poi colpire: "Partendo da un estratto conto, anche solo arrivato per posta al vecchio indirizzo di casa, si può riuscire a ottenere una carta o una linea di credito. O far sapere di sé e della propria famiglia può costituire il punto di partenza per ricostruire una identità al 100 per cento per rubarla o magari spacciarsi per un amico di vecchia data ed avere altre informazioni". E chi sono i target preferiti?

Chiunque possa fornire e detenere informazioni importanti oppure chiunque possa diventare tramite, anche inconsapevole, dell'accesso a esse. Secondo alcuni recenti report negli ultimi anni sono aumentati gli attacchi verso persone che lavorano in aziende. La prassi è di inviare loro email personalizzate e cucite su misura per far sì che vengano aperte, consultate e che si interagisca con esse in modo da fare breccia e riuscire così a entrare nella rete aziendale.