Data breach, al via la prima indagine globale

Al via oggi l'indagine a carattere internazionale dedicata quest'anno alla gestione dei data breach da parte di soggetti pubblici e privati denominata "**Privacy Sweep 2019**".

L'iniziativa, coordinata dalla Global Privacy Enforcement Network (**GPEN**), ha come obiettivo di promuovere la cooperazione internazionale fra le Autorità di controllo in materia di privacy alla luce della globalizzazione dei mercati e del crescente flusso di informazioni personali.

Le Autorità di protezione dati che svolgeranno l'indagine (tra cui il Garante italiano) prenderanno in esame i processi e le procedure adottati per la gestione delle violazioni dei dati personali dai titolari dei trattamenti che operano sui rispettivi territori nazionali.

Lo "Sweep" ("indagine a tappeto") sulla gestione dei data breach fa seguito ad analoghe indagini effettuate negli scorsi anni che hanno preso in esame il principio di responsabilizzazione (accountability), le informative privacy su siti web e le app per la telefonia mobile, i servizi online destinati a minori, l'Internet delle cose.

Garante privacy: focus su eCommerce

Allo Sweep 2019 partecipano, oltre a quella italiana, altre 17 Autorità garanti della privacy di vari Paesi del mondo.

Il Garante per la protezione dei dati personali concentrerà la sua attività sul settore **dell'eCommerce** attraverso l'analisi

di un campione significativo di aziende italiane.

I risultati dell’indagine internazionale saranno resi pubblici il prossimo novembre.

https://www.key4biz.it/data-breach-al-via-la-prima-indagine-globale/271878/

Facebook suspends tens of thousands of apps in ongoing privacy investigation

reader comments

54 with 45 posters participating

Share this story

Facebook—the social media company that has been under intense public criticism for not adequately safeguarding the personal information of its 2 billion users—has suspended tens of thousands of apps for a variety of violations, including improperly sharing private data.

In a post published on Friday, Facebook VP of Product Partnerships Ime Archibong said the move was part of an ongoing review that began in March 2018, following revelations that, two years earlier, Cambridge Analytica used the personal information of as many as 87 million Facebook users to build

voter profiles for President Donald Trump's presidential campaign. Facebook has been embroiled in several other privacy controversies since then.

The tens of thousands of apps were associated with about 400 developers. While some of the apps were suspended, in a few cases others were banned completely. Offenses that led to banning included inappropriately sharing data obtained from the Facebook platform, making data available without protecting user's identities, or clear violations of the social network's terms of service.

One of the few apps Facebook identified was called myPersonality. According to Archibong, it "shared information with researchers and companies with only limited protections in place, and then refused our request to participate in an audit."

Friday's post said Facebook took legal action against some groups associated with the apps. Companies LionMobi and JediMobi, Archibong said, used their apps to infect users' phones with malware in a profit-generating scheme. Facebook has already stopped the alleged fraud and refunded advertisers. Facebook has also sued Ukrainian men Gleb Sluchevsky and Andrey Gorbachov for allegedly using quiz apps to scrape users' Facebook data. Facebook has also sued South Korean data-analytics company Rankwave for allegedly failing to cooperate with the investigation.

Archibong wrote:

> *And we are far from finished. As each month goes by, we have incorporated what we learned and reexamined the ways that developers can build using our platforms. We've also improved the ways we investigate and enforce against potential policy violations that we find.*
>
> *Beyond this investigation, we've made widespread improvements to how we evaluate and set policies for all developers that*

> *build on our platforms. We've removed a number of APIs, the channels that developers use to access various types of data. We've grown our teams dedicated to investigating and enforcing against bad actors. This will allow us to, on an annual basis, review every active app with access to more than basic user information. And when we find violators, we'll take a range of enforcement actions.*

According to The New York Times, court documents filed in state court in Boston as part of an investigation by the Massachusetts attorney general into Facebook show that the company has suspended 69,000 apps. Of those, 10,000 were removed from Facebook for potentially misappropriating Facebook users' data, the NYT reported.

Over the past 12 months, Facebook has faced scathing criticism for practices that have revealed personal information of its users. In July, the company agreed to pay the Federal Trade Commission $5 billion to settle charges it "subverted users' privacy choices to serve its own business interests."

Friday's revelations suggest that the scope of the privacy controversies may be bigger than company officials have previously acknowledged. Now would be a good time for readers who use Facebook to review the apps they've installed and delete any that request large amounts of data or don't provide a meaningful benefit.

https://arstechnica.com/?p=1572585

AT&T tells court: Customers can’t sue over sale of phone location data

Getty Images | SOPA Images

reader comments

34 with 27 posters participating

Share this story

AT&T is trying to force customers into arbitration in order to avoid a class-action complaint over the telecom’s former practice of selling users’ real-time location data.

In a motion to compel arbitration filed last week, AT&T said that plaintiffs agreed to arbitrate disputes with AT&T when they entered into wireless service contracts. The plaintiffs, who are represented by Electronic Frontier Foundation (EFF) attorneys, will likely argue that the arbitration clause is invalid.

The case is pending in US District Court for the Northern District of California. In March 2018, a judge in the same court ruled that AT&T could not use its arbitration clause to avoid a class-action lawsuit over the company’s throttling of unlimited mobile data plans. That’s because the California Supreme Court had ruled in *McGill v. Citibank* “that an arbitration agreement that waives the right to seek the statutory remedy of public injunctive relief in any forum is contrary to California public policy and therefore unenforceable,” the District Court judge wrote at the time.

In the new case, AT&T argues that the *McGill* decision does not apply "because the injunctive relief Plaintiffs seek is directed at a subgroup of AT&T customers, not the general public as a whole."

"Indeed, numerous district courts in this Circuit have held McGill inapplicable when—as here—plaintiffs seek what amounts to private injunctive relief on behalf of a class rather than an injunction benefiting the public in general," AT&T wrote in its motion to compel arbitration.

AT&T also claims that the Federal Arbitration Act (FAA) preempts the *McGill* standard but acknowledged that a panel of judges on a federal appeals court "recently held that the FAA does *not* preempt the McGill rule." AT&T claims that federal appeals court ruling "contravene[s] Supreme Court precedent" and noted that "*En banc* review is being sought" in the case.

AT&T also told the court that AT&T itself shouldn't be a defendant in the case because AT&T Inc. is just "a holding company organized in Delaware and headquartered in Texas" that does no business in California. This motion wouldn't end the case, because two AT&T Inc. subsidiaries, AT&T Mobility and AT&T Services, would still be defendants.

When contacted by Ars, EFF staff attorney Aaron Mackey said the EFF "look[s] forward to responding to the motions" but declined comment on how the group will respond.

Data sales were "dangerous breach of… privacy"

The class-action complaint was filed in July against AT&T and two location data aggregators called LocationSmart and Zumigo. "AT&T used LocationSmart and Zumigo to manage the buying and selling of its customers' real-time location data," the lawsuit said. The lawsuit seeks monetary damages for

customers, an injunction preventing AT&T from selling location data, and certification of a class including all AT&T wireless subscribers between 2011 and the present "whose carrier-level location data AT&T permitted or caused to be used or accessed by any third party without proper authorization."

The lawsuit says:

> *Despite vowing to its customers that it does not "sell [their] Personal Information to anyone for any purpose," AT&T has been selling its customers' real-time location data to credit agencies, bail bondsmen, and countless other third parties without the required customer consent and without any legal authority. AT&T's practice is an egregious and dangerous breach of Plaintiffs' and all AT&T customers' privacy, as well as a violation of state and federal law.*

AT&T previously denied that selling phone location data was illegal, even though Section 222 of the Communications Act says phone companies may not use or disclose customer location information "without the express prior authorization of the customer." The lawsuit alleges that AT&T violated the Communications Act, the California Unfair Competition Law, the California Constitution's right to privacy, and the California Consumers Legal Remedies Act.

A series of reports by Motherboard beginning in January 2019 showed that T-Mobile, Sprint, and AT&T continued selling customers' real-time location data after all the major cellular carriers promised to stop doing so. The data "end[ed] up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country," Motherboard reported at the time. The news site also wrote about AT&T's motion to compel arbitration yesterday.

Wireless carriers now say they've really stopped the controversial data sales. In addition to the case against AT&T in California, more class action suits seeking refunds for

customers were filed in May against AT&T, Verizon, T-Mobile, and Sprint in US District Court for the District of Maryland.

https://arstechnica.com/?p=1572295

Smart TV, la regina del salotto (che ci spia) non vuole abdicare

Rubrica settimanale **SosTech**, frutto della collaborazione tra **Key4biz** e **SosTariffe**. Per consultare gli articoli precedenti, **clicca qui**.
Schermi. Non possiamo farne a meno: smartphone, smartwatch, computer, tablet. E la **televisione**. Un dispositivo che in tanti, non troppi anni fa, dicevano già destinato all'estinzione. Guarderemo ogni cosa sul telefonino, si diceva, troppo comoda la possibilità di dedicarci a un film o a una serie mentre andiamo al lavoro in metropolitana o a letto, sotto le coperte.

Ed è vero che oggi la nostra fruizione dei **contenuti audio e video** contempla in molte occasioni la mobilità, con la complicità di tariffe sempre più convenienti per **Internet mobile** (basta dare un'occhiata al comparatore di **SosTariffe.it** per toccare con mano quanto siano scesi i prezzi in questo settore); ma dal salotto, il televisore non ha alcuna intenzione di andarsene.

Soprattutto oggi, quando non passa anno che non ci sia qualche novità a rivitalizzare uno dei dispositivi più storici della nostra casa: **4K**, **HDR**, **8K**, **OLED**, **QLED**, dimensioni sempre più mastodontiche, lunghe discussioni su angoli di visione e "nero

che è vero nero”, e poi tutti a dare un’occhiata alle offerte in occasione del **Black Friday** e del **Cyber Monday**.

La televisione che ci spia

Eppure, per quanto possa essere rassicurante – è lì nel nostro salotto ormai da (ben) più di mezzo secolo – la televisione, da quando è diventata smart, può nascondere **insidie** tipiche dell’era di Internet. Ad esempio la possibilità, tipica in genere di tutti i dispositivi **IoT** (a maggior ragione se dotati di altoparlanti e microfoni per i comandi vocali), di inviare i nostri dati a terzi. Due diversi studi, condotti da ricercatori della **Northeastern University** di Boston e dell’**Imperial College London**, di recente hanno mostrato come perfino in standby le tv siano in grado di trasmettere informazioni a nostra insaputa.

Il problema non riguarda soltanto le tv, ma anche gli **stick HDMI** (come il Fire Stick di Amazon, ad esempio) e i **set top-box** di Samsung, LG, Roku e Amazon. I destinatari dei dati “rubati”? **Netflix**, **Google**, **Facebook**, **Microsoft**, **Akamai**, **Spotify** e le altre aziende che sui nostri gusti possono elaborare intere campagne di marketing, e perfino (come nel caso di Netflix) se non siamo abbonati al servizio.

La ricerca, svolta su 81 diversi dispositivi tra gli USA e il Regno Unito, ha mostrato come circa la metà dei televisori coinvolti fosse composta da “messaggeri” di questo tipo. Il che, attenzione, non vuol dire per forza violazione della privacy: è molto probabile che noi stessi abbiamo dato l’assenso a un comportamento di questo tipo, spuntando

frettolosamente le varie opzioni durante l'attivazione o la prima configurazione di un servizio. Si tratta comunque di una condotta abbastanza scorretta, considerando la **scarsa trasparenza** degli avvisi a disposizione dell'utente; il tutto tipico di un ambiente ancora troppo poco regolato. **Netflix**, nel frattempo, si è affrettata a precisare che le informazioni riguardano esclusivamente il buon posizionamento dell'app della tv streaming nell'ecosistema dell'utente e null'altro.

Largo ai top-box e alla tv firmate Amazon

Il fatto che il settore delle "scatolette", i **set top–box** che rendono smart (o "più" smart) i televisori che non lo sono, vada a gonfie vele, è un'ulteriore testimonianza della centralità del televisore. Per questo i colossi dell'entertainment via streaming e non solo si stanno concentrando particolarmente su questo settore: un esempio recentissimo è quello di **YouTube**, con **Google** che ha implementato un nuovo metodo per trasmettere contenuti pubblicitari in tv quando si apre l'applicazione. Ancora per il fronte media player, oltre alla **Fire Stick 4K**, da poco arrivata in Italia (e ancora più intelligente con il supporto ad Alexa), all'**IFA 2019** di Berlino Amazon ha lanciato la nuova generazione di **Fire TV Cube**, a 119,99 euro (ma ancora non disponibile in Italia) per consentire di accedere ai contenuti Netflix, YouTube, Prime Video, con supporto Dolby Vision, Dolby Atmos e naturalmente **Alexa**, con il riconoscimento vocale migliorato grazie alla presenza di 8 microfoni ed alla soppressione del rumore. E visto che non si ha un'esperienza televisiva degna di questo nome se manca un comparto audio all'altezza, l'azienda di Bezos ha mostrato anche la sua prima soundbar, **Nebula Soundbar**, con supporto per 4K UHD e Dolby

Vision, a 209,99 euro.

Ma la notizia veramente ghiotta è un'altra: Amazon ha ufficializzato una serie di collaborazioni con produttori di smart tv per lanciare nuove tv "brandizzate" Fire TV Edition: tra i marchi coinvolti, **JVC** e una vecchia conoscenza, **Grundig**.

Per Sky la tv è sempre al centro

Anche le ultime mosse di **Sky** in Italia – che da poco ha chiuso l'accordo con **DAZN** e si appresta a farlo con Netflix – vanno in una sola direzione: non disdegnare, certo, la mobilità (che continuerà a essere supportata con **Sky Go** e con i satelliti **Sky Q Platinum**), ma ampio spazio per il televisore principale, che sempre più si configura come una "centrale" in grado di soddisfare tutti i bisogni di una famiglia in materia di entertainment. Già, perché se il cinema è affascinante ma scomodo e costoso, guardarsi un film a pochi mesi dall'uscita nelle sale comodamente seduti sul divano, su uno schermo a 65" di qualità sempre più alta e con un impianto audio da far invidia a quello di un **multiplex**, si capisce come il televisore sia lontano dal pensionamento; e ragionamenti analoghi possono essere fatti per lo sport, che in Italia è più che mai un fattore di aggregazione, meno adatto di quanto si pensi alla visione in solitaria sul ridotto schermo dello smartphone.

Già la relazione dell'**Agcom 2019** aveva dimostrato come la televisione, insieme alla radio, rappresenti «*il mezzo che, a fronte dell'ascesa del web, è riuscito a mantenere una solidità nel tempo in termini di ricavi, poiché ha potuto giovarsi della digitalizzazione del segnale e della più recente diffusione delle reti a banda larga e ultralarga*». In un'epoca in cui la politica sembra dettata dai social network, da **Twitter** a **Facebook**, è invece ancora la televisione che fa la differenza ed è considerato il mezzo primario dove farsi un'idea di quello che succede nel mondo. Uno stato di salute

sicuramente molto migliore di quello della carta stampata, e non solo.

Fonti:

https://www.key4biz.it/smart-tv-la-regina-del-salotto-che-ci-spia-non-vuole-abdicare/271528/

Apocalisse privacy: dati sensibili di milioni di utenti sul Web

Set 18, 2019 Marco Schiaffino In evidenza, Leaks, News, Privacy, RSS, Vulnerabilità 0

In poche ore sono stati scoperti due leak di dimensioni spaventose. Online i dati sanitari di 24 milioni di persone e di milioni di clienti Lion Air.

Niente da fare: il vizietto di "perdere" dati sensibili su Internet sembra davvero difficile da cancellare. A dimostrare quanto il fenomeno sia ampio, in queste ore ci pensano due casi clamorosi riportati da numerosi esperti di sicurezza.

Il primo riguarda **Lion Air**, la più grande compagnia aerea privata indonesiana che avrebbe "perso" i dati personali di decine di milioni di passeggeri.

Stando a quanto riporta un ricercatore che su Twitter si fa chiamare **Under The Breach**, i dati sarebbero contenuti in due database collegati a Lion Air che circolano da almeno un mese

nei forum specializzati nella compravendita di dati.

I due archivi sembrano provenire da **Malindo Air** e **Thai Lion Air** (entrambe di proprietà di Lion Air) e, secondo le prime ricostruzioni, potrebbero provenire (tanto per cambiare) da un **Bucket AWS** che sarebbe stato lasciato online senza alcuna protezione e di cui si è avuta notizia già ad agosto.

Non è chiaro, invece, quale tipo di informazioni siano contenuti nei database. Probabile però che ci siano dati sufficienti a consentire ai pirati informatici di sfruttarli per attacchi di phishing o truffe online.

Il secondo episodio riguarda invece il settore medico e, in particolare, alcuni server che contengono i dati sanitari di circa **24 milioni di persone**.

A lanciare l'allarme è stata la società di sicurezza **Greenbone**, che nel suo report spiega che i dati sensibili sono ospitati su dei server **PACS (Picture Archiving and Communication Systems)**, una tipologia di server utilizzata per memorizzare immagini ottenute attraverso analisi mediche come radiografie, risonanze magnetiche e simili.

Molti di questi, però, non hanno alcuna forma di protezione e vi si può accedere senza che sia necessario inserire delle

credenziali.

I ricercatori ne hanno fatto un censimento e ne hanno individuati numerosi nel Regno Unito, negli USA, Canada, Germania, Francia, Giappone, Russia e Svizzera.

Al loro interno ci sono circa **700 milioni di immagini organizzate in 24 milioni di record**, che potrebbero contenere anche informazioni sensibili come i nomi dei pazienti, il numero di previdenza sociale (per quanto riguarda gli Stati Uniti), date ed esiti degli esami, nomi di medici e tecnici di laboratorio.

Usiamo il condizionale perché i ricercatori di Greenbone specificano di non aver scaricato il contenuto del server ma di essersi limitati a eseguire il conteggio dei file visibili. I prossimi che dovessero individuare i server in questione (o chi li ha già individuati) potrebbero però essere meno corretti.

Condividi l’articolo

Simjacker mette a rischio privacy e sicurezza di 1 miliardo di telefoni

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/18/apocalisse-privacy-dati-sensibili-di-milioni-di-utenti-sul-web/

Smart TV, speaker e telecamere inviano dati utenti a Netflix, Fb, Google, Amazon, Spotify e Microsoft

Allarme privacy. Smart TV, tra cui i dispositivi di **Samsung**, **LG** e **Amazon**, gli stick **Roku** e **Amazon Fire Tv**, gli speaker e le telecamere in casa hanno trasmesso i dati degli utenti, come la posizione, l'indirizzo Ip e il modo di utilizzo, a **Netflix**, **Facebook**, **Google**, **Spotify** e **Microsoft**. A scoprirlo i ricercatori della **Northeastern University**, dell'**Imperial College** di Londra e dell'Università di **Princeton**, negli Stati Uniti, citati dal *Financial Times.*

Lo studio della Northeastern University, condotto su 81 dispositivi diversi, sia nel Regno Unito sia negli Usa, è il più grande report pubblicato su questa problematica e ha scovato *"notevoli casi di esposizione alle informazioni".* Amazon, Google, **Akamai** e Microsoft sono state le aziende più frequentemente contattate, anche perché forniscono servizi di cloud e networking per i dispositivi intelligenti, si legge nel report. Analizzando il traffico di rete, il team di Northeastern ha concluso che le terze parti ricevono, per lo meno, informazioni sul dispositivo utilizzato dalle persone, sulla loro posizione e, eventualmente, anche quando interagiscono con esso. *"Quindi potrebbero sapere quando sei a casa e quando non lo sei",* ha detto il professor Choffnes al *Ft*.

"Anche quando le smart Tv sono inattive trasmettono i dati degli utenti ad aziende come Netflix, Google e Facebook", scrivono i ricercatori, che aggiungono *"anche quando non si ha un account Netflix".*

Illustrazione del Financial Times
Poiché gran parte dei dati inviati dai produttori dei dispositivi erano crittografati, gli accademici non sono a conoscenza di quali dati aggiuntivi siano stati trasmessi.

In un altro studio sulle smart TV condotto dall'Università di Princeton, i ricercatori hanno scoperto che alcune app supportate da **Roku** e **FireTV** stavano inviando dati, come l'indirizzo Ip degli utenti, a terze parti, tra cui Google.

Secondo un rapporto Nielsen di marzo, alla fine del 2018, circa il 68% delle famiglie statunitensi aveva un dispositivo televisivo connesso a Internet, considerando anche dispositivi hardware esterni come Roku e **Apple Tv**.

Le repliche di Netflix, Facebook, Google

Netflix ha dichiarato, riporta il *Financial Times*: *"Le informazioni che Netflix riceve dalle smart TV che non hanno effettuato l'accesso alla nostra piattaforma sono limitate al modo in cui Netflix è mostrata sullo schermo. Non riceviamo informazioni su altre applicazioni o attività sulle smart TV".*

La replica di **Facebook**: "*È comune per dispositivi e app inviare dati ai servizi di terze parti integrati in essi. Ciò potrebbe, ad esempio, includere un'app che invia dati a Facebook per creare un'interfaccia di accesso o fornire un pulsante Mi piace*".

Google ha affermato: *"Come altri editori, gli sviluppatori di app di smart TV possono utilizzare i servizi di annunci di*

Google per mostrare pubblicità in base ai loro contenuti o misurare il rendimento degli spot. A seconda delle preferenze scelte dall'utente sul dispositivo e sui consensi, l'editore può condividere dati con Google simili ai dati utilizzati per gli annunci nelle app o sul Web".

Ha aggiunto Big G, confermando quanto scoperto dai ricercatori inglesi e statunitensi: *"A seconda del produttore del dispositivo o il proprietario dell'app, i dati inviati a Google potrebbero includere la posizione dell'utente, il tipo di dispositivo e ciò che l'utente sta guardando all'interno di un'app specifica in modo che possano essere targetizzati con pubblicità personalizzata".*

Dunque, forte è il rischio di tracciamento di ciò che si guarda con le Tv collegate alla Rete. Siamo spiati in casa dal produttore del dispositivo, senza esserne consapevoli anche se distrattamente abbiamo dato il consenso, che invia i dati, vendendoli altrimenti perché dovrebbe farlo, ai giganti del web e agli inserzionisti.

https://www.key4biz.it/smart-tv-speaker-e-telecamere-che-inviano-i-dati-degli-utenti-a-netflix-facebook-google-spotify-e-microsoft/271195/

Simjacker mette a rischio privacy e sicurezza di 1 miliardo di telefoni

Set 17, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, Privacy, RSS, Vulnerabilità 0

La tecnica di attacco permette di colpire qualsiasi modello di telefono sfruttando una vulnerabilità nel codice delle SIM. E viene usato da due anni…

Potremmo definirla una vulnerabilità "democratica", che colpisce sia gli smartphone **Android**, sia quelli con sistema **iOS**.

Stiamo parlando di **Simjacker**, la tecnica di attacco scoperta dai ricercatori di **AdaptiveMobile Security** e che interessa almeno **un miliardo di dispositivi** in tutto il mondo.

La chiave di tutto è **S@T Browser**, una funzionalità integrata nelle SIM dei telefoni e che viene normalmente utilizzata per visualizzarne il contenuto. Il problema è che S@T Browser può anche ricevere istruzioni attraverso semplici messaggi SMS che contengono istruzioni **SIM Toolkit (STK)**.

Come spiegano i ricercatori nella pagina Web dedicata a Simjacker, l'invio di questi comandi avviene in maniera del tutto "trasparente" per il proprietario del dispositivo. **In altre parole: la ricezione del messaggio non viene segnalata in alcun modo e consente, di conseguenza, di portare un attacco silenzioso e invisibile**.

Ma quali sono le azioni che si possono compiere attraverso l'invio di comandi con Simjacker? L'attacco individuato dai ricercatori è, in buona sostanza, un sistema per tenere sotto controllo la posizione della vittima.

Attraverso un semplice SMS, infatti, è possibile istruire la SIM per inviare una risposta con **la posizione rilevata dal GPS** (o l'identificativo della cella a cui il telefono è collegato se non è dotato di GPS) a un numero predefinito.

Secondo gli analisti di AdaptiveMobile Security, questo attacco è stato utilizzato per almeno due anni da quella che i ricercatori definiscono “una società specializzata nel cyber-spionaggio”.

Non ne fanno il nome, ma molti esperti di sicurezza hanno fatto notare che la descrizione corrisponde ad almeno un paio di aziende di spionaggio (per esempio **NSO Group**) specializzate nella fornitura di strumenti di controllo a governi (non sempre di specchiata democraticità) e forze di polizia.

L’uso dei comandi STK, però, apre potenzialmente la strada

anche ad altri tipi di attacchi che possono avere conseguenze decisamente più gravi.

Attraverso l'invio di SMS confezionati ad hoc sarebbe possibile, infatti, forzare la SIM a effettuare telefonate o ad aprire automaticamente pagine Web. Un pirata informatico, di conseguenza, potrebbe avviare a distanza una chiamata a un numero a pagamento per frodare la vittima.

La possibilità di "forzare" l'apertura di una pagina Web rappresenta invece un vettore di attacco formidabile per portare attacchi di phishing o colpire uno smartphone con un malware, sfruttando per esempio un exploit inserito nel codice della pagina stessa.

Insomma: gli scenari che si aprono sono devastanti e, almeno per il momento, non si vede quale possa essere la soluzione per correggere la vulnerabilità. **A peggiorare la situazione, poi, c'è il fatto che le SIM vulnerabili vengono stimate in circa 1 miliardo**.

Nel report dedicato a Simjacker, i ricercatori si rivolgono infatti direttamente agli operatori telefonici (gli stessi che hanno lasciato un software obsoleto e pericoloso sulle loro SIM) suggerendo di mettere in atto policy che siano in grado di filtrare i messaggi per bloccare quelli potenzialmente dannosi.

Condividi l'articolo

Esperti di sicurezza arrestati per effrazione. "Stavamo lavorando"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/17/simjacker-mette-a-rischio-privacy-e-sicurezza-di-1-miliardo-di-telefoni/

Reti del futuro, con il 6G addio agli smartphone: esperienze di realtà estesa e fino a 1 Tbps per utente

Il 5G procede a grandi passi verso il suo dispiegamento naturale su tutto il pianeta. Si parte dalle città, per arrivare ai distretti industriali e le aree a maggiore densità di imprese. Al resto dei territori pensa il 4G. L'innovazione, però, non perde un attimo di tempo e di fatto già si guarda con grande attenzione, curiosità e qualche dato alla mano, alle nuove reti del futuro, quelle di sesta generazione, o **6G**.

> *MT @businessoulucom: #6G Flagship programme organised the world's first #6GSummit with almost 300 participants from 28 countries https://t.co/mBXpz6Gero @6Gflagship @UniOulu #Oulu #Finland*
>
> *— GoodNewsfromFinland (@goodnewsfinland) May 5, 2019*

Dall'**Università di Oulu**, dal cuore della Finlandia sulle rive del Golfo di Botnia, arriva il primo Libro bianco sul 6G dal titolo: "***Key drivers and research challenges for 6G ubiquitous wireless intelligence***". Un *whitepaper* realizzato a partire da sette temi chiave, dai driver sociali e commerciali alle nuove

forme dei device e le più ardite esperienze utente; dall'uso dello spettro nel regime *terahertz* (THz) alla diffusione finale dell'**intelligenza artificiale**; dal networking avanzato ai servizi di nuova generazione; fino a nuovi hardware e materiali.

Il documento è frutto del lavoro e del confronto di un primo summit lappone di marzo 2019 proprio sul futuro della rete e in particolare sul 6G, proponendo una lettura che parta dalle sfide prossime, dalla ricerca e gli investimenti, dai temi chiave (di cui molti già elencati) alle strategie industriali.

"*Se la ricerca sul 5G sta decisamente maturando ed è in grado di supportare la standardizzazione globale della nuova tecnologia, nostro compito è continuare a misurarci con le nuove sfide poste dall'innovazione e dai mercati, motivo per cui ci stiamo già impegnando a lavorare sul 6G*", ha spiegato il professor **Matti Latva-aho**, Direttore del programma di ricerca sul 6G all'Università di Oulu, e curatore, assieme al professor **Kari Leppänen**, del Libro bianco.
"*Al cuore del 6G ci sono **i dati**. Il modo in cui vengono raccolti, elaborati, trasmessi e consumati all'interno delle reti wireless dovrebbe favorire e accelerare lo sviluppo del 6G*", ha precisato Latva-aho.

Diversi gli elementi interessanti che emergono dal documento finlandese: prima di tutto il valore sociale della tecnologia, con grande attenzione alla *privacy*/proprietà dei dati e alla condivisione e moltiplicazione delle reti all'interno delle città, che d'altronde vedranno aumentare a dismisura i propri abitanti a metà del secolo; poi il graduale abbandono del tradizionale smartphone per accedere ad un nuovo ecosistema

digitale, fatto di realtà virtuale/aumentata/*mixed*, che gli studiosi chiamano "*XR*", ***extended reality***; un'intelligenza artificiale distribuita, diffusa, ubiqua ed integrata praticamente a tutto.

> *"The bottom line of #6G is data. The way in which #data is collected, processed, transmitted and consumed within the #wireless #network should drive #6Gdevelopment."*
> *Download the publication+contribute the 6G Summit March 2020 @6Gflagship @SuomenAkatemia https://t.co/vMuq3Ar9oy*
>
> *— University of Oulu (@UniOulu) September 10, 2019*

Ovviamente, al seguito del 6G il Libro elenca tutta una serie di novità, tra cui la telepresenza con immagini ad altra risoluzione e crescente capacità di *sensing*, tecnologie indossabili, *mobile robot*, droni, reti *wireless* avanzate ed intelligenti, auto connesse e a guida autonoma, efficienza energetica, basso impatto ambientale.

La forte integrazione che caratterizza 6G ed intelligenza artificiale si ritrova anche nel lavoro di altri centri di ricerca e innovazione, perché a livello mondiale, secondo un Report Mind Commerce ("*Sixth generation cellular Report: looking beyond 5G to the 6G technology markets*"), i chipset IA potrebbero raggiungere le 240 milioni di unità già entro il 2028, mentre **il mercato 6G nel suo complesso (hardware, software, infrastrutture) potrebbe iniziare a valere 4,1 miliardi di dollari entro il 2030**.

https://www.key4biz.it/reti-del-futuro-con-il-6g-addio-agli-smartphone-esperienze-di-realta-estesa-e-fino-a-1-tbps-per-utente/270785/

Come gestire un attacco informatico e quali errori non fare. Il truck di IBM

Simulare un cyber attack, è un modo per capire come le aziende potrebbero reagire ad un eventuale attacco informatico imparando a gestire lo stress e a difendersi da un possibile data breach.

Tutto questo è opera di **IBM** che ha investito 200 milioni di dollari nella costruzione del'**X-Force Command Cyber Tactical Operations Center** (C-TOC), una sala operativa cyber su ruote, approdata al **Politecnico di Milano,** in piazza Leonardo da Vinci (dove rimarrà fino al 20 settembre).

X-Force Command C-TOC

[embedded content]
L' X-Force C-TOC è un **Cybersecurity Operation Center** basato sul modello dei centri operativi tattici utilizzati dalle postazioni di comando militari. La struttura mobile contiene un centro di sorveglianza, un data center e strutture per conferenze in grado di ospitare oltre venti operatori tra analisti e personale.

L'autoarticolato, equipaggiato con alimentazione autosufficiente e comunicazioni satellitari e cellulari, offre una rete sterile e resiliente per indagini sugli incidenti informatici e relativa risposta.

"*Grazie all'X-Force andiamo a creare una simulazione immersiva e integrale per far testare alle aziende la risposta ad un attacco informatico",* ha spiegato **Francesco Teodonno**, IBM

Security Leader per l'Italia. *"Gli attacchi al giorno d'oggi sono diventati molto più sofisticati, non parliamo di malware ma di veri e propri sistemi di attacco. Quindi per affrontare una sfida di questo tipo bisogna essere preparati a saper prendere l'attacco".*

La simulazione

Durante la simulazione cerchiamo di prendere in considerazione più punti di vista. Non solo l'aspetto tecnico, ma anche la gestione degli aspetti di leadership, di gestione del rischio, di gestione della comunicazione, di policy e la relazione che c'è con i media", ha spiegato durante la simulazione **Pompeo D'Urso**, C-TOC Technical Leader di IBM Security. *"E' quello che facciamo nella nostra tipologia di sessione, orientata quindi alla leadership e alla Business Relationship Responsive, nella quale l'azienda deve vedere il livello di preparazione nel caso in cui devono interagire anche con enti esterni.*

La sala operativa dell'X-Force durante la simulazione
"E' in virtù di tutta una serie di possibili attacchi – continua Pompeo *– come ad esempio problemi con i bancomat, problemi con la divulgazione online dei dati degli utenti e di quanti questi abbiamo un impatto sulla brand reputation, che ne può derivare un danno economico. Quindi bisogna considerare più punti di vista e allenarsi il più possibile per essere pronti ad affrontare nel momento in cui si è esposti ad un cyber attack".*

> *#CToc #CyberSecurity #IBM a #Milano in collaborazione con @polimi: #presstour e simulazione di un #CyberAttack: come gestire al meglio un attacco informatico. pic.twitter.com/vV4OlCAx9D*
>
> *— IBM Italia (@IBMItalia) September 12, 2019*

Formazione e mancanza di cyberskills

La funzione del camion C-TOC non è solo quella di aiutare le aziende nella loro formazione sulla sicurezza informatica, ma anche di fornire uno scopo educativo per aiutare a colmare il crescente divario delle **cyberskills**.

Portando il camion C-TOC nelle scuole e nelle università, IBM si augura di incoraggiare sempre più studenti a prendere in considerazione una carriera nel settore della sicurezza informatica.

L'X-Force Command C-TOC di IBM in piazza Leonardo Da Vinci a Milano
Nei prossimi giorni saranno ospiti del truck anche gli studenti del Politecnico che potranno provare le simulazioni **il 19 settembre**. Partito dagli Usa nel 2018 e dopo aver toccato le principali città europee, il truck andrà alla volta di Madrid per l'ultima tappa del suo tour europeo.

https://www.key4biz.it/come-gestire-un-attacco-informatico-e-quali-errori-non-fare-il-truck-di-ibm/270613/

Hackers are exploiting a platform-agnostic flaw to

track mobile phone locations

Enlarge / Simjacker attack flow.
AdaptiveMobile Security

reader comments

33 with 26 posters participating

Share this story

Hackers are actively exploiting a critical weakness found in most mobile phones to surreptitiously track the location of users and possibly carry out other nefarious actions, researchers warned on Thursday.

The so-called Simjacker exploits work across a wide range of mobile devices, regardless of the hardware or software they rely on, researchers with telecom security firm AdaptiveMobile Security said in a post. The attacks work by exploiting an interface intended to be used solely by cell carriers so they can communicate directly with the SIM cards inside subscribers' phones. The carriers can use the interface to provide specialized services such as using the data stored on the SIM to provide account balances.

Simjacker abuses the interface by sending commands that track the location and obtain the IMEI identification code of phones. They might also cause phones to make calls, send text messages, or perform a range of other commands.

"Pretty f***ing bad"

Dan Guido, a mobile security expert and the CEO of security firm Trail of Bits, told Ars the threat looked "pretty fucking

bad.” He added: “This attack is platform-agnostic, affects nearly every phone, and there is little anyone except your cell carrier can do about it.”

Over the past two years, AdaptiveMobile Security researchers said, they have observed devices from “nearly every manufacturer being successfully targeted to retrieve location.” Device makers include Apple, ZTE, Motorola, Samsung, Google, Huawei, and even those who produce Internet-of-things products that contain SIM cards. While basic attacks work on virtually all devices, more advanced variations—such as making a call—would work only on specific phones that don’t require users to confirm they want the call to go through.

The attacks were “developed by a specific private company that works with governments to monitor individuals,” Thursday’s report said. The researchers didn’t identify the exploit developer but said it had “extensive access” to core networks using both the SS7 and Diameter traffic-routing protocols. In some cases, the attacker exploits widely known weaknesses in SS7 as a fall-back mechanism when Simjacker attacks don’t work.

According to Motherboard reporter Joseph Cox, Sprint and T-Mobile said their customers weren’t vulnerable, and AT&T said its US-based network wasn’t affected. Verizon, meanwhile, said it had no indication it was affected either.

The attacks are happening to phones in “several” unnamed countries. Thursday’s report went on to say:

> *In one country we are seeing roughly 100-150 specific individual phone numbers being targeted per day via Simjacker attacks, although we have witnessed bursts of up to 300 phone numbers attempting to be tracked in a day, the distribution of tracking attempts varies. A few phone numbers, presumably high-value, were attempted to be tracked several hundred times over a 7-day period, but most had much smaller volumes.*

> *A similar pattern was seen looking at per-day activity, many phone numbers were targeted repeatedly over several days, weeks, or months at a time, while others were targeted as a once-off attack. These patterns and the number of tracking indicates it is not a mass surveillance operation, but one designed to track a large number of individuals for a variety of purposes, with targets and priorities shifting over time. The "first use" of the Simjacker method makes sense from this viewpoint, as doing this kind of large volume tracking using SS7 or Diameter methods can potentially expose these sources to detection, so it makes more sense to preserve those methods for escalations or when difficulties are encountered.*

The attacks work by sending targeted phones an SMS message that contains special formatting and commands that get passed directly to the universal integrated circuit card, which is the computerized smart card that makes modern SIMs work. The message contains commands for software—called the S@T browser—that runs on the SIM card. The commands cause the S@T browser to send the location of the unique IMEI of the device in a separate SMS message to a number designated by the attacker.

Here's how Thursday's report explained it:

> *The attack relies both on these specific SMS messages being allowed, and the S@T Browser software being present on the UICC in the targeted phone. Specific SMS messages targeting UICC cards have been demonstrated before on how they could be exploited for malicious purposes. The Simjacker attack takes a different approach, and greatly simplifies and expands the attack by relying on the S@T Browser software as an execution environment. The S@T (pronounced sat) Browser—or SIMalliance Toolbox Browser to give it its full name—is an application specified by the SIMalliance, and can be installed on a variety of UICC (SIM cards), including eSIMs. This S@T Browser software is not well known, is quite old, and its*

initial purpose was to enable services such as getting your account balance through the SIM card. Globally, its function has been mostly superseded by other technologies, and its specification has not been updated since 2009, however, like many legacy technologies it is still been used while remaining in the background. In this case we have observed the S@T protocol being used by mobile operators in at least 30 countries whose cumulative population adds up to over a billion people, so a sizable amount of people are potentially affected. It is also highly likely that additional countries have mobile operators that continue to use the technology on specific SIM cards.

This attack is also unique, in that the Simjacker Attack Message could logically be classified as carrying a complete malware payload, specifically spyware. This is because it contains a list of instructions that the SIM card is to execute. As software is essentially a list of instructions, and malware is "bad" software, then this could make the Simjacker exploit the first real-life case of malware (specifically spyware) sent within a SMS. Previous malware sent by SMS—such as the incidents we profiled here—have involved sending links to malware, not the malware itself within a complete message.

The researchers said other commands UICCs are capable of executing include:

- PLAY TONE
- SEND SHORT MESSAGE
- SET UP CALL
- SEND USSD
- SEND SS
- PROVIDE LOCAL INFORMATION (including location, battery, network, and language)
- POWER OFF CARD
- RUN AT COMMAND

- SEND DTMF COMMAND
- LAUNCH BROWSER
- OPEN CHANNEL (CS BEARER, DATA SERVICE BEARER, LOCAL BEARER, UICC SERVER MODE, etc.)
- SEND DATA
- GET SERVICE INFORMATION
- SUBMIT MULTIMEDIA MESSAGE
- GEOGRAPHICAL LOCATION REQUEST

The attack reported Thursday is similar to one demonstrated in 2013 at the Black Hat security conference in Las Vegas.

“We could trigger the attack only on SIM cards with weak or non-existent signature algorithms, which happened to be many SIM cards at the time,” Karsten Nohl, the chief scientist at SRLabs who presented the 2013 findings, told Ars. “AdaptiveMobile seems to have found a way in which the same attack works even if signatures are properly checked, which is a big step forward in attack research.”

Nohl added that he doubted Simjacker was being widely exploited, since location data is generally not interesting to criminals and other methods exist to track specific targets. Those methods include SS7 attacks, phone malware, or simply buying the data from mobile networks or app makers who collect it.

In response to the attacks, the SIMalliance—an industry group representing major UUIC makers—issued a new set of security guidelines for cellular carriers. The recommendations include:

- Implementing filtering at the network level to intercept and block “illegitimate binary SMS messages” and
- Making changes to the security settings of SIM cards issued to subscribers.

As Nohl noted, snoops have long had a variety of ways to track the location of many cellular devices. Thursday’s report means that, until carriers implement the SIMalliance

recommendations, hackers have another stealthy technique that previously went overlooked.

https://arstechnica.com/?p=1568241