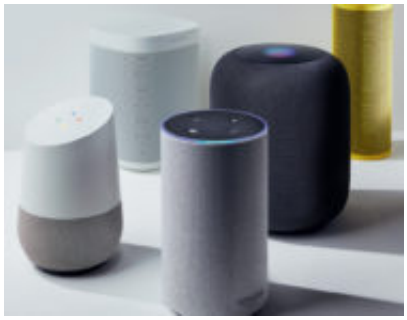
Da simpatici aiutanti a spie indiscrete: come proteggersi dagli “Smart Speaker”

Author : Emanuele Spagnoli

Date : 26 Febbraio 2019



Analizzando i dati relativi al boom di vendite di Smart Speaker degli ultimi mesi, compresi i record raggiunti durante gli ultimi Black Friday e Cyber Monday, **gli italiani sognano sempre di più una casa intelligente**, gestita attraverso semplici controlli vocali. Nelle nostre abitazioni è sempre più frequente ascoltare un “Ok Google!”, oppure un “Alexa!”, invece di un classico “Ciao!”. La possibilità di connettere, attraverso la rete Wi-Fi, qualsiasi sistema e oggetto presente nelle nostre case sta infatti introducendo nelle nostre vite **infinite possibilità di personalizzazione**, migliorando in maniera significativa la vivibilità domestica. Attraverso un comando vocale è possibile aprire e chiudere le porte, accendere e spegnere le luci senza doversi alzare, abbassare e alzare le tapparelle delle finestre, coordinare tutte le installazioni elettriche, termiche e idriche. La **rivoluzione digitale dell’IoT** (Internet of Things) è dunque entrata ufficialmente nelle nostre case.

Amazon Echo, Google Home, Homepod sono solo alcune tra le più conosciute soluzioni offerte sul mercato; quello che è certo è che gli **Smart Speaker** sono assoluti dominatori del momento. Tali dispositivi sono destinati ad essere una presenza costante nelle nostre case, introducendo innumerevoli benefici ma, allo stesso tempo, un'analoga quantità di problematiche relative a **sicurezza e privacy**. La connessione di questi dispositivi alla rete apre le porte, infatti, a tutti quei fattori di rischio cyber che gli italiani stanno lentamente ma inesorabilmente conoscendo.

Per “entrare subito nel gioco” e capire uno dei rischi che si incorrono con una semplice frase, consideriamo un semplice esempio[1]: un utilizzatore che vuole scaricare per la sua Smart TV un gioco chiamato "Quiz". Un malintenzionato potrebbe fare in modo che un’App si chiami "Quiz Perfavore" e, se un utente chiedesse educatamente di scaricare quel gioco, potrebbe inavvertitamente installare un’applicazione malevola senza nemmeno saperlo. Attraverso questa applicazione, lo sviluppatore avrebbe dunque accesso a dati e registrazioni vocali, che potrebbero essere utilizzati per ricattare la vittima.

In questo articolo si vogliono dunque analizzare alcuni dei **rischi cyber connessi agli Smart Speaker**, con alcuni esempi di possibili attacchi ed intrusioni cyber a cui gli stessi possono

essere soggetti, fornendo infine alcuni **semplici ma utili consigli** che l'utente può mettere in pratica per innalzare il livello di sicurezza dei propri dispositivi.

Porte aperte per gli Hacker

L'introduzione di nuovi dispositivi Smart tra le nostre mura introduce una quantità elevatissima di "porte" che gli hacker potrebbero tranquillamente aprire senza far alcun rumore. La figura del ladro scassinatore sarà infatti presto sostituita da abili hacker capaci di rubare le nostre chiavi di casa, o della nostra impresa, senza mai incontrarci di persona.

Sfruttando l'esplosione nelle vendite di Smart Assistant, ad aprile 2017, Burger King ha sperimentato negli Stati Uniti una breve pubblicità di 15 secondi fatta appositamente per sfruttare la popolarità dell'assistente vocale di Google. Nella pubblicità un impiegato, sostenendo di non avere abbastanza tempo per descrivere tutte le caratteristiche del famoso Whopper, si avvicina alla telecamera dicendo: "Ok Google, che cos'è l'hamburger Whopper?". Sentendo una domanda di questo tipo, l'assistente vocale risponde di solito leggendo le prime righe di una voce di Wikipedia in tema. In questa maniera, attraverso lo spot in televisione, in tantissime case americane è stato attivato l'assistente vocale che ha iniziato ad elencare tutti gli ingredienti del famoso panino.

Per alcuni, è stata una idea geniale di marketing; per altri, un'opportunità per portare alla luce i rischi posti dagli assistenti vocali, sempre più presenti nella vita quotidiana.

Sfruttando il fatto che **questi assistenti non vengono mai "spenti"**, possono rispondere a determinati comandi vocali anche quando i dispositivi a cui sono collegati risultano bloccati. In questo modo, alcuni ricercatori[2] hanno trovato un modo per aggirare la schermata della password su un computer Windows utilizzando Cortana, l'assistente virtuale di Windows 10.

Un'altra vulnerabilità che ha invece visto protagonista la Apple è relativa alla **funzionalità di riservatezza** che può essere utilizzata dall'utente per nascondere il contenuto dei messaggi che appaiono sulla schermata di blocco dei suoi dispositivi. Tale funzione è stata aggirata sfruttando proprio Siri, l'assistente vocale proprietario di Apple, trasformandolo in un "cavallo di Troia". Il sito web brasiliano Mac Magazine[3] ha infatti rivelato che chiunque poteva accedere a questi messaggi nascosti, chiedendo semplicemente a Siri di leggerli ad alta voce.

Ma c'è ancora molto altro, ancora più preoccupante: gli Smart Speaker possono sentire anche quello che l'udito umano non può percepire. Parliamo infatti di un particolare tipo di attacco chiamato "**Dolphin Attack**". Tale tipologia di attacco richiama proprio il fatto che i delfini sono in grado di sentire una gamma molto più ampia di frequenza rispetto agli esseri umani, fino a 7 volte maggiore.

Attraverso tali attacchi audio, alcuni ricercatori[4] stanno sfruttando il divario tra riconoscimento vocale umano e quello della macchina. I sistemi di riconoscimento vocale tipicamente traducono ciascun suono in una lettera, eventualmente alla fine in parole e frasi. Modificando leggermente file audio come registrazioni e musiche, i ricercatori hanno dimostrato che è effettivamente possibile nascondere un comando vocale all'interno di altre registrazioni in un modo che è quasi

irrilevabile per l’udito umano. Ma un simile attacco potrebbe essere condotto anche sfruttando trasmettitori ad ultrasuoni. Tale avvertimento è stato confermato quando ricercatori dell'Università dell'Illinois hanno dimostrato la possibilità di condurre attacchi ad ultrasuoni da circa 8 metri di distanza. Sebbene tali comandi non potevano penetrare nei muri, è stato possibile controllare gli Smart Speaker attraverso le finestre aperte di un edificio.

E la Privacy?

Le tipologie di attacco contro tali dispositivi intelligenti sono in continuo aumento; maggiore sarà la loro diffusione nelle nostre case e maggiori saranno gli sforzi che hacker ed attori malintenzionati faranno per poter irrompere nelle nostre vite.

Attraverso il controllo dei dispositivi intelligenti, un hacker potrebbe visitare siti Web dannosi, avviare telefonate, scattare una foto o inviare messaggi di testo. È chiaro che un utente, acquistando un dispositivo simile, introdurrebbe un ulteriore fattore di rischio per la propria privacy.

Google, a novembre 2018, durante un evento organizzato a San Francisco all'interno di un'abitazione da diversi milioni di dollari[5], ha allestito un modello di casa intelligente dotato di ogni dispositivo Google e di tutti i gadget immaginabili connessi in rete, svelando il suo piano di portare almeno un dispositivo intelligente in ogni stanza della casa. Un ecosistema digitale progettato per consentire la comunicazione tra le stanze ed i suoi proprietari, anche se non fisicamente presenti a casa.

Ma **cosa accadrebbe se tali dispositivi trasmettessero conversazioni riservate o registrassero i nostri movimenti a nostra insaputa?**

MailOnline[6] ha ricevuto un numero di trascrizioni di conversazioni che mostrano i record che Google conserva delle ricerche effettuate utilizzando gli assistenti vocali. Un record sembra sia stato registrato accidentalmente, all'insaputa dell'utente. Una trascrizione scritta della registrazione rivela: "Se per qualche ragione hai bisogno di entrare a casa mia, il codice di sicurezza per la porta sul retro è 0783".

Ricorderete sicuramente le numerose notizie riguardanti i ladri che preparavano il colpo in un appartamento segnando sul citofono alcuni simboli per indicare le caratteristiche dell'appartamento o della famiglia su cui portare a termine il furto. Il nuovo ladro non avrà più bisogno di doversi scomodare per tali ricognizioni; accedendo ai vari dispositivi potrebbe registrare i piani delle nostre vacanze, i numeri della carta di credito quando vengono dettati per ordinare un pasto o, semplicemente, per sapere chi è presente in casa in un giorno specifico. I dati raccolti possono quindi essere utilizzati dai criminali per ricattare, derubare o impersonare una persona online per varie finalità.

Registrazioni e dati provenienti da Smart Speaker, inoltre, potrebbero essere utilizzati anche per scopi totalmente diversi da quelli sopra descritti. È infatti recente la notizia[7] che un giudice del New Hampshire ha ordinato ad Amazon di fornire due giorni di registrazioni per la risoluzione in un caso di duplice omicidio.

I pubblici ministeri ritengono che le registrazioni, effettuate da un Amazon Echo presente nella casa in cui due donne sono state uccise nel gennaio 2017, possano fornire ulteriori indizi sul loro assassino.

Prevenire è meglio che curare

Come è possibile adottare alcuni accorgimenti utili a proteggere i nostri dispositivi e la nostra privacy anche dai più banali incidenti?

Si propongono di seguito alcuni consigli che qualsiasi utente può mettere facilmente in pratica ma che allo stesso tempo eviteranno di imbattersi in spiacevoli sorprese:

- **Collegare l'essenziale:** come linea guida di base non si dovrebbero collegare agli assistenti vocali dispositivi di sicurezza quali serrature delle porte, allarmi o cassette di sicurezza, a meno che gli stessi non siano protetti attraverso ulteriori metodi come l'autenticazione a due fattori. Lo stesso vale per le relative informazioni sensibili: questi dispositivi non devono essere mai utilizzati per memorizzare password o altri dati come quelli della carta di credito.
- **Utilizzare una rete Wi-Fi crittografata WPA2**: è una regola generale che dovrebbe essere adottata non appena si introduce un router Wi-Fi nelle nostre case. Che si usi un assistente vocale o qualsiasi altro dispositivo IoT, è necessario utilizzare una rete con crittografia WPA2 ed una password sicura diversa da quella di default.
- **Cancellare la cronologia dei comandi vocali**: tutti i principali assistenti vocali consentono di rivedere la cronologia dei comandi vocali impartiti. È dunque buona prassi eliminare frequentemente la cronologia dei comandi vocali ed eliminare eventuali registrazioni memorizzate. Un malintenzionato, ottenendo l'accesso all'account collegato allo Smart Speaker, potrebbe facilmente accedere alla cronologia o alle registrazioni archiviate.
- **Spegnere/disattivare lo Smart Speaker**: sapendo che per un periodo più o meno prolungato non si farà utilizzo dell'assistente vocale, disattivalo. Potrebbe essere un po' scomodo perché probabilmente lo si troverà spento/disattivato una volta che se ne avrà effettivamente bisogno ma questo accorgimento potrebbe evitare che l'assistente venga utilizzato contro il nostro volere.
- **Non disabilitare gli aggiornamenti automatici**: i dispositivi possono avere diverse vulnerabilità, come dimostrato dall'episodio relativo alla connessione Bluetooth noto come BlueBorne. Questa vulnerabilità consentiva ad un attaccante di prendere facilmente il controllo di uno Smart Speaker solamente entrando nel suo raggio d'azione. Le vulnerabilità BlueBorne sono state successivamente riparate e, pertanto, tutti i dispositivi dovrebbero utilizzare la funzionalità di aggiornamento automatico per installare tempestivamente le patch rilasciate.
- **Abilitare un "beep" prima di ogni registrazione**: gli Smart Speaker generalmente si illuminano ogni volta che vengono attivati, dando modo di capire all'utente che può impartire il comando vocale. Se invece il dispositivo non è all'interno del campo visivo, l'utente potrebbe non sapere se il dispositivo sia attivato o meno. Come buona regola sarebbe importante abilitare la funzionalità che riproduce un breve segnale acustico ogni qualvolta l'assistente vocale viene attivato.

Alcune tipologie di attacco più tradizionali - come il ransomware o il phishing - risultano ancora più diffuse e facili da usare per i criminali informatici ma, di fronte all'infinita immaginazione degli hacker, è necessario sensibilizzare l'utente su tutte le problematiche di sicurezza e privacy connesse agli Smart Speaker. A seguito delle impronte digitali, le impronte vocali potrebbero dunque essere la **nuova password biometrica** per autenticare chi ha accesso agli assistenti vocali?

Sitografia

[1] https://www.cnet.com/news/voice-of-concern-smart-assistants-are-creating-new-openings-for-hackers/.

[2] https://www.stormshield.com/voice-assistants-and-cybersecurity-is-it-already-too-late/.

[3] https://macmagazine.uol.com.br/2018/03/20/bug-de-privacidade-do-ios-faz-a-siri-ler-notificacoes-escondidas-na-tela-bloqueada/.

[4] https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html.

[5] https://edition.cnn.com/2018/11/14/tech/google-demo-home/index.html.

[6] https://www.dailymail.co.uk/sciencetech/article-6392913/Google-wants-virtual-assistant-room-home.html.

[7] https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case/.

Articolo a cura di **Emanuele Spagnoli**