Come funziona la smart home e come è possibile hackerarla!

Lug 23, 2019 Kaspersky Attacco non convenzionale, Kaspersky Partner Space, Minacce, Social engineering 1

Le *smart home* stanno diventando sempre più comuni ormai; se qualche tempo fa solo gli appassionati di tecnologie richiedevano **il meglio della domotica**, al giorno d'oggi si tratta di sistemi sempre più popolari e alla portata di quasi tutte le tasche.

Sono passati anni da quando è stata effettuata la prima indagine sulla sicurezza dell'Internet of Things (IoT) e **la continua espansione ed evoluzione del panorama IoT** ha reso sempre più importante questo tipo di ricerche.

Infatti, insieme a nuovi prodotti e soluzioni emergono anche **nuove minacce che mettono a repentaglio la sicurezza degli utenti**. Un dipendente di Kaspersky ha invitato i ricercatori dell'azienda a esaminare il sistema smart implementato nella propria abitazione concedendo ai ricercatori l'accesso al controller della sua smart home.

È stato scelto il controller perché è **in grado di collegare e supervisionare tutte le operazioni dell'intera smart home** e, in caso di una riuscita compromissione, consentirebbe ad un criminale informatico di penetrare nell'intero ecosistema domestico ed effettuare qualsiasi tipo di operazione, dallo spionaggio al furto fino al sabotaggio fisico.

La fase iniziale di raccolta delle informazioni ha portato gli esperti a identificare i vari vettori potenziali di attacco ovvero **il protocollo di comunicazione wireless Z-Wave** ampiamente utilizzato per la domotica, l'interfaccia web del pannello di amministrazione e l'infrastruttura cloud.

Quest'ultima si è rivelata il vettore di attacco più efficace: l'esame dei metodi usati per elaborare le richieste del dispositivo ha rivelato **una vulnerabilità nel processo di autorizzazione** e la possibilità di esecuzione del codice a distanza.

Combinati tra loro, questi vettori permetterebbero a terzi di **accedere a tutti i backup caricati sul cloud** da tutti i Fibaro

Home Center Lite e di caricare, sempre sul cloud, backup infetti e, in seguito, di scaricarli su uno specifico controller, pur non avendo diritti di amministrazione sul sistema.

Per finalizzare l'esperimento, gli esperti di Kaspersky hanno effettuato un test di **attacco sul controller**. Per farlo, hanno preparato uno specifico backup con uno script protetto da password e sviluppato separatamente.

Successivamente, tramite cloud, hanno **inviato un'email e un SMS al dispositivo del proprietario**, invitandolo ad aggiornare il firmware del controller. Come richiesto, la "vittima" ha accettato e scaricato il backup infetto.

Questo ha permesso ai ricercatori di **ottenere i diritti di amministratore sullo smart home controller**, consentendo loro di manipolare l'ecosistema connesso. Per dimostrare il successo della loro intrusione nel sistema, i ricercatori hanno modificato la suoneria della sveglia. Il giorno dopo, il dipendente di Kaspersky è stato svegliato da una musica fatta di percussioni e bassi che suonava a tutto volume.

Naturalmente, una persona accorta e che sa qualcosa di sicurezza informatica si renderebbe conto subito che si tratta di un'esca, ma **un utente medio e ingenuo probabilmente non vedrebbe nulla di sospetto**. Ed è in questo modo che i cybercriminali hanno ottenuto l'accesso allo smart hub e a tutti i dispositivi che esso gestiva.

E, ancora più importante, **hanno ottenuto accesso alla rete domestica**. Questo significa che sono riusciti ad aprire da remoto la porta principale, a disattivare le telecamere di sicurezza lasciando campo libero ai ladri. Per maggiori dettagli potete leggere il report su Securelist.

Per la sicurezza dei dispositivi i ricercatori di Kaspersky raccomandano di:

- Valutare i rischi legati alla sicurezza qualora si decidesse di rendere una parte della propria vita più “smart”
- Fare una ricerca su internet circa le possibili vulnerabilità presenti prima di comprare un dispositivo IoT
- Oltre ai bug standard che si trovano nei nuovi prodotti, i dispositivi lanciati di recente potrebbero avere problemi di sicurezza che non sono stati ancora scoperti dai ricercatori. Con questa premessa, la scelta migliore è quella di acquistare prodotti che hanno già sperimentato diversi aggiornamenti software piuttosto che i prodotti più recenti rilasciati sul mercato.
- Assicurarsi che tutti i dispositivi siano aggiornati con i protocolli di sicurezza e i firmware più recenti.

- Adottare il servizio Kaspersky Security Cloud che protegge l’account online dell’utente e la rete Wi-Fi di casa, assicurandosi che la private network rimanga privata: facendo questo, l’utente riceverà una notifica nel caso in cui ospiti indesiderati cerchino di connettersi proteggendo tutti i dispositivi IoT dell’abitazione. L’utente sarà automaticamente avvisato in caso di minacce alla sicurezza e sarà supportato da esperti che, se necessario, agiranno di conseguenza.

Condividi l’articolo

Falla in ProFTPd. Un milione di server vulnerabili La Russia come gli USA: ecco i piani di spionaggio sul Web

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/07/23/come-funziona-la-smart-home-e-come-e-possibile-hackerarla/