Sopravvivere in un mondo sempre più dipendente dalla tecnologia IoT: ecco come utilizzare i dispositivi intelligenti e stare al sicuro dagli attacchi hacker

I ricercatori di Kaspersky Lab hanno scoperto elementi di particolare interesse: macchine da caffè che mettono a repentaglio le password delle reti Wi-Fi; baby monitor che consentono agli hacker di spiarvi; sistemi di sicurezza domestica, controllati da smartphone, che possono essere "ingannati" con un semplice magnete.

Sommario

Victor Alyushin, Vladimir Krylov

Le ricorrenti voci allarmistiche che circolano attorno all'Internet delle Cose (Internet of Things, IoT) evocano immagini di individui malintenzionati vestiti con felpe anonime, che vivono per l'hacking, e per rendere più difficile la vita degli altri, inventandosi milioni di modi diversi per infiltrarsi nelle vostre vite, proprio attraverso i dispositivi che possedete. Una simile percezione rappresenta, ad ogni caso, una ragione sufficiente per smettere di utilizzare i dispositivi smart? Noi non la pensiamo in questo modo; riteniamo, comunque, che i clienti debbano essere consapevoli dei potenziali rischi

esistenti, e debbano essere ugualmente a conoscenza delle modalità che permettono di mitigare tali rischi, prima di avventurarsi nel complesso mondo dei dispositivi IoT.

Più di un anno fa, un nostro collega del Global Research and Analysis Team, David Jacoby, si è messo a dare un'occhiata in giro, nel proprio soggiorno di casa, decidendo di investigare su quanto potessero essere vulnerabili, nei confronti di eventuali cyber-attacchi, i dispositivi in suo possesso. Egli ha scoperto, in pratica, come quasi tutti risultassero vulnerabili. Ci siamo quindi chiesti: si è trattato, nell'occasione, di una semplice coincidenza, oppure i prodotti intelligenti 'IoT' attualmente presenti sul mercato possono essere realmente oggetto di violazione da parte di malintenzionati? Per trovare una risposta a tale quesito, alcuni mesi fa abbiamo raccolto una selezione casuale di dispositivi domestici collegati in Rete, ed abbiamo iniziato ad esaminare il funzionamento degli stessi.

I dispositivi prescelti per la conduzione del nostro esperimento sono stati i seguenti:

- un dongle USB per lo streaming video (Chromecast di Google);
- una telecamera IP controllata tramite smartphone;
- una macchina da caffè controllata da smartphone;
- un sistema di sicurezza domestica, anch'esso controllato tramite smartphone.

Il compito che ci siamo posti era alquanto semplice: scoprire se qualcuno di questi prodotti poteva costituire, per il proprietario dello stesso, una minaccia a livello di sicurezza IT. I risultati della ricerca da noi condotta hanno fornito numerosi spunti di riflessione.

Google Chromecast. Hacking IoT per principianti

Rischio: il contenuto trasmesso in streaming sullo schermo della vittima può provenire da una fonte di cui è proprietario un attacker

Chromecast, aggiornato di recente con una versione più avanzata, è un dispositivo interessante. Si tratta di un dongle USB dal costo limitato, il quale consente di trasmettere in streaming contenuti multimediali dal proprio smartphone, o tablet, ad una TV o ad un altro schermo. Funziona così: l'utente collega il dispositivo alla porta HDMI del televisore; Chromecast in tal modo si accende. Il dongle USB di Google lancia poi la propria rete Wi-Fi, per la configurazione iniziale. Una volta stabilita la connessione con uno smartphone o un tablet, Chromecast spegne il suo Wi-Fi, e si collega alla rete Wi-Fi domestica di cui è provvisto l'utente. È un dispositivo molto comodo, conveniente e di facile utilizzo.

Esso, tuttavia, potrebbe divenire molto meno conveniente, e decisamente poco “amichevole” nei confronti dell’utente, qualora nelle sue vicinanze si trovasse un hacker. La famosa vulnerabilità “rickrolling”, scoperta da Dan Petro, consulente per la sicurezza IT, ne è la prova. Tale vulnerabilità consente, di fatto, di poter trasmettere in streaming, sullo schermo dell’utente-vittima, contenuti provenienti da una fonte di cui è proprietario l’attacker. Ecco come funziona lo schema in questione: l'attaccante invia al dispositivo un elevato numero di speciali richieste ‘disconnect’, utilizzando un device malevolo, basato su Raspberry Pi; quando poi Chromecast, in risposta, attiva il proprio modulo Wi-Fi, Google Chromecast si ricollega al dispositivo dell’attacker: viene così realizzato lo streaming dei contenuti desiderati dall’hacker.

L’unico modo per evitare tutto questo è spegnere la TV, collocare il dongle al di fuori della portata del vostro hotspot Wi-Fi ed attendere finché l’attacker non si sia annoiato, lasciandovi così in pace.

La sola limitazione, riguardo a tale genere di attacco, consiste nel fatto che l’attacker dovrà necessariamente trovarsi nel range della rete Wi-Fi alla quale è connesso il Chromecast preso di mira. Abbiamo tuttavia scoperto, effettuando il nostro esperimento, che non si tratta per forza di una restrizione, qualora si disponga di un’antenna Wi-Fi direzionale, anche dal costo contenuto, e di qualche software Kali Linux. Utilizzando tale sistema abbiamo in effetti scoperto che Chromecast può essere sottoposto a “rickrolling” da una distanza molto maggiore rispetto al normale range di segnale che caratterizza i network Wi-Fi domestici. Questo significa che, mentre con l’hack originale realizzato da Dan Petro l’attaccante correrebbe il rischio di essere scoperto dal proprietario del Chromecast, di sicuro molto arrabbiato nei suoi confronti, con un’antenna direzionale tale “rischio”, in pratica, non sussiste più.

Da parte nostra, non consideriamo certo tale elemento alla stregua di una nuova scoperta nel campo della sicurezza; esso amplifica, semplicemente, un problema di sicurezza già ben conosciuto, e per il quale non è stata ancora rilasciata la patch occorrente. Si tratta, se vogliamo, di una sorta di esercizio

per principianti a livello di hacking rivolto ai dispositivi IoT, anche se ciò che abbiamo appena descritto potrebbe essere utilizzato in modo realmente nocivo; su tale argomento, ad ogni caso, torneremo in seguito. Riferiremo, innanzitutto, in merito alle altre scoperte emerse a seguito della breve ricerca da noi condotta.

Mitigazione: Utilizzare in locali remoti della vostra abitazione; questo ridurrà il rischio di eventuali attacchi eseguiti tramite antenna direzionale.

Stato attuale: Non patchata

Telecamera IP

Problema n. 1

Rischio: gli attacker ottengono l'accesso agli indirizzi e-mail relativi a tutti gli utenti della telecamera che hanno sperimentato problemi tecnici

La telecamera IP oggetto della nostra analisi è stata adibita, dal produttore, alla specifica funzione di baby monitor. In pratica, si posiziona il dispositivo nella camera del bambino, si scarica un'applicazione sul proprio smartphone, si collega la telecamera all'app e alla rete Wi-Fi, ed il gioco è fatto: potrete monitorare vostro figlio ogni volta che volete, da qualsiasi luogo lo desideriate.

Vi state forse chiedendo, adesso, per quale motivo qualcuno dovrebbe hackerare proprio un baby monitor. In realtà, sono stati registrati vari casi del genere, verificatisi già a partire dal 2013: http://www.cbsnews.com/news/baby-monitor-hacked-spies-on-texas-child/. Un caso simile è avvenuto nel 2015: http://www.kwch.com/news/local-news/whitewater-woman-says-her-baby-monitor-was-hacked/32427912. Vi sono quindi persone che, per un motivo o per l'altro, intendono hackerare i baby monitor.

Quando abbiamo analizzato la nostra telecamera IP (nella primavera del 2015), esistevano due diverse applicazioni, per i clienti, che consentivano di poter comunicare con il dispositivo. Entrambe presentavano problemi di sicurezza. Abbiamo in seguito appreso, dal produttore, che una di tali applicazioni era, in realtà, un'app legacy, quindi già "vecchia"; essa, ad ogni caso, veniva ancora

utilizzata da un certo numero di proprietari del dispositivo. Abbiamo scoperto che la suddetta applicazione legacy conteneva credenziali hardcoded relative ad un account Gmail.

```
public static final String EMAIL_FROM = "*****@gmail.com";

    public static final String EMAIL_PASSWORD = "**********";

    public static final String EMAIL_PORT = "465";

    public static final String EMAIL_SMTP_HOST = "smtp.gmail.com";

    public static final String EMAIL_TO;

    public static final String EMAIL_TO_MAXIM = "maximidc@gmail.com";

    public static final String EMAIL_TO_PHILIPS = "*****@philips.com";

    public static final String EMAIL_USERNAME = "*****@gmail.com";
```

Il vendor ci ha comunicato, in seguito, che l'account di posta elettronica veniva utilizzato per raccogliere i report relativi ad eventuali problemi tecnici riscontrati dagli utenti della telecamera.

Il fatto è che, nella circostanza, i report in questione venivano inviati al suddetto account, prestabilito dal vendor, attraverso gli indirizzi e-mail personali degli utenti. Un ipotetico attaccante, quindi, non avrebbe nemmeno avuto bisogno di acquistare una telecamera; sarebbe risultato sufficiente, per eventuali malintenzionati, effettuare il download e il reverse-engineering di una delle due applicazioni, per accedere all'account e-mail tecnico, e raccogliere così gli indirizzi di posta elettronica di tutti gli utenti del dispositivo che si fossero trovati ad affrontare problemi di natura tecnica. Sarebbe davvero un grosso problema, se la vostra e-mail venisse "esposta" a terze parti a seguito dello sfruttamento di tale vulnerabilità? Sì, potrebbe esserlo. Tuttavia, realisticamente parlando, la vulnerabilità sopra descritta non sembra essere un bersaglio così allettante per realizzare una raccolta in massa di informazioni personali, in primo luogo per la base relativamente limitata di potenziali vittime. I problemi tecnici, inoltre, si manifestano raramente; per di più, l'applicazione era in pratica già "vecchia", e non così diffusa, al momento della conduzione della nostra indagine. I baby monitor, tra l'altro, sono un prodotto di nicchia; per tale motivo non viene di certo custodito un numero di indirizzi e-mail così elevato.

D'altro canto, se possedete un baby monitor, siete molto probabilmente dei genitori; questo fa di voi (e del vostro indirizzo e-mail, per estensione) un target molto più interessante, nel caso in cui un attacker pianifichi una campagna fraudolenta mirata.

In altre parole, non si tratta di una vulnerabilità di sicurezza critica; la stessa, tuttavia, potrebbe essere ancora utilizzata da eventuali aggressori. Non è stata, in ogni caso, l'unica vulnerabilità da noi rilevata nel momento in cui abbiamo analizzato il funzionamento della telecamera e delle relative applicazioni.

Stato attuale: risolta

Problema n. 2

Rischio: pieno controllo della telecamera da parte di un attaccante

Dopo aver esaminato l'applicazione legacy, siamo passati alla versione più recente della stessa, ed abbiamo immediatamente individuato un'altra interessante problematica.

L'applicazione comunica con la telecamera attraverso un servizio cloud; la comunicazione tra l'app e il cloud service risulta inoltre codificata tramite protocollo https. Per eseguire la procedura di autenticazione, l'applicazione si avvale dell'ID di sessione, il quale viene automaticamente cambiato ogni volta che un utente avvia una nuova sessione. Potrebbe sembrare, in apparenza, un'operazione del tutto sicura; di fatto, è possibile intercettare l'ID della sessione e controllare la telecamera attraverso il cloud, oppure recuperare la password necessaria per l'accesso locale al dispositivo.

Prima che l'applicazione avvii lo streaming dei dati provenienti dalla telecamera IP, essa provvede ad inviare una richiesta http al servizio cloud:

```
type=android&id=APA91bEjfHJc7p6vw3izKmMNFYt7wJQr995171iGq2kk_rD4XaMEHhTXqTmFaAALjWD15bnaVcyMuV2a7
zvEFdtV13QXildHQn0PCvQbPikag2CPJwPwOWWsXtP7B0S-Jd3W-7n0JUo-nMFg3-
Kv02yb1AldWBPfE3UghvwECCMANYU3tKZCb2A&sessionId=100-U3a9cd38a-45ab-4aca-98fe-29b27b2ce280
```

Tale richiesta contiene l'ID della sessione, che potrebbe essere intercettato, visto che la query viene inviata in chiaro. Il Session ID viene in seguito utilizzato per recuperare la password corrente. Abbiamo scoperto che ciò potrebbe essere realizzato creando un apposito link, contenente, nella sua parte finale, proprio l'ID della sessione.

https://*****/*****/*****sessionId=100-U3a9cd38a-45ab-4aca-98fe-29b27b2ce280

In cambio del link, il servizio cloud invierebbe la password relativa alla sessione.

https:// *****/*****/*****sessionId=100-U3a9cd38a-45ab-4aca-98fe-29b27b2ce280

… "local_view":{"password":"N2VmYmVlOGY4NGVj","port":9090} …

Utilizzando la password, è possibile ottenere il pieno controllo della telecamera IP, incluso la possibilità di guardare il video trasmesso in streaming, ascoltare l'audio, e riprodurre l'audio sul dispositivo stesso.

È importante sottolineare che non si tratta, nella fattispecie, di un attacco remoto: in effetti, per poter intercettare la richiesta iniziale, l'attacker deve necessariamente trovarsi sulla stessa rete di cui si avvale l'utente dell'applicazione; tale circostanza, ovviamente, rende meno probabile lo sfruttamento della vulnerabilità. Gli utenti dell'app dovrebbero ad ogni caso agire con cautela, specialmente se fanno uso di network particolarmente estesi e frequentati, ai quali accedono, di solito, molte persone. Ad esempio, se si collega alla propria telecamera attraverso una rete Wi-Fi pubblica, l'utente potrebbe esporsi al rischio derivante dalla presenza di un attacker all'interno del medesimo network. In simili condizioni, non sarebbe certo difficile immaginare uno scenario - a livello di utilizzo dell'app nella vita di tutti i giorni - che prospetti il coinvolgimento di una terza parte.

Stato attuale: risolta

Problema n. 3

Rischio: God Mode – un attacker può fare qualsiasi cosa con il firmware della telecamera

Il terzo problema a livello di sicurezza IT, individuato durante la ricerca da noi condotta in merito alla telecamera IP controllata tramite smartphone, non risiedeva nell'applicazione, bensì nella telecamera stessa. Si tratta di un problema piuttosto semplice, legato alla password di root assegnata in fabbrica per il protocollo di rete SSH, a livello di firmware. Semplice, certo, in quanto la telecamera funziona su Linux, e la relativa password di root abilita il God Mode per chiunque abbia accesso al dispositivo e conosca la

password. Risulta così possibile fare qualsiasi cosa con il firmware di cui è provvista la telecamera IP: modificarlo, oppure cancellarlo, in pratica qualunque cosa. Tutto quello che un ipotetico attaccante deve fare, per estrarre la password, è semplicemente scaricare ed estrarre il firmware dal sito web del produttore (anche se l'attacker, in realtà, avrebbe bisogno di trovarsi all'interno della medesima rete utilizzata dal device sottoposto ad attacco, per ottenere l'URL attraverso il quale viene effettuato il download del firmware), estrarre lo stesso e seguire questo percorso: \\ubifs\\home/.config. Ed eccola qua, sotto forma di semplice testo.

```
CONFIG_*******_ROOT_PASSWORD="sVGhNBRNyE57"

CONFIG_*******_ROOT_PASSWORD="GFg7n0MfELfL"
```

La cosa più preoccupante, nella circostanza, è che, a meno di non essere un esperto di Linux, non vi è davvero modo, per un utente inesperto, di rimuovere o modificare la password da solo.

Il motivo per cui la password SSH si trovasse proprio lì rimane per noi un mistero, anche se abbiamo alcune idee in proposito. L'accesso di root, in effetti, potrebbe rivelarsi utile per sviluppatori e specialisti del supporto tecnico, in una situazione in cui un cliente si imbatte in un problema tecnico imprevisto, che non può essere risolto telefonicamente. In tal caso, uno specialista potrebbe connettersi da remoto alla telecamera IP, utilizzare la password SSH per ottenere l'accesso di root e risolvere così il problema. A quanto pare, si tratta di una pratica comune per i nuovi modelli di tali dispositivi, i quali possono contenere bug che non sono stati ancora scoperti e corretti nella fase precedente al rilascio. Abbiamo poi dato un'occhiata al firmware di cui sono dotate altre telecamere, prodotte da un vendor alternativo; anche qui abbiamo individuato le password SSH. Nella circostanza, la conclusione che abbiamo tratto è la seguente: gli sviluppatori lasciano la password SSH nel firmware, per essere poi in grado di correggere eventuali bug inattesi; in seguito, quando viene rilasciata una versione stabile del firmware, gli stessi si dimenticano, semplicemente, di rimuovere o crittografare la password.

Una seconda ipotesi da noi formulata suggerisce, invece, che gli sviluppatori si dimenticano, in pratica, del fatto che il firmware contiene tale password. L'indagine da noi svolta ci ha inoltre permesso di scoprire che il componente del dispositivo in cui sono state trovate le password SSH, ovvero il chipset, viene abitualmente fornito da un vendor di terze parti. E tale produttore, per convenienza, lascia di default la password SSH nella telecamera, per assicurarsi che il vendor del prodotto finale (il baby monitor) possa essere in grado di regolare il chipset e di collegare lo stesso con altro hardware e software. Il vendor esegue poi tali operazioni, e semplicemente si dimentica, in seguito, di rimuovere la password. Non potrebbe essere più semplice di così.

Stato attuale: risolta

Comunicazioni intercorse con il vendor

Non è stato affatto difficoltoso scoprire le vulnerabilità qui sopra descritte; dobbiamo al tempo stesso ammettere che non è stato nemmeno difficile riferire al vendor riguardo ad esse, così come aiutare quest'ultimo a risolverle. La telecamera utilizzata per effettuare la nostra ricerca portava il marchio Philips, anche se, effettivamente, era stata Gibson Innovations a produrla e curarne la manutenzione. I rappresentanti della società si sono dimostrati estremamente rapidi nel reagire alle problematiche

evidenziate nel nostro report. Le vulnerabilità da noi segnalate sono state così corrette, sia a livello di telecamera IP, sia delle relative applicazioni (Android e iOS).

Questo autunno, Rapid7 ha pubblicato un report davvero molto interessante riguardo alle vulnerabilità individuate nei baby monitor; nell'elenco dei dispositivi vulnerabili è stato tra l'altro inserito un prodotto Philips (una versione leggermente diversa rispetto a quella da noi esaminata): è stata in effetti rilevata, riguardo ad esso, una serie di vulnerabilità, alcune delle quali simili a quelle scoperte nel corso della nostra ricerca. A giudicare dalle apposite timeline "dalla-scoperta-alla-patch" presentate nel report, Gibson Innovations è tuttavia uno dei pochi vendor di dispositivi IoT a prendere seriamente in considerazione i problemi di sicurezza riscontrati nei propri prodotti, e a far questo, oltretutto, con pregevole continuità. A loro vanno i nostri complimenti, per l'approccio responsabile dimostrato a più riprese.

Ma torniamo alla nostra ricerca.

Qualcuno potrebbe affermare che i problemi di sicurezza da noi scoperti nella telecamera IP implicano necessariamente il dover accedere alla stessa rete utilizzata dal proprietario del dispositivo, o alla telecamera stessa; tale osservazione è corretta. Questo, tuttavia, non rappresenta affatto un ostacolo insormontabile per un eventuale attacker, soprattutto se l'utente dispone di un altro device connesso a tale rete.

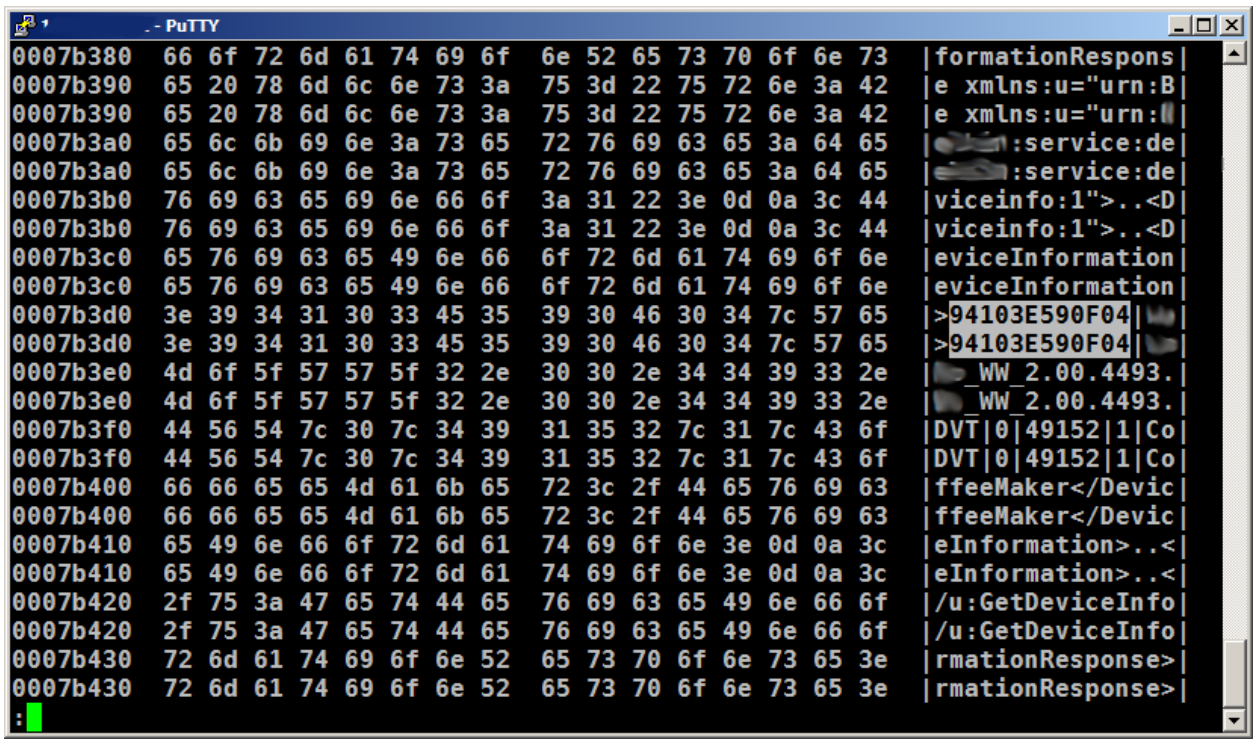
Una macchina da caffè controllata tramite smartphone

Che cosa potrebbe mai accadere?

Rischio: fuga della password utilizzata per accedere alla rete wireless domestica

La macchina da caffè che abbiamo casualmente scelto è in grado di preparare, dietro apposito comando impartito da remoto, una bella tazza di caffè, nel momento esatto in cui l'utente lo desidera. Basta semplicemente impostare l'orario, e quando il caffè è pronto la relativa applicazione provvede ad inviarvi una notifica push. È inoltre possibile monitorare lo stato della macchina attraverso un'app dedicata. Si può ad esempio sapere se la coffee machine sta in quel momento erogando o meno il caffè, se è pronta per l'erogazione della bevanda, oppure se è giunto il momento di riempire nuovamente il contenitore dell'acqua. Si tratta, in altre parole, di un dispositivo decisamente carino, oltreché utile, il quale, tuttavia, può fornire ad un attacker l'opportunità di effettuare l'hijacking della password normalmente utilizzata per accedere alla vostra rete Wi-Fi locale.

Prima di procedere all'utilizzo, dovete ad ogni caso impostarlo. In pratica avviene questo: quando il dispositivo è collegato, esso crea un hotspot non criptato, ed ascolta il traffico UPNP. Lo smartphone sul quale è installata l'applicazione necessaria per comunicare con la macchina da caffé si collega a tale hotspot ed invia una richiesta UDP di trasmissione, chiedendo se, nell'ambito della rete, sono presenti dispositivi UPNP. Visto che la nostra coffee machine è proprio uno di tali dispositivi, essa risponde alla richiesta inoltrata. Successivamente, viene tra le altre cose inviata, dallo smartphone al dispositivo, una breve comunicazione contenente l'SSID e la password relativa alla rete wireless domestica.



È proprio qui che abbiamo rilevato il problema. Sebbene la password venga inviata in forma criptata, i componenti della chiave di cifratura vengono trasmessi attraverso un canale aperto, non protetto. Tali componenti sono, nello specifico, l'indirizzo Ethernet della macchina da caffè e varie altre credenziali uniche. Utilizzando questi componenti, viene generata, nello smartphone, la chiave di cifratura. La password relativa al network domestico viene codificata attraverso tale chiave, utilizzando il protocollo AES a 128 bit, per essere poi inviata sotto forma di base64 alla macchina per il caffè. La chiave in questione viene ugualmente generata nella coffee machine, utilizzando tali componenti; la password può essere così decifrata. La macchina da caffè si collega poi alla rete wireless domestica e cessa di essere un hotspot fino al momento del reset. Da questo momento in poi, la coffee machine risulta accessibile solo tramite la rete Wi-Fi domestica. Poco importa, tuttavia, visto che la password, in pratica, è già compromessa.

Stato attuale: la vulnerabilità è ancora presente

Comunicazioni intercorse con il vendor

Abbiamo provveduto a segnalare al vendor della macchina da caffè i risultati emersi dalla nostra ricerca; il produttore del dispositivo ha riconosciuto l'esistenza del problema da noi evidenziato, ed ha fornito la seguente dichiarazione:

«Sia la user experience, sia la sicurezza, sono elementi di estrema importanza, per noi; per quel che ci riguarda, ci sforziamo continuamente di trovare il giusto equilibrio tra i due fattori. Gli effettivi rischi associati alle vulnerabilità da voi menzionate riguardo alla fase di set-up del dispositivo sono estremamente bassi. Per ottenere l'accesso, un hacker dovrebbe trovarsi, fisicamente, entro il raggio di portata della rete domestica, nel momento stesso in cui viene effettuata l'impostazione, ovvero una finestra di tempo di solo pochi minuti. In altre parole, un hacker dovrebbe prendere di mira un utente specifico della macchina da caffè "intelligente", e trovarsi poi nelle immediate vicinanze del luogo esatto in cui viene eseguito il set-up; si tratta di circostanze altamente improbabili. Per tali motivi, non riteniamo che le potenziali vulnerabilità possano giustificare il notevole impatto negativo che tutto ciò avrebbe sulla user experience, qualora realizzassimo i cambiamenti suggeriti. Sebbene al momento non

siano previsti piani specifici riguardo alla modifica delle nostre procedure di set-up, rivalutiamo costantemente, da parte nostra, le scelte tecniche effettuate; non esiteremmo quindi ad apportare eventuali modifiche nel caso in cui i rischi divenissero più significativi. Se nell'immediato futuro dovesse cambiare qualcosa, vi terremo debitamente informati».

Non siamo completamente in disaccordo con la dichiarazione qui sopra riportata, e dobbiamo ammettere che la finestra utile per la conduzione dell'attacco risulta estremamente limitata. La vulnerabilità potrebbe essere corretta in vari modi; tuttavia, in base alle conclusioni tratte dalla nostra analisi, quasi tutte le possibili modalità individuate comporterebbero modifiche a livello di hardware (la porta Ethernet posta sulla macchina del caffè o una tastiera per l'inserimento della password risolverebbero il problema), oppure la fornitura di un codice PIN unico per ogni coffee machine, incluso quelle che sono state già vendute; si può comprendere come tale soluzione non si riveli semplice da realizzare dal punto di vista logistico. Simili cambiamenti avrebbero un impatto considerevole sull'esperienza d'uso, e la procedura di set-up diverrebbe più complessa.

L'unica soluzione software che possiamo proporre consiste nell'implementazione della crittografia asimmetrica. In tal caso, la macchina da caffè dovrebbe inviare la chiave di crittografia pubblica allo smartphone dell'utente; lo scambio di dati sensibili verrebbe così avviato soltanto una volta compiuta tale operazione. Questo, tuttavia, permetterebbe ancora a qualsiasi utente che si trovasse all'interno di una data rete Wi-Fi, incluso l'attaccante, di assumere il controllo della coffee machine. La chiave pubblica sarebbe in effetti disponibile per tutti; così, il primo utente che ricevesse la chiave e stabilisse, quindi, il collegamento con la macchina del caffè, sarebbe in grado di poter controllare quest'ultima. Il legittimo utente della coffee machine avrebbe, tuttavia, perlomeno un indizio riguardo al fatto che qualcosa non procede nella maniera giusta, visto che, nel corso di un attacco riuscito, egli non sarebbe in grado di comunicare con il dispositivo. Non è questo il caso del software attualmente eseguito sulla macchina da caffé.

Possiamo quindi affermare che comprendiamo, in qualche misura, la logica del produttore: il livello di rischio generato dal problema da noi segnalato non è pari al livello di complessità delle misure che dovrebbero essere implementate per eliminare il problema rilevato. Sarebbe inoltre sbagliato sostenere che il vendor non si è affatto preoccupato della sicurezza dei propri prodotti: come abbiamo detto in precedenza, la password viene trasmessa in forma protetta, e dovrebbero essere adottati accorgimenti particolari.

La vulnerabilità, ad ogni caso, esiste ancora, e per un cybercriminale abile ed esperto non sarebbe certo un problema sfruttare la stessa, allo scopo di carpire la password della vostra rete Wi-Fi. La situazione è interessante: l'utente di tale macchina da caffè, ogni volta che modifica la password della rete Wi-Fi domestica, allo scopo di rendere la stessa più sicura, "espone", in pratica, la nuova password, visto che, ogni volta che viene implementata una nuova password, deve essere nuovamente eseguita la procedura di set-up della coffee machine. E non si può di fatto sapere se qualcuno ha "sniffato" o meno la nuova password inserita. Per alcune persone, questo potrebbe non rivelarsi un problema; per altri utenti, invece, una simile circostanza può di sicuro rappresentare un evidente problema di sicurezza.

Per tale motivo, non riveleremo il nome del produttore, né il modello del dispositivo esaminato, in modo tale da non attirare attenzioni indesiderate sul prodotto vulnerabile. Tuttavia, qualora utilizziate una macchina da caffè controllata da smartphone, e siate preoccupati riguardo al problema da noi

segnalato, non esitate a contattare il vendor, chiedendo a quest'ultimo se ciò che abbiamo scoperto ha qualcosa a che fare con il prodotto che possedete, o intendete acquistare.

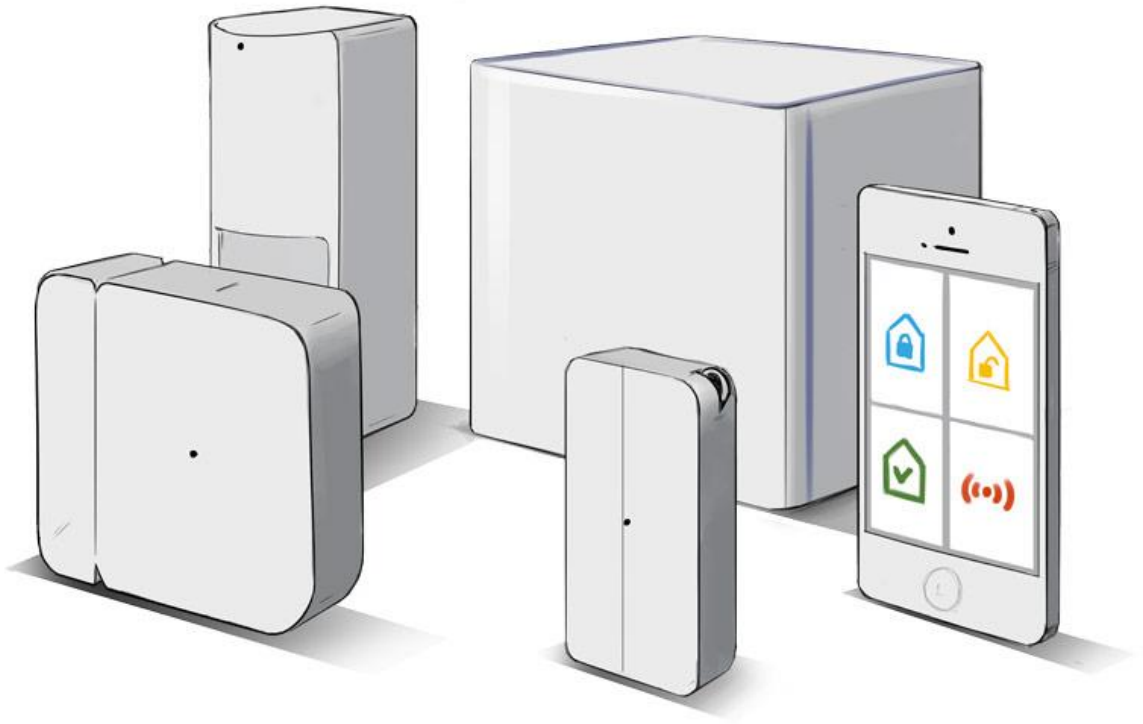
Passiamo, adesso, al capitolo conclusivo del nostro viaggio nel mondo insicuro dell'IoT.

Sistema di sicurezza domestico vs Fisica

Rischio: poter bypassare i sensori di sicurezza senza che scatti l'allarme

I sistemi di sicurezza domestica controllati tramite app stanno acquisendo una crescente popolarità. Sul mercato è già presente, di fatto, un considerevole numero di prodotti destinati a garantire la sicurezza delle vostre abitazioni nei confronti di eventuali intrusioni fisiche da parte di malintenzionati. Tali sistemi comprendono, di solito, un hub centrale collegato alla vostra rete domestica e al vostro smartphone, così come una serie di sensori alimentati a batteria, i quali comunicano in modalità wireless con il suddetto hub. I sensori utilizzati, abitualmente, sono costituiti da sensori di contatto per porte e finestre, preposti a rilevare l'eventuale apertura della finestra o della porta da essi sorvegliata, e ad informare quindi, all'istante, il proprietario dell'abitazione; sensori di movimento, telecamere.

Quando, inizialmente, abbiamo "messo le mani" su un sistema smart di sicurezza domestica, eravamo davvero entusiasti. Avevamo in effetti raccolto, in precedenza, tutta una serie di notizie relative alla scoperta, da parte di vari ricercatori, di gravi vulnerabilità in tali prodotti; citiamo, a tal proposito, l'interessante indagine effettuata da HP, oppure la dettagliata ricerca, presentata alla conferenza Black Hat svoltasi nell'anno in corso, riguardo all'insufficiente livello di sicurezza del protocollo ZigBee, utilizzato dai prodotti in questione. Ci eravamo quindi preparati a svolgere un facile lavoro, che avrebbe permesso di individuare numerose problematiche di sicurezza.



In realtà, non è stato affatto così. Quanto più abbiamo esaminato a fondo il sistema, tanto meglio abbiamo compreso che, dal punto di vista della cyber-sicurezza, si trattava di un dispositivo davvero ben progettato. Per impostare il sistema, occorre collegare l'hub centrale direttamente al router Wi-Fi, e per far sì che l'applicazione comunichi con l'hub, è necessario creare un account sul sito web del vendor, fornire il proprio numero di telefono ed inserire il codice PIN segreto trasmesso all'utente via SMS. Tutte le comunicazioni intercorrenti tra l'applicazione e il sistema di sicurezza vengono instradate tramite il servizio cloud del produttore; tutto quanto si svolge attraverso il protocollo https.

Esaminando la modalità con cui l'hub effettua il download di nuove versioni del firmware, abbiamo rilevato che il firmware risulta privo della relativa firma; si tratta di una prima circostanza problematica, in quanto essa consente, potenzialmente, di scaricare sul dispositivo qualsiasi firmware. Allo stesso tempo, per far questo, si dovrebbero conoscere la password e il login inerenti all'account dell'utente. Inoltre, quando ci troviamo sulla stessa rete utilizzata dal sistema di sicurezza risulta possibile inviare comandi all'hub, ma per capire quale genere di comandi possano essere inviati, si dovrebbe effettuare il reverse-engineering del firmware di cui è provvisto l'hub; si tratta, nella fattispecie, non proprio di una ricerca sulla sicurezza IT, ma di hacking aggressivo. E noi non siamo di certo hacker aggressivi.

Quindi, dal punto di vista del software – a meno che non si abbia intenzione di hackerare a tutti i costi un dispositivo – il sistema di sicurezza domestico oggetto della nostra analisi si è rivelato sicuro.

In seguito, però, abbiamo esaminato i sensori.

Avere la meglio sui sensori di contatto utilizzando le loro stesse armi

I sensori di intrusione, o di contatto, inclusi nella confezione, sono costituiti da tre parti principali: il magnete (la parte che viene collocata su una porta o sulla parte mobile di una finestra), il radiotrasmettitore ed il sensore di campo magnetico. Funzionano così: il magnete emette un campo magnetico, e il sensore di campo magnetico lo registra. Nel caso in cui la porta o la finestra venissero aperte, il sensore cesserà di registrare la presenza del campo magnetico, ed invierà una notifica all'hub centrale, indicando che la porta/finestra è aperta. Se, tuttavia, il campo magnetico risulta presente, non verrà trasmesso alcun allarme; questo significa, in pratica, che tutto ciò che occorre per bypassare il sensore è un semplice magnete, abbastanza potente da rimpiazzare il campo magnetico. Nel nostro laboratorio abbiamo posizionato un magnete nei pressi del sensore, poi abbiamo aperto la finestra, siamo entrati dentro, abbiamo chiuso la finestra e rimosso il magnete. Nessun allarme, e nessuna sorpresa.

Qualcuno potrebbe sostenere che tale "soluzione" funzioni esclusivamente con le finestre, visto che in tal caso si può essere abbastanza fortunati da poter localizzare facilmente il punto esatto in cui è posizionato il sensore. I campi magnetici, tuttavia, sono "infidi", e possono "camminare" attraverso le pareti; così, persino la più elementare app per smartphone adibita al rilevamento del campo magnetico sarà in grado di localizzare esattamente il sensore, anche in assenza di contatto visivo con lo stesso. Anche le porte, quindi (a meno che non siano metalliche), risultano ugualmente vulnerabili. Nella circostanza, vince la fisica!

Sensore di movimento

Incoraggiati dalla facile "vittoria" ottenuta sui sensori di contatto, siamo passati al sensore di movimento; abbiamo provveduto a smontarlo, ed abbiamo così scoperto che si trattava di un sensore a infrarossi piuttosto semplice, in grado di rilevare il movimento di un oggetto avente una certa temperatura. Questo significa che, se un oggetto non è abbastanza "caldo", il sensore non lo considera. Come abbiamo scoperto nel corso dell'esperimento da noi condotto, si rivelerebbe sufficiente, nell'occasione, indossare un cappotto, degli occhiali, un cappello e/o una maschera per divenire invisibili al sensore. Vince di nuovo la fisica!

Strategie di protezione

La cattiva notizia è che i dispositivi basati sui sensori di campo magnetico, e i sensori di movimento ad infrarossi di qualità non eccelsa, non vengono utilizzati esclusivamente dal sistema di sicurezza domestico da noi analizzato. Si tratta di sensori piuttosto standard, che possono essere reperiti in vari altri prodotti simili. È sufficiente ricercare i negozi online specializzati nella vendita di dispositivi IoT, per rendersene conto in prima persona. L'ulteriore cattiva notizia è che risulta impossibile risolvere il problema con un semplice aggiornamento del firmware. Il problema, in effetti, risiede nella tecnologia stessa.

La buona notizia, ad ogni caso, è che possiamo comunque proteggerci anche nei confronti dei ladri di appartamento che non hanno marinato le lezioni di fisica, a scuola. Le regole essenziali sono le seguenti:

1. Non fate esclusivamente affidamento sui sensori di contatto, per proteggere la vostra abitazione, se utilizzate un sistema del tipo qui sopra descritto. I produttori di sistemi smart per la sicurezza domestica offrono, di solito, dispositivi supplementari, quali, ad esempio, telecamere in grado di rilevare rumori e movimenti, che non possono essere di certo bypassate con semplici magneti. Sarebbe pertanto saggio e prudente abbinare ai sensori di contatto alcune telecamere "intelligenti", anche se in tal modo possono aumentare i costi. Utilizzare solo i sensori di contatto trasforma, in pratica, il vostro sistema di sicurezza domestico, per quanto high-tech, in un sistema di sicurezza "giocattolo".

2. Se utilizzate sensori di movimento ad infrarossi, cercate di posizionare gli stessi di fronte ad un radiatore, nelle stanze dove si presume possa transitare l'eventuale ladro, nel caso in cui quest'ultimo penetri all'interno della vostra abitazione. L'intruso, in questo caso, indipendentemente dai vestiti indossati, proietterà la propria "ombra" sul radiatore; il sensore rileverà così il cambiamento intervenuto, e provvederà a segnalare lo stesso al vostro smartphone.

Conclusioni

Sulla base di ciò che abbiamo scoperto nel corso del breve esperimento da noi condotto, possiamo senza'altro affermare che i vendor stiano realmente facendo del loro meglio per non far passare in secondo piano il tema della cyber-sicurezza, relativamente ai dispositivi da essi prodotti; questo, indubbiamente, è un elemento positivo. Tuttavia, qualsiasi dispositivo interconnesso, controllato tramite app, e abitualmente definito come "dispositivo IoT", presenta, quasi sicuramente, almeno un problema legato alla sicurezza. La probabilità che si tratti di una vulnerabilità critica, ad ogni caso, non è così elevata.

Allo stesso tempo, il basso livello di gravità di tali issue di sicurezza non garantisce affatto che le stesse non possano essere in qualche modo utilizzate, da malintenzionati, nel corso di un attacco. All'inizio del presente articolo abbiamo promesso di descrivere il modo attraverso il quale la vulnerabilità "rickrolling", in apparenza innocua e persino "buffa", potrebbe essere utilizzata nell'ambito di un pericoloso attacco informatico. È giunto il momento.

Immaginate, semplicemente, che un bel giorno, una TV equipaggiata con un dispositivo Chromecast, ad essa collegato - entrambi appartenenti ad un utente inesperto - inizi a mostrare continui messaggi di errore, attraverso i quali si comunica che, per risolvere il problema, l'utente deve necessariamente resettare il proprio router Wi-Fi, riportandolo alle impostazioni di fabbrica. Questo significa, in pratica, che l'utente dovrebbe poi ricollegare tutti i propri dispositivi, incluso la macchina del caffè controllata tramite la rete Wi-Fi. L'utente provvede quindi a resettare il router, e a ricollegare tutti i dispositivi che possiede. Una volta compiute tali operazioni, Chromecast torna a funzionare normalmente, così come tutti gli altri dispositivi presenti nel network domestico. Ciò di cui l'utente non si accorge è che qualcun altro, nel frattempo, si è collegato al router, per poi raggiungere la telecamera IP adibita a baby monitor, o altri dispositivi collegati in rete, proprio quelli che non presentano, di fatto, vulnerabilità particolarmente critiche, ma varie falle di sicurezza di minore entità.

Da un punto di vista strettamente “economico”, non risulta ancora evidente il motivo per cui i cybercriminali dovrebbero attaccare i dispositivi domestici interconnessi. Però, visto che il mercato dell’Internet delle Cose sta letteralmente decollando, e tali tecnologie divengono sempre più diffuse e standardizzate, è di sicuro solo una questione di tempo, prima che i cosiddetti “black hat” (gli hacker maligni) trovino il modo di monetizzare anche un attacco rivolto ai dispositivi IoT. Il ransomware, ovviamente, è una delle possibili “strade” che possono essere percorse dai malintenzionati, ma non certamente l'unica.

I cybercriminali, inoltre, non sono gli unici che potrebbero essere interessati al mondo dell'IoT. L'estate scorsa, ad esempio, il Ministero degli Affari Interni della Federazione Russa ha dato ordine di ricercare i possibili modi per effettuare la raccolta dei dati forensi provenienti dai dispositivi costruiti con l'utilizzo delle tecnologie intelligenti. Da parte sua, l'esercito canadese ha lanciato, di recente, una gara di appalto per reperire un fornitore in grado di "individuare vulnerabilità e misure di sicurezza" inerenti agli autoveicoli, e di "sviluppare e dimostrare le relative possibilità di sfruttamento di tali vulnerabilità tramite exploit".

Questo non significa che gli utenti debbano evitare l'utilizzo della tecnologia IoT, a causa di tutti i rischi ad essa collegati. La scelta più sicura è indubbiamente quella improntata alla saggezza e alla lungimiranza: occorre considerare bene quale dispositivo o sistema IoT si desidera, quale utilizzo si intende farne e in che luogo.

Riportiamo, qui di seguito, un elenco di suggerimenti in proposito da parte di Kaspersky Lab:

1. Prima di acquistare un dispositivo IoT, ricercare in Internet le notizie relative ad eventuali vulnerabilità che lo riguardino. L'Internet delle Cose è un tema molto caldo, attualmente, e un elevato numero di ricercatori sta svolgendo un lavoro davvero pregevole, volto ad individuare gli eventuali problemi di sicurezza presenti nei prodotti di questo tipo, dai baby monitor ai fucili controllati tramite app. È molto probabile che il dispositivo che si sta per acquistare sia stato già esaminato da ricercatori operanti nel campo della sicurezza IT; è quindi possibile scoprire se i problemi riscontrati nel dispositivo siano stati già debitamente corretti tramite apposita patch.

2. Non è sempre una buona idea acquistare gli ultimi prodotti lanciati sul mercato. Oltre ai bug standard che regolarmente accompagnano i nuovi prodotti, i dispositivi rilasciati più di recente potrebbero contenere issue di sicurezza che non sono state ancora scoperte dai ricercatori specializzati nell'IT security. La scelta migliore è quella di comprare prodotti per i quali sono stati già effettuati numerosi aggiornamenti a livello di software.

3. Al momento di scegliere quale parte della nostra vita si vuole rendere un po' più "smart", occorre prendere in considerazione i rischi legati alla sicurezza. Se la vostra abitazione è il luogo in cui custodite numerosi oggetti di valore, sarebbe probabilmente una buona idea scegliere un sistema di allarme professionale, che possa sostituire o integrare il sistema di allarme domestico già esistente, controllato tramite app; in alternativa, sarebbe di sicuro auspicabile impostare il sistema di sicurezza di cui già disponete in modo tale che qualsiasi potenziale vulnerabilità non possa comprometterne il funzionamento. Allo stesso modo, quando scegliete il dispositivo che raccoglierà informazioni sulla vostra vita personale e sulla vita degli altri componenti della vostra famiglia, ad esempio un baby monitor, la scelta più appropriata sarebbe forse quella di optare per il modello RF più semplice, in grado di trasmettere soltanto segnali audio, e non provvisto di connettività Internet. Se non avete modo di optare tra varie soluzioni, seguite allora il nostro primo consiglio: scegliete sempre in maniera saggia e responsabile!

Per quel che riguarda, infine, i produttori di dispositivi IoT, abbiamo solo un suggerimento da proporre, tuttavia importante: quello di collaborare con la community degli esperti di sicurezza IT, quando vengono creati i nuovi prodotti e si migliorano quelli già presenti sul mercato. Esistono, tra l'altro, speciali iniziative quali Builditsecure.ly, o il progetto OWASP dedicato all'Internet of Things, che potrebbero realmente fornire un valido aiuto per la costruzione di qualche favoloso dispositivo interconnesso, che non presenti serie problematiche di sicurezza. Kaspersky Lab, da parte sua, continuerà la propria ricerca, al fine di raccogliere ulteriori elementi ed informazioni riguardo ai

dispositivi IoT, e individuare, in tal modo, le migliori soluzioni per proteggere efficacemente gli utenti nei confronti delle minacce IT che possono derivare dall'utilizzo di tali dispositivi.