I pirati nelle case intelligenti

Oltre 750.000 email con virus in 15 giorni

Torni a casa e trovi le serrature bloccate. Oppure ti svegli di soprassalto perché la temperatura è scesa a livelli polari. Apri il frigo «intelligente » e il cibo è andato a male. Sono gli incubi dell'utente della *CASA DOMOTICA* ai quali viene da pensare leggendo un comunicato di Proofpoint, una società specializzata in sistemi di difesa da attacchi informatici, che annuncia la prima offensiva in grande stile degli «hacker» contro abitazioni dotate di elettrodomestici connessi ad Internet.

Dopo dieci anni di annunci la «casa domotica» comincia a diventare realtà: parliamo di uno degli affari del futuro super-tecnologico che attrae grandi Aziende come Cisco Systems, Google che ha appena speso 3,2 miliardi di dollari per acquisire Nest Labs (una società che produce termostati ultratecnologici) e Samsung che, al Ces, il Salone elettronico di Las Vegas, ha appena lanciato il suo progetto di «smart home» col quale punta a diventare leader mondiale degli elettrodomestici a partire dal frigorifero.

Ma appena l'«Internet delle cose» comincia ad affacciarsi, ecco spuntare, la minaccia degli «hacker». Scoperta, guarda caso, da chi ha tutto l'interesse ad alimentare questo business. Secondo Proofpoint nei giorni che vanno dal 23 dicembre al 6 gennaio scorsi più di 500.000 email contenenti virus sono state inviate a tantissimi elettrodomestici intelligenti, collegati via web. Attacchi difficili da contrastare perché nessun indirizzo IP è stato usato per lanciare più di godi questi messaggi distruttivi. Dove? In tutto il mondo.

La notizia è stata ripresa da molti siti tecnologici Usa e dal Financial Times il quale afferma che i suoi tecnici non sono riusciti a verificarne la fondatezza. Ma che quello degli «hacker» sia un incubo destinato a incombere sul nuovo mondo della domotica è sicuramente vero ed è

riconosciuto anche dai grandi gruppi che si contendono questo nuovo mercato.

«La "casa domotica" è particolarmente vulnerabile agli attacchi dei criminali cibernetici perché chi fa sistemi digitali per la casa non ha le stesse preoccupazioni di sicurezza di chi disegna servizi per le imprese. E un'azienda investe più di un individuo in tecnologie di protezione » dice l'«hacker pentito» Kevin Mitnick, che dopo due condanne e sei anni di galera e diventato uno dei più accreditati imprenditori dei sistemi di sicurezza informatica. O, meglio, sono cose che Mitnick va dicendo da anni, visto che la frase è tratta da una sua intervista al New York Times del 2oo6.

Il vero cambiamento degli ultimi anni è che davanti ai criminali cibernetici si sono aperte nuove praterie grazie a due innovazioni:

la moltiplicazione degli «smartphone» coi quali ci si può collegare a Internet e la rapida diffusione di sensori a basso costo che consentono di rendere «intelligente» e controllare a distanza quasi tutto, dalla guida di un'auto al ritmo cardiaco.

«Gli attacchi criminali in rete l'anno scorso sono cresciuti del 14% raggiungendo livelli mai visti prima» dicono gli analisti di Cisco Systems. E l'allarme che ora si diffonde sulla domotica non è, di certo, la preoccupazione maggiore. Più ancora di quelli alla casa, preoccupano (a parte i rischi di sabotaggio a scopo militare), la possibilità che vengano attaccati i sistemi di guida di aerei in volo o protesi e congegni medici dotati di sensori. *Anche se con le attuali conoscenze risulterebbe impossibile mettersi al comando di un aereo, come da alcuni millantato, in quanto c'è sempre il pilota a bordo ed il pilota automatico non si può comandare da terra, si potrebbe più facilmente sostituirsi alla torre di controllo per interferire con le comunicazioni inviate ai piloti, come in un famoso film di Bruce Willis.*

Ancora una volta l'allarme è partito proprio dal mondo degli esperti di cybercrimine durante «Black Hat», una conferenza sulla sicurezza che si tiene ogni anno negli Usa, e a Def Con, un raduno di hacker. Due anni fa a una di queste conferenze Jerome Radcliffe, un esperto di sicurezza, dimostrò come fosse possibile alterare da lontano il funzionamento della pompa dell'insulina di un diabetico e modificare la quantità di medicinale somministrato. Alcuni mesi fa un altro ricercatore, Barnaby Jack, annunciò di aver trovato il modo di bloccare i «pacemaker» dei cardiopatici e di sapere come provocare a distanza fibrillazioni mortali.

Per i gruppi che, non trovando sufficienti fonti di reddito nei business della gestione delle informazioni e della pubblicità in rete, cercano di sviluppare altri ricchi business nel nuovo mondo della domotica, il significato di tutto ciò è evidente: dovranno investire molto più in sicurezza se vorranno raggiungere un livello di affidabilità tale da scongiurare il rischio di crisi di rigetto degli utenti.

Un problema che riguarda soprattutto Google, vulnerabile non solo nel suo nuovo investimento nella domotica, ma anche negli occhiali digitali che, ancora in fase sperimentale, sono già stati attaccati dagli «hacker». E c'è da giurare che qualcuno starà già pensando a come alterare il funzionamento delle ancor più nuove (e sperimentali) lenti a contatto di Google per misurare i livelli di insulina nei diabetici.