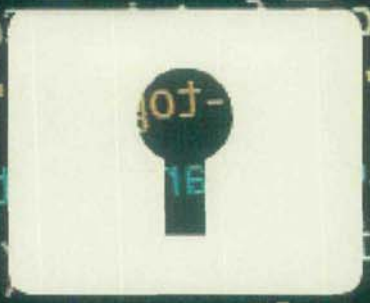
MERCATI E BUSINESS

CYBER SECURITY

# In difesa del corpo digitale

**Come ha di recente mostrato Vault 7, l'operazione di spionaggio orchestrata dalla Cia, è la domotica la nuova porta per entrare nelle case e nella privacy delle persone. Argomento che andrà affrontato dai legislatori**

DI GLORIA VALDONIO



Chi non ha più vent'anni, potrà ricordare il caso Echelon, un'intercettazione telematica di massa nelle reti infrastrutturali (allora erano i cavi sottomarini) allo scopo di sottrarre tutti i pacchetti di dati che viaggiavano da una sponda all'altra dell'Atlantico, emersa a metà degli anni Novanta. Chi invece vent'anni non ce li ha ancora, potrà ricordare il Datagate, ovvero l'attività di sorveglianza di massa denunciata da **Eduard Snowden** e compiuta dal 2001 fino almeno al 2011 dall'Nsa (l'agenzia per la sicurezza degli Stati Uniti) nei confronti dei cittadini statunitensi e stranieri. A firmare l'ultimo attacco di cyber spionaggio, nome in codice Vault 7, è invece la Cia, e a rivelarlo è stato qualche settimana fa Wikileaks, l'organizzazione di **Julian Assange**.

Vault 7 è un sistema di intercettazione attraverso l'installazione di malware (come vengono chiamati i software cattivi) nei vari device. La Cia, come è emerso, possiede strumenti per violare smartphone Android e iOS, per penetrare la cifratura delle conversazioni protette dai protocolli di tutti i messenger più diffusi (Signal, Telegram, Whatsapp, Wiebo e molti altri), è in grado di ascoltare le conversazioni che vengono svolte davanti a una smart tv con un microfono montato, e manovrare tramite satellitare anche le auto senza lasciare traccia dell'irruzione. «Il caso Echelon è legato a un momento storico differente che aveva come obiettivo il controllo massivo attraverso il prelievo indiscriminato di dati», dice **Giuseppe Vaciago**, partner dello studio R&P Legal. «Invece Vault 7, permette di colpire, attraverso lo strumento infettato, il singolo utente per appropriarsi delle sue informazioni, o meglio del suo corpo digitale».

CYBER CIA
Secondo i documenti diffusi da Wikilieaks, la Cia è in grado di violare tutti i messenger più diffusi

**Lo spionaggio 2.0** Secondo l'esperto è lo spionaggio del nuovo millennio, né più né meno quello che si è sempre fatto dalla nascita delle nazioni, e anche prima, e che internet ha reso però molto più potente e invasivo rendendo possibile la creazione di una rete di intelligence che può scivolare in

centinaia e migliaia di device contemporaneamente. Ovviamente il confine tra l'attività di intelligence e la sorveglianza indiscriminata o la violazione della privacy è labile. E nell'attesa che l'argomento venga affrontato dai legislatori, il web è una prateria da esplorare per chiunque sia alla ricerca di informazioni personali. Una prateria il cui ingresso è favorito dal crescente numero di "porte": non più solo smartphome e computer, ma anche smart tv, occhiali di realtà aumentata come i google glass, sistemi intelligenti di videosorveglianza, braccialetti per il fittness, orologi, autovetture intelligenti e tutti gli oggetti della domotica.

«Parliamo almeno di 50 miliardi di device che circoleranno entro il 2020», dice l'avvocato **Stefano Mele**, specializzato in diritto delle tecnologie, privacy, sicurezza delle informazioni e intelligence, nonché of counsel di Carnelutti Studio Legale Associato. «Stiamo parlando di oggetti di uso comune che saranno sempre più intelligenti e interconnessi, ma sui quali i produttori non hanno inserito strumenti di sicurezza informatica per contenere i costi».

Insomma per quanto riguarda la sicurezza ormai nessun oggetto, anche di uso domestico, può considerarsi innocuo, se interconnesso. L'ambito della domotica è forse quello meno analizzato, ma anche il più insidioso a causa delle previsioni di crescita del settore: tra assistenti digitali, robot ed elettrodomestici intelligenti, il giro d'affari della smart home è destinato a toccare quota 72,2 miliardi nel 2021 rispetto ai 16,8 miliardi del 2016, con una crescita media annua del 36,4%. Il mercato principale è quello statunitense, ma la Cina segnerà la migliore performance poiché il numero delle case connesse sta crescendo a un ritmo del 56% l'anno. Quanto all'Europa, sempre nel 2021, si ipotizza che ci saranno 26,8 milioni di case connesse e un giro d'affari di 6,6 miliardi di dollari.

## Il corpo digitale

Sempre più facile quindi ferire il nostro "corpo digitale", fatto di dati, immagini, suoni. Attraverso l'arma del captatore è possibile rubare le identità, accedere alle informazioni confidenziali, acquisire le credenziali bancarie, effettuare acquisti on line con l'account della vittima inconsapevole. Se partiamo dalle premessa che questo strumento sia, di fatto, un'arma, è necessario interrogarci su tre distinti ordini di problemi: il livello di sicurezza con cui tali software vengono conservati; l'esportabilità e la produzione di tali strumenti; la valutazione se le pene previste per chi opera illecitamente nel mercato dei malware siano adeguati.

**50 MILIARDI DI RISCHI**
Stefano Mele, of counsel di Carnelutti, spiega «che entro il 2020 circoleranno almeno 50 miliardi di device interconnessi»

«La sicurezza ha un costo, ma è anche complessa per l'utente finale che in genere non ha voglia di perdere tempo per configurare un telefonino, figuriamoci un oggetto intelligente», dice Vaciago. Che aggiunge: «Manca una cultura della sicurezza. Ma così come introduciamo antivirus nei nostri pc, lo stesso comportamento deve essere tenuto per esempio nei confronti dei nostri cellulari, che sono computer molto più potenti e oltretutto oggetti ancora più personali». «Se non approfondiamo subito il tema della sicurezza, acquisteremo oggetti intelligenti che somiglieranno a veicoli senza fari, senza freni e senza cinture», aggiunge Mele.

## Email oscure e spazio alla poesia

Ma esiste qualche semplice trucco per difendersi da questo controllo e invasione della privacy? Il più importante è senza dubbio il controllo attento di tutte le email, anche quelle che provengono da soggetti conosciuti, perché basta aprire un messaggio infettato per lasciare campo libero al virus di impadronirsi di tutto il terminale e permettergli di trasformarlo anche in una telecamera. «L'email è il veicolo principale per infettare qualsiasi sistema», conferma Vaciago. Il secondo accorgimento è aggiornare frequentemente tutti i sistemi applicativi. Infine, il capitolo password, che sono importantissime. Per tutelare la privacy non è più possibile utilizzare codici alfanumerici (tanto meno quelli delle date di nascita di mogli, figli e fratelli), ma è necessario inserire codici complessi. Un suggerimento è quello di trascrivere le consonanti della propria canzone o poesia preferita inserendo qua e là alcuni numeri. Un esempio (da non copiare) è il seguente: «Nel mezzo del cammin di nostra vita…» che diventa nmzzcmmn, che potrebbe trasformarsi nel codice nmz2zcm333n aggiungendo qualche cifra. ♦

**ATTENTI ALLA MAIL**
Giuseppe Vaciago, partner dello studio R&P Legal, ricorda che «l'email è il veicolo principale per infettare qualsiasi sistema»