La nostra vita è digitale

Navigare in rete è come passeggiare lungo una strada, dove legalità e crimine si confondono. Come muoverci?

di **Biagio Simonetta**

La digitalizzazione ha portato con sé un dono del quale si farebbe volentieri a meno: il rischio concreto che i nostri dati possano essere trafugati in qualunque istante. E fate attenzione, perché questo argomento è tutt'altro che banale. Navigare su internet è sempre più uguale a passeggiare lungo una strada. Una strada infinita, che incrocia i salotti buoni dei boulevard parigini e i vicoli bui delle favelas di Rio. Una strada lungo la quale legalità e crimine si mescolano, si confondono, diventano la stessa cosa. C'è un malvivente dietro a ogni angolo pronto a rubarti la borsa se non la apri con cautela. Il mouse è allo stesso tempo il tuo killer e il tuo scudo. Il pericolo è ovunque, non c'è un luogo più sicuro di un altro. Ed è costante. Perché la vita virtuale non ha fasce orarie, per i borseggiatori del web giorno e notte sono la stessa cosa.

Le regole del web non seguono quelle della vita reale. Ogni volta che apriamo una mail, ogni volta che accediamo al nostro conto corrente online, ogni volta che acquistiamo qualcosa su internet con la nostra carta di credito, da qualche parte nel mondo c'è qualcuno pronto a rubare la nostra identità, il nostro denaro. Qualcuno nascosto chissà dove, magari in qualche stanza buia e umida, dall'altra parte dell'oceano. Oppure in qualche lussuosa suite di un hotel russo. Qualcuno che non vedremo mai in faccia, ma che magari userà la nostra, di faccia, per fare transazioni bancarie, noleggio di automobili, prenotazioni di camere d'alberghi. Qualcuno che è pronto a spendere 10mila euro in una puntata di poker online, perché quei 10mila euro li ha presi dal nostro conto, dove li avevamo conservati per comperare la macchina nuova. Qualcuno che ruba la nostra identità e quella di migliaia di altri cittadini perché i nostri dati sono un pacchetto facilmente vendi-

Digitalizzazione. Dal tablet è possibile gestire elettrodomestici, illuminazione, sistema d'allarme e tapparelle

bile ad acquirenti con disponibilità economiche importanti, disposti a pagare cifre ingenti: le organizzazioni criminali. Come nella vita reale, o forse anche più che nella vita reale, il crimine 2.0 attraversa ogni classe sociale. Dal grande istituto bancario al comune cittadino: ognuno è una potenziale vittima. Dipende dalle competenze del cracker, dalla sua smania di danaro, dall'organizzazione per la quale lavora. Il colpo può valere pochi euro, o qualche milione. È il totale ciò che importa. E il totale dice che intorno al cybercrimine ruota un giro d'affari mostruoso. Addirittura maggiore rispetto a quello che ruota attorno al traffico di droga.

In casa

Il web ha dato la possibilità ai criminali di raggiungere le loro vittime ovunque. Anche a casa. Come? Per esempio attraverso le smart Tv. Alzi la mano chi, acquistando al centro commerciale un televisore di ultima generazione, ha pensato solo per un attimo che quell'oggetto possa essere fonte di un attacco informatico. Eppure proprio la smart tv ha catalizzato, negli ultimi mesi, l'attenzione dei maggiori produttori di antivirus. Perché una smart tv è connessa in rete, e soprattutto, ha una webcam. E pensare che un hacker, davanti al suo pc in chissà quale posto del mondo, possa entrare nel vostro salotto, o nella vostra camera da letto, attraverso il televisore, non è fantascienza. Anzi, è un rischio concreto.

Oggi è lecito pensare che sin dal prossimo televisore che compreremo, le possibilità che questo sia smart sono altissime. Se fino a qualche mese fa acquistare una tv 2.0 voleva dire fare un investimento abbastanza importante, oggi i prezzi sono calati notevolmente, tanto da risucchiare le tv tradizionali. Una smart tv è qualcosa di molto simile a uno smartphone. Ha un sistema operativo e ogni cosa funziona con delle App.

?

LA DOMANDA

Qual è il malware che ha colpito di più nel 2017?

—

Ransomware, con più di 11 milioni di account italiani in vendita nel Dark Web

3.962
Milioni

Gli euro spesi dagli italiani nel 2017 per acquisti online di prodotti elettronici e informatici

Molte di queste App hanno un legame diretto con la nostra carta di credito (come Netflix, per citarne una). Attualmente i sistemi sono molto vulnerabili, e sono un invito abbastanza goloso per qualsiasi pirata informatico. E poi c'è il rischio delle webcam, del quale dicevamo prima. Rischio che secondo Eugene Kaspersky non sottovaluta affatto: «La possibilità che un hacker ci guardi mentre siamo nel nostro salotto mentre vediamo la Tv esiste, e negli ultimi anni vari esperti di sicurezza hanno dimostrato la possibilità di attacchi di questo tipo. Tuttavia, finora non abbiamo registrato casi del genere. Ma temo che sia solo una questione di tempo. Non appena i criminali vedranno interesse finanziario nel farlo, diventerà realtà».

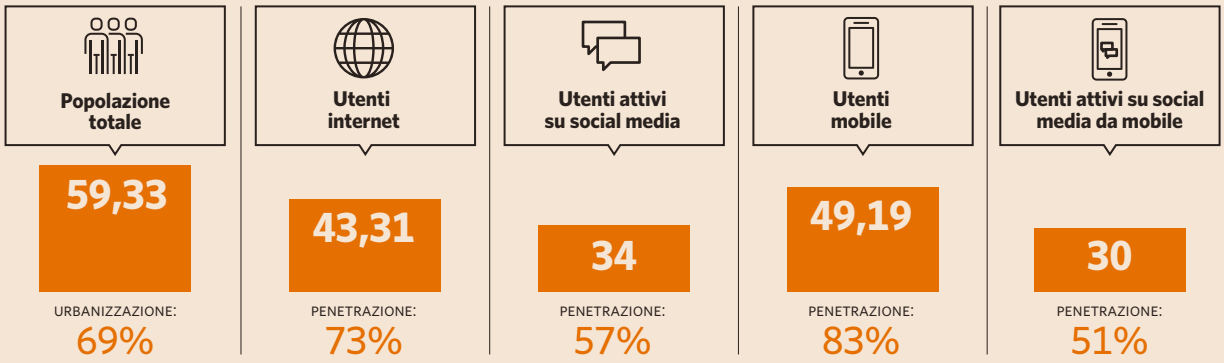
Altro capitolo interessante riguarda tutta la domotica che sempre più spesso gestisce la nostra casa: dall'impianto di riscaldamento a quello di illuminazione e tanto altro ancora. È ormai risaputo che i cyber criminali stiano puntando anche su questo tipo di oggetti. Se da una parte può essere comodo con un semplice click, a distanza, avviare il ciclo di lavaggio di una lavatrice o controllare il consumo energetico di un frigorifero, ma anche gli alimenti da comprare grazie a un sms, essendo manovrati da remoto, quando non si è in casa, questi dispositivi sono destinati a offrire nuove idee ai cybercriminali su come e quando svaligiare un'abitazione.Occhio anche all'elettronica a bordo dell'auto. Se un tempo al massimo si rubava l'autoradio o la targa, ora gli attacchi wireless possono agire su vari componenti e funzioni del veicolo. Uno studio presentato all'ultimo DefCon (la più grande convention in materia) ha evidenziato come sia possibile per un hacker, oltre a infettare l'auto con un virus, addirittura azionare improvvisamente i freni a una velocità di 128 chilometri orari, far vibrare il volante, accelerare i giri del motore e persino inibire l'uso dei freni quando l'auto viaggia a bassa velocità.

A scuola

E se vi dicessero che le intrusioni informatiche possono colpire anche la scuola? È proprio così. Con la diffusione delle nuove tecnologie nelle scuole aumentano anche i rischi per la sicurezza. Negli Usa i pirati del web hanno addirittura un tariffario per alterare voti e assenze. E l'Italia si mostra particolarmente vulnerabile a eventuali attacchi. Cinquecento dollari: è questa la cifra che basta per falsificare un test scolastico negli Stati Uniti. Come? Grazie a internet e alle mani esperte di un hacker assoldato per l'occasione. Perché nell'era del web diffuso che controlla le nostre vite – scuola compresa – i pirati informatici si mettono sul mercato, al servizio di studenti che non hanno voglia di studiare o che cercano di mostrare le falle nella sicurezza di un sistema scolastico, come quello Usa, sempre più dipendente dalle tecnologie. Basti pensare che, oltreoceano, quasi tutti gli esami (a ogni livello d'istruzione) si svolgono con computer connessi in rete e che i registri elettronici sono una realtà consolidata da molti anni. Questa storia l'ha segnalata il sito Skuola.net,

La diffusione del digitale

Uno snapshot degli indicatori statistici primari relativi all'Italia. Dati gennaio 2018 in milioni di utenti



FONTE: Hootsuite

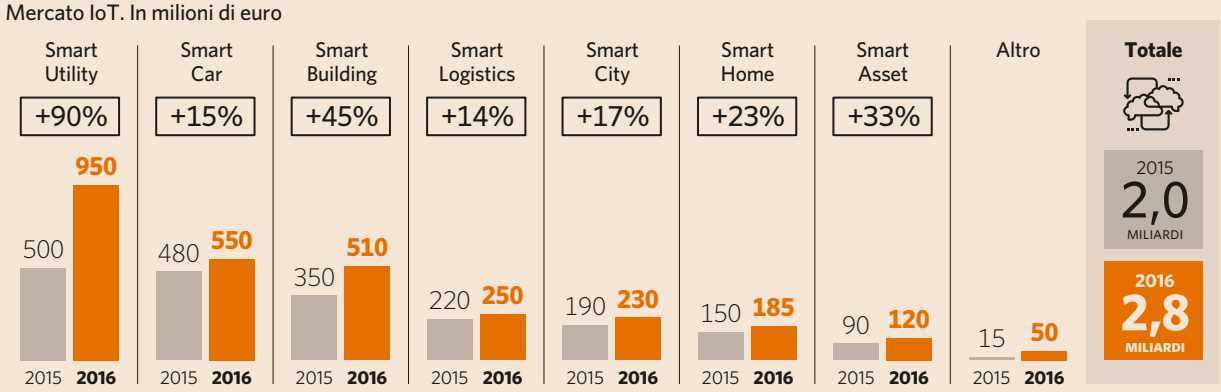
che ha raccontato come decine di hacker, hanno colto la palla al balzo per arricchirsi alle spalle degli "asini 2.0". Un tempo, infatti, si doveva ricorrere agli stratagemmi più assurdi per saltare un compito in classe (allagamenti nelle scuole, invasioni di insetti, telefonate minatorie e chi più ne ha più ne metta); oggi, basta farsi un giro del Deepweb (o Darknet) - quella parte nascosta di internet che presta il fianco ai traffici più loschi – per essere accontentati. Senza esporsi in prima persona.

In ospedale

Per quanto riguarda la nostra salute, il capitolo dei cyber attacchi è decisamente inquietante. E per capirlo partiamo da un esempio che riguarda gli oltre 745mila pacemaker teoricamente a rischio hacker per un "bug" nel software che potrebbe essere sfruttato da malintenzionati. Lo afferma la casa produttrice, che ha invitato i pazienti a far aggiornare il firmware, il "sistema operativo" dei dispositivi. L'allarme è stato rilanciato qualche tempo fa negli Usa dall'Fda, e riguarda i pacemaker prodotti da San Jude Medical, recentemente acquisita dalla multinazionale Abbott. I dispositivi sono in grado di comunicare con l'esterno tramite wifi per regolare alcune funzioni, ma questa possibilità sarebbe teoricamente sfruttabile da malintenzionati per inserirsi nel sistema e provocare malfunzionamenti, anche se nella pratica non è ancora mai stato descritto nessun caso. Per mettere una "toppa" la casa produttrice ha pubblicato un aggiornamento del firmware che può essere installato in tre minuti, invitando i pazienti a richiederlo alla prossima visita di controllo. «I dispositivi connessi stanno avendo un impatto significativamente positivo sui pazienti e la loro salute - afferma Robert Ford, vicepresidente Abbott -. Per proteggere i nostri pazienti abbiamo sviluppato il nuovo firmware.

L'evoluzione dell'Internet delle cose

Mercato IoT. In milioni di euro



FONTE: Osservatori.net

Secondo un rapporto del Department of Homeland Security statunitense riuscire a compromettere la sicurezza di questi dispositivi richiede una complessa serie di circostanze».

In ufficio

Infine parliamo del pericolo che i nostri dati vengano trafugati quando siamo in ufficio. Durante l'orario lavorativo, solitamente, ci sentiamo più protetti da questo punto di vista. Anche perché in genere utilizziamo macchine (nel senso di computer, tablet o altro) aziendali, dunque non di nostra proprietà. Tuttavia, nonostante l'hardware non sia nostro, il pericolo di contrarre danni che ci riguardino da vicino è altissimo. Non dobbiamo dimenticare, infatti, che sui computer dell'ufficio accediamo ai nostri account mail e social. Dunque apriamo il nostro mondo alla rete aziendale che, ironia della sorte, è molto spesso più soggetta ad aggressioni cyber rispetto a quella domestica. C'è da aggiungere, poi, una considerazione molto importante, che il team di Kaspersky Lab sostiene da sempre: per la maggior parte di noi, la giornata lavorativa inizia accendendo il computer. Ma pochi si rendono conto che una mossa informatica sbagliata può mettere a rischio un'intera carriera professionale. La maggior parte delle volte è la distrazione o la disattenzione a giocarci un tiro mancino. Nonostante i dipendenti di un'azienda debbano firmare una seria politica di sicurezza al momento dell'assunzione, molto spesso queste regole non vengono seguite o prese in considerazione, mettendo da parte le possibili conseguenze che questa scelta potrebbe portare. Conseguenze che, come detto, vanno ben al d€
i là dei nostri dati, e rischiano di compromettere il lavoro dei nostri colleghi. Parola d'ordine, dunque, massima attenzione.

© RIPRODUZIONE RISERVATA

?

LA DOMANDA

Quali sono i principali vettori degli attacchi malware?

—

Office (61%), Script (23%), Executable (14%), Archive (1%), Pdf (1%)