REGOLE PER BATTERE I VIRUS AL RISTORANTE NIENTE FOTO

I nuovi malware con l'intelligenza artificiale scoprono i dati personali dai post sui social network. E il ricatto non è più «Paga» ma: «Infetta due amici». Ecco come difendersi

di **Umberto Torelli**

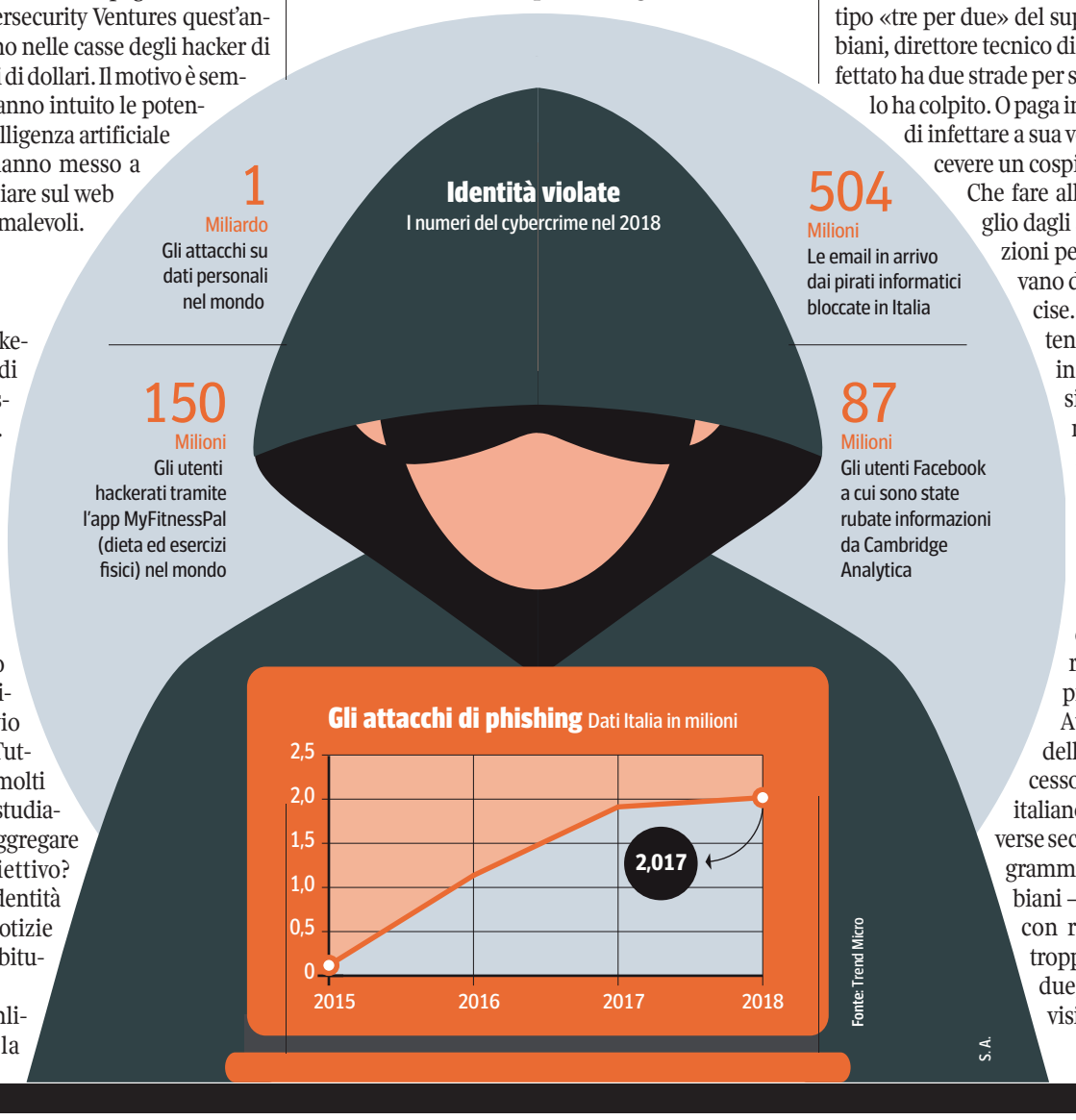
Quattro miliardi e 134 milioni. È il numero aggiornato degli utenti web secondo Internet Live Stat, il sito di sviluppatori internazionali che monitora ogni giorno la Rete. Ebbene, nel corso del 2018 un utente di Internet su quattro ha subito un attacco ai propri dati personali. Sono stati colpiti tutti: singoli cittadini, istituzioni, piccole e grandi imprese (fonte, Ermes Cyber Security). E le previsioni per il 2019 dicono che il fenomeno è in aumento. Check Point Software, azienda israeliana specializzata in sicurezza informatica, ha individuato per il 2019 nuove forme di ransomware, i virus che rendono inaccessibili i dati del computer e chiedono il pagamento di un riscatto. E secondo Cybersecurity Ventures quest'anno gli attacchi porteranno nelle casse degli hacker di tutto il mondo 11 miliardi di dollari. Il motivo è semplice: i cybercriminali hanno intuito le potenzialità dei sistemi di intelligenza artificiale (Ai). Di conseguenza, hanno messo a punto app per sguinzagliare sul web gli «agenti intelligenti» malevoli.

Le tracce

Ne è un esempio l'hackeraggio di 773 milioni di email e 21 milioni di password di Collection #1. Definito come il più grande furto di dati personali della storia, è stato scoperto nei giorni scorsi dal ricercatore informatico Troy Hunt. Sono informazioni private raccolte nel corso degli anni e immagazzinate in un mega archivio digitale di 87 Gigabyte. Tutto questo si aggiunge ai molti programmi di phishing studiati per catturare prima e aggregare poi i nostri dati. L'obiettivo? Tracciare i profili delle identità digitali, con tanto di notizie personali sulle nostre abitudini.

È proprio «la pesca online» di informazioni la nuova insidia 2019 per i 43 milioni di utenti italiani del web (dati We Are Social). Tante le fonti da cui attingono informazioni i pirati, tracce seminate durante la navigazione sul web da utenti spesso ignari, a volte semplicemente distratti o poco consapevoli. Quali? «Le credenziali bancarie, i programmi fidelity sottoscritti durante gli acquisti, gli accumuli di miglia aeree e le raccolte premi — elenca Gastone Nencini, responsabile della società di analisi di mercato Trend Micro Italia —, ma anche le recensioni di ristoranti e le risposte ai sondaggi sui social».

Siamo a rischio dunque se postiamo con leggerezza foto e informazioni sui piatti mangiati al ristorante con gli amici. Così lo scorso anno sono caduti nella trappola degli hacker oltre due milioni di italiani. È come nella storia di Pollicino, che lasciava sassolini nel bosco per ritrovare la strada. Noi invece lasciamo tracce della nostra identità digitale, che poi i pirati del web rivendono online per pochi dollari, o usano per operazioni fraudolente.



Le catene

Adesso i ricatti per sbloccare computer e file infetti non si esprimono soltanto con richieste di denaro. Stiamo assistendo a forme di marketing maligno del tipo «tre per due» del supermercato. Dice David Gubiani, direttore tecnico di Check Point: «Chi viene infettato ha due strade per sbloccare il ransomware che lo ha colpito. O paga in bitcoin o riceve la richiesta di infettare a sua volta due nuovi utenti per ricevere un cospicuo sconto».

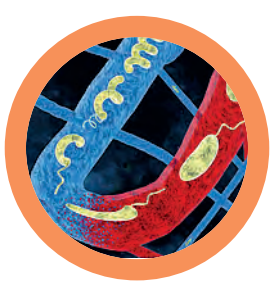
Che fare allora per proteggerci al meglio dagli attacchi sul web? Le indicazioni per privati e aziende che arrivano dai cyberpoliziotti sono precise. Primo, prestare grande attenzione ai dati che postiamo in Rete e sui social. Quelli sensibili vanno inseriti soltanto nei siti sicuri, meno che mai nei link diretti ricevuti via mail da sconosciuti. Secondo, tenere sempre aggiornati gli antivirus e i sistemi operativi. Terzo, in caso di gravi attacchi formattare computer e telefonini, ricaricando i file di lavoro da precedenti backup.

Attenzione anche sul fronte delle password, le porte di accesso ai nostri dati. «Soltanto un italiano su dieci usa password diverse secondo le applicazioni e i programmi installati — conclude Gubiani — e meno del 5 % le cambia con regolarità». Gli altri? Purtroppo digitano sempre le stesse due, aumentando il rischio di visite dei pirati informatici.

Metropolis

Invece della pillola, inghiotti un micro-robot

Micro-robot biocompatibili ed elastici, progettati per muoversi nel corpo umano e somministrare farmaci in zone mirate. È il progetto della Scuola Politecnica Federale di Losanna. Con i colleghi del Politecnico di Zurigo, i ricercatori hanno sviluppato piccolissimi meccanismi, ispirati ai batteri, che possono essere ingoiati o iniettati. Fatti in idrogel contenente nanoparticelle magnetiche, grazie a un'intelligenza artificiale integrata, i robot riescono ad adattare la propria forma all'ambiente che li ospita, scegliendola autonomamente, per muoversi lungo tutti i tessuti, anche attraverso i vasi sanguigni più stretti e gli organi più vischiosi. E raggiungere così l'obbiettivo senza perdere velocità. I minuscoli robot possono essere programmati in anticipo e controllati poi, utilizzando un campo magnetico. Sarebbero facili da produrre e convenienti.



Qui Losanna
I micro meccanismi inventati in Svizzera: da ingoiare o iniettare, sono in idrogel e somministrano farmaci dove serve

Com'è pulita la CO2

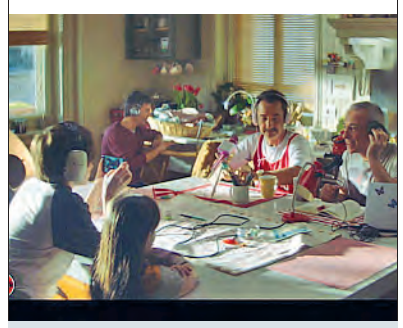
Trasformare le emissioni di anidride carbonica in energia pulita. È la missione dell'Istituto nazionale di scienza e tecnologia di Ulsan, Corea del Sud. Qui hanno creato un nuovo sistema, Hybrid Na-CO_2, che combina sodio e anidride carbonica per ottenere elettricità e idrogeno, grazie a una reazione elettrochimica. Il sistema si presenta come una sorta di una pila a combustibile, in cui il la parte liquida è l'acqua, mentre il catodo è il sodio. Sono poi presenti un anodo e un separatore. Introdotta nell'acqua l'anidride carbonica, si avvia una reazione per cui la Co_2 viene totalmente eliminata, mentre si ottiene H_2 ed energia elettrica. I test hanno dimostrato che l'efficienza di conversione dell'anidride carbonica in nuova energia è del 50% e che il nuovo sistema ha abbastanza stabilità per funzionare oltre mille ore senza danni agli elettrodi.

Cristina Pellecchia

Pit Spot

Se Vodafone entra in casa con Linus

a cura di **Aldo Grasso**
pitspotcorriere@gmail.com
in collaborazione con
Massimo Scaglioni



Cosa non si riesce a fare con la fibra ultra-veloce. Addirittura è possibile ricostruire uno studio radiofonico per allestire, all'ultimo secondo, una diretta in onda con l'Italia. È il concept da cui prende avvio lo spot di Vodafone per Giga Network Fibra, la connessione ultra-veloce che vuole rivoluzionare le abitudini degli italiani. Prosegue la retorica degli esempi: cioè tutto quello che si potrebbe fare con tale potenza nel telefonino. Siamo nel traffico di una grande città che potrebbe essere Milano; Linus e Nicola Savino sono imbottigliati. «Non arriveremo mai...», osserva sconsolato Linus. Ma Nicola ha un'idea. In pochi secondi l'auto è abbandonata (come nella scena di un film d'azione), e i due suonano alla porta di una comune famiglia italiana: «Signora, avete il wi-fi qui a casa? Dobbiamo fare la diretta...», intonano i due. Sono fortunati: «Abbiamo la Giga Network Fibra di Vodafone». Bene, un ostacolo è superato: i nostri eroi fanno comicamente irruzione nella casa, tutti bagnati per la pioggia battente. Gli italiani, si sa, sono ospitali, e la famiglia si mette all'opera per ricreare uno studio da dove trasmettere il programma del mattino. Trucco, parrucco, microfoni, studio: tutto improvvisato, ma funzionante. Ma ciò che più importa è la connessione: non solo si inizia a trasmettere in voce, anche le immagini, grazie al cellulare del piccolo di casa, sono disponibili. «Eccoci anche oggi in diretta, dalla cucina di casa Rossi, in via...». Colpo di scena, suonano alla porta, arriva un terzo ospite. «Sono io», dice Fedez, che ha sentito l'indirizzo per radio. La campagna (di Utopia, casa di produzione Akita Films) prosegue sul filone dello scorso anno, e con Linus. Mentre lo spot diventa anche un format ospitale per testimonial di passaggio.