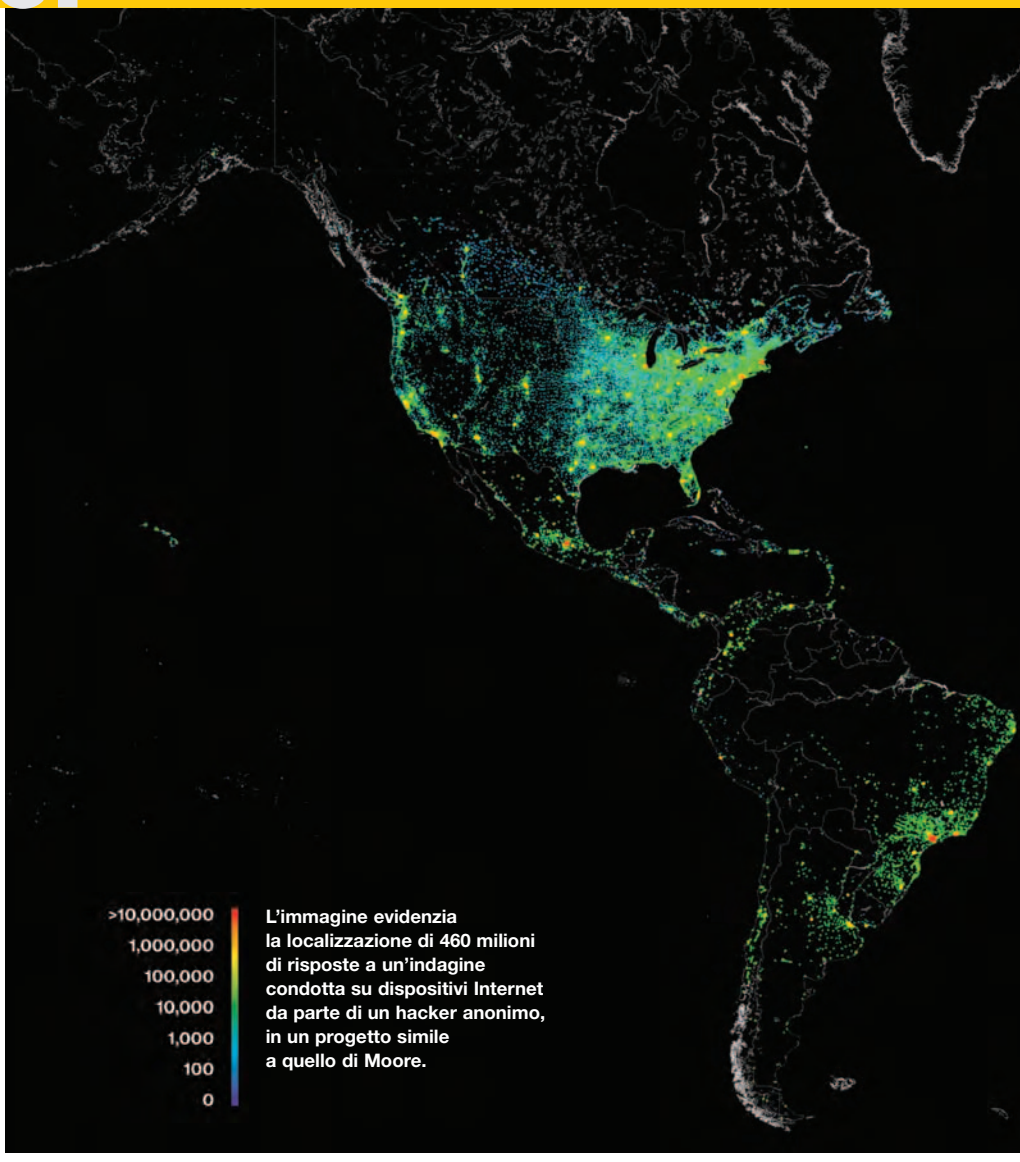
Se ti muovi, ti fulmino

Un esperimento scientifico ha sondato miliardi di dispositivi Internet rivelando che migliaia di sistemi aziendali offrono l'accesso remoto a chiunque.

Tom Simonite



L'immagine evidenzia la localizzazione di 460 milioni di risposte a un'indagine condotta su dispositivi Internet da parte di un hacker anonimo, in un progetto simile a quello di Moore.

Probabilmente non avrete sentito parlare di H.D. Moore, ma fino a poche settimane fa tutti i dispositivi Internet del mondo, inclusi magari alcuni dei vostri, sono stati contattati approssimativamente tre volte al giorno da una serie di computer che saranno ancora caldi nella sua sala operativa. «Ho diversi impianti di raffreddamento per accertarmi che la mia casa non prenda fuoco», dice Moore, che è a capo della ricerca presso la Rapid7, un'azienda di sicurezza informatica. Nel febbraio del 2012 Moore ha deciso di condurre personalmente un censimento su ogni dispositivo connesso a Internet.

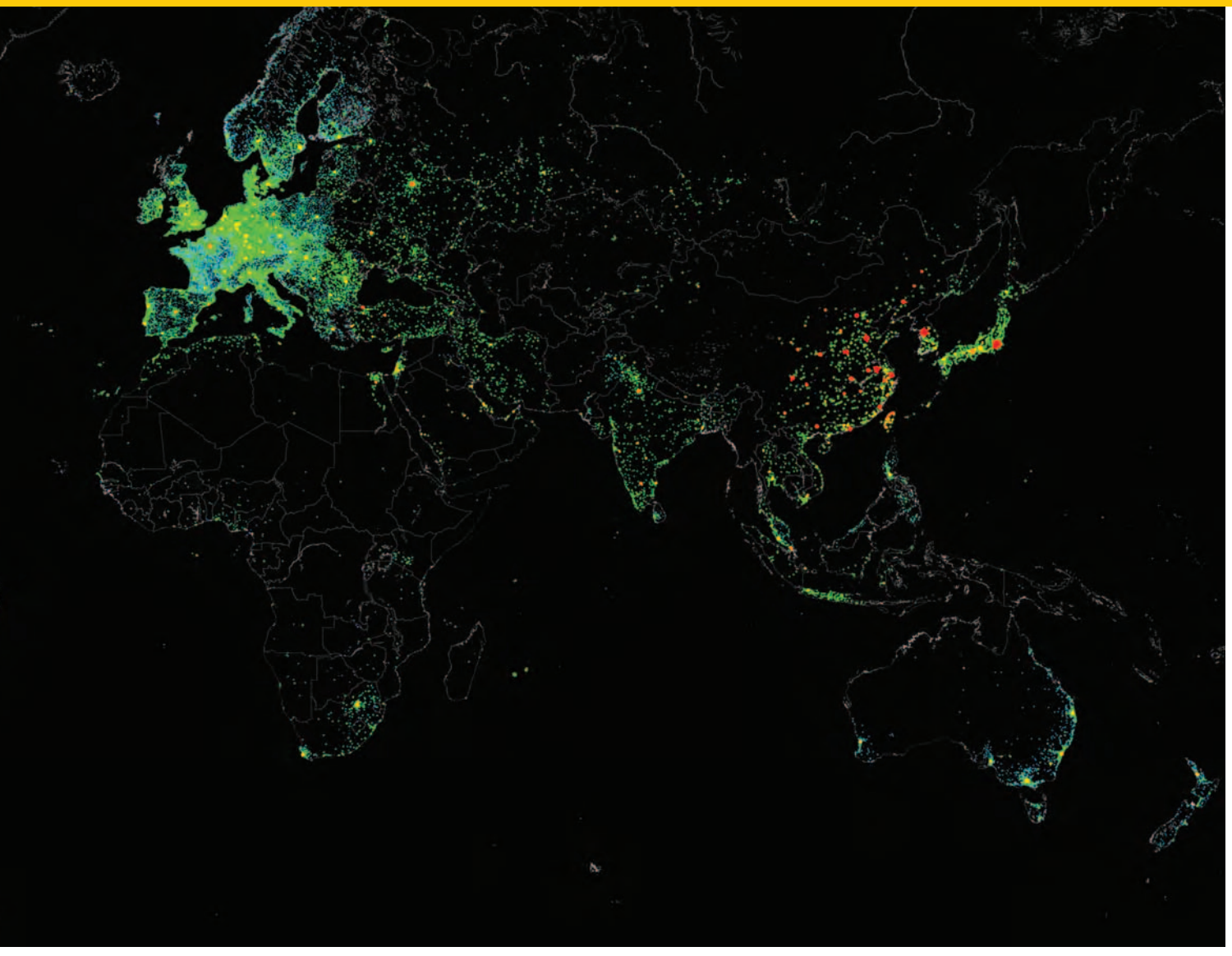
Moore ha ora sospeso l'esperimento, perché «ha scatenato parecchie lamentele, messaggi d'odio e telefonate da parte delle forze dell'ordine». I dati raccolti hanno rivelato alcuni seri problemi di sicurezza e reso manifesta le vulnerabilità di alcune attività e sistemi industriali, utilizzati per controllare di tutto, dalle luci del traffico alle reti elettriche.

Il censimento è stato effettuato semplicemente inviando con regolarità dei messaggi automatici a ciascuno dei 3,7 miliardi di indirizzi IP assegnati a dispositivi connessi alla Rete in giro per il mondo (Google, al contrario, raccoglie le informazioni offerte pubblicamente dai siti Web). Molti dei due terabyte (2mila gigabyte) di risposte che Moore ha ricevuto da oltre 310 milioni di IP provenivano da dispositivi vulnerabili o configurati in maniera tale da consentire a chiunque di assumerne il controllo.

Moore ha pubblicato i risultati di un segmento particolarmente preoccupante di questi dispositivi vulnerabili: quelli adoperati da sistemi industriali e commerciali. Molti di questi sistemi potrebbero venire violati utilizzando password generiche e 13mila consentivano un accesso diretto senza bisogno di password. Questi sistemi vulnerabili offrono agli aggressori notevoli opportunità, spiega Moore, tra cui il riavvio dei server e dei sistemi IT delle aziende, l'accesso ai registri di dispositivi medici e alle informazioni dei pazienti e persino a sistemi industriali di controllo di fabbriche o infrastrutture elettriche. Le scoperte di Moore sono state supportate da dati analoghi, pubblicati il mese scorso da un hacker anonimo e raccolti violando 420mila hardware connessi alla Rete.

Le connessioni che Moore stava cercando sono conosciute come server seriali, utilizzati per connettere a Internet quei dispositivi che non sono dotati di connessione autonoma. «I server seriali agiscono da collante tra sistemi arcaici e il mondo della rete», spiega Moore, che non sa se i difetti da lui scoperti sono già stati sfruttati, ma ha fornito dettagli su come le aziende possono ispezionare i propri sistemi alla ricerca di questi difetti.

Joel Young, responsabile delle tecnologie della Digi International, costruttrice di molti dei server seriali identificati da Moore, sostiene che la ricerca ha aiutato la sua azienda a comprendere come le persone utilizzano i suoi prodotti: «Alcuni dei clienti che acquistano i nostri prodotti non hanno seguito le giuste pratiche di sicurezza. Dobbiamo intervenire con una tempestiva educazione alla sicurezza dei nostri clienti». Young precisa che la sua azienda vende un servizio cloud capace di assicurare una connessione privata e sicura, lontana dal pubblico di Internet. Ciononostante, la Digi continua a distribuire i propri prodotti con password di default, perché semplifica il setup iniziale e sollecita i clienti a modificare personalmente le password.



Billy Rios, un ricercatore di sicurezza informatica che lavora a sistemi di controllo industriali presso la startup di sicurezza informatica Cylance, sostiene che il progetto di Moore quantifica validamente le dimensioni di un problema ben noto tra esperti come lui, ma non apprezzato dalle aziende a rischio. Secondo Rios, i sistemi utilizzati da utenze più sensibili, quali le infrastrutture energetiche, sono vulnerabili al pari dei sistemi di controllo delle porte automatiche di una piccola impresa.

La rimozione dei server seriali dalla rete pubblica, in maniera da renderli accessibili unicamente tramite una connessione privata, potrebbe prevenire molti degli attacchi più semplici, spiega Rios, ma gli aggressori potrebbero comunque ricorrere a varie tecniche per rubare le credenziali necessarie. Il lavoro si aggiunge ad altre significative scoperte compiute da Moore. I risultati da lui pubblicati a gennaio mostrano che intorno a 50 milioni di stampanti, postazioni di gioco, router e unità di memoria sono connesse alla Rete e possono diventare facile preda, a causa di un protocollo denominato Universal Plug and Play (UPnP). Questo protocollo consente ai computer di trovare automaticamente le stampanti, ma è anche installato all'interno di alcuni dispositivi di sicurezza, router a banda larga e sistemi di memoria dati, mettendo importanti dati a rischio.

I dati raccolti dal censimento di Moore hanno anche aiutato i colleghi della Rapid7 a identificare come alcune parti di software, denominate FinFisher, venissero utilizzate per spiare attivisti politici.

Sempre grazie a questi dati è stato possibile svelare la struttura di una campagna di nome Red October, che aveva da tempo infiltrato diversi sistemi governativi in Europa.

Moore crede che l'industria della sicurezza stia trascurando alcuni seri e basilari problemi di sicurezza concentrandosi prevalentemente sui computer utilizzati nelle aziende: «Per me è ovvio che abbiamo problemi più seri nell'uso che facciamo di Internet». Tuttavia Moore non ha alcuna intenzione di sondare nuovamente l'intera Rete. I costi elevati dell'elettricità e del traffico Internet, nonché incidenti quali la richiesta da parte del Computer Emergency Response Team del governo cinese alle autorità statunitensi di bloccare "gli attacchi hacker" di Moore, lo hanno convinto che è tempo di dedicarsi a qualche altro aspetto della sicurezza on-line: «Siamo seduti su montagne di nuove vulnerabilità». ■

Tom Simonite è redattore di MIT Technology Review.