[L'INTERVISTA]

"L'intelligenza artificiale è l'arma più efficace per la cybersicurezza"

IL RE DEGLI HACKER Una manifestazione ad Hong Kong in favore di Edward Snowden, tecnico informatico ex dipendente della Cia, che carpì dai computer governativi un immenso numero di informazioni segrete: per questo è diventato un simbolo della libertà assoluta che dovrebbe dominare, secondo una visione radicale, nel mondo internet

DAVE PALMER, UNA VITA PASSATA A COMBATTERE GLI HACKER PARTENDO DAI SERVIZI SEGRETI BRITANNICI, PRESENTA DARKTRACE: "I NOSTRI PROGRAMMI SONO IN GRADO DI ADATTARSI AUTOMATICAMENTE ALLE MODIFICHE CHE SUBISCE UN VIRUS QUANDO CERCA DI SFONDARE I VARI LIVELLI DI PROTEZIONE". COMUNQUE, NIENTE PAURA: "NON SIAMO ALLA VIGILIA DELL'ARMAGEDDON INFORMATICO"

Filippo Santelli

Roma

«No, non sarà l'Armageddon. Non ci sveglieremo domani con gli smartphone muti o la rete elettrica in tilt». È raro, nel mondo della cybersicurezza, trovare qualcuno che non agiti apocalittici spauracchi, imminenti attacchi hacker capaci di mettere in ginocchio il mondo. Sarà il passato nell'Mi5, la super agenzia inglese per la sicurezza e il controspionaggio, ma Dave Palmer preferisce un approccio più misurato: «Il problema è che gli attacchi si sviluppano sempre più veloci e pochissime istituzioni sono attrezzate per gestirli». Basso profilo, britannica compostezza, massima serietà: le stesse qualità con cui Darktrace, la startup di cui ora Palmer è responsabile della tecnologia, sta conquistando finanziamenti (179,5 milioni di dollari) e clienti in tutto il mondo. Un'alleanza tra ex spie di Sua Maestà e cervelloni di Cambridge, tra strategia e intelligenza artificiale, basato su un'intuizione: «Che la sicurezza delle aziende debba cambiare, ispirandosi al nostro sistema immunitario».

Cosa cambierebbe in concreto?

«Oggi le aziende costruiscono delle difese esterne, che però non bastano più a contenere gli attacchi visto che i loro sistemi informatici sono necessariamente globali, complessi e permeabili. Quindi a quelle difese noi aggiungiamo una componente di intelligenza artificiale che imita il corpo umano: anziché provare a identificare la minaccia, si studia il funzionamento normale della rete, evidenziando eventi inusuali che possono essere spia di una breccia».

Intelligenza artificiale è un'espressione di cui spesso e volentieri si abusa.

«I nostri brevetti nascono da ricerche di frontiera dell'Università di Cambridge sulla teoria della probabilità applicata al machine learning. Significa che l'intelligenza artificiale può rallentare o interrompere l'attacco in maniera automatica».

La guerra per la sicurezza si giocherà senza l'intervento umano? Le aziende si fideranno?

«Lo sviluppo è velocissimo e credo che arriveremo a quel punto: un sistema di sicurezza governato dalle macchine, in cui gli uomini non specificheranno più da quali tecnologie difendersi, come si fa ora, ma il tipo di minacce da evitare. Per esempio: non voglio che utenti sconosciuti accedano alla lista fornitori dell'impresa. Anche perché pure gli assalitori presto inizieranno a usare l'intelligenza artificiale, algoritmi in grado di capire il linguaggio umano e generare un messaggio mail coerente e rilevante dentro cui nascondere un virus. Quello sarà un brutto giorno per la sicurezza».

Siamo all'indomani di due vasti attacchi hacker, WannaCry e NotPetya. Cosa hanno rivelato sull'evoluzione del crimine informatico?

«Sono due casi diversi. WannaCry è un'arma digitale messa a punto dall'agenzia per la sicurezza Usa finita nelle mani degli hacker, una dinamica nota ma che non era mai stata così veloce. NotPetya invece è una copia di WannaCry messa a punto da un gruppo di criminali informatici legati al governo russo con il preciso intento di danneggiare l'Ucraina. Questa è una novità: governi che copiano gli hacker. Ma la cosa che colpisce di questi attacchi è la rapidità».

In che senso?

«Secondo una vecchia favola ci volevano mesi, anche un anno, per infiltrarsi nei sistemi. Qui è successo tutto nel giro di giorni. Non ci sono molti business pronti a gestire questa velocità. Pensiamo per esempio a Deloitte, che ha appena annunciato un attacco avvenuto un anno fa e scoperto a marzo. Molte aziende non sono coperte sette giorni su sette e 24 ore al giorno, a questo serve una risposta automatica».

L'ultimo caso è Equifax, la società di merito creditizio americana che gli hacker hanno infiltrato per mesi, mettendo a rischio i dati di 140 milioni di persone e portando il Ceo a dimettersi.

«Le società hanno un grosso problema di visibilità: non riescono a percepire ciò che accade nelle loro reti. I nuovi attacchi sono sempre meno evidenti e come nel caso di Equifax possono minare la fiducia dei consumatori nella capacità dell'impresa di tutelare i loro dati. Le grandi aziende soffrono ma spesso recuperano, per quelle più piccole perdere i dati degli utenti può portare al fallimento. Ma ciò che mi preoccupa ancora di più è l'impatto di lungo periodo di questi attacchi sul sistema economico: il livello di fiducia tra gli operatori si riduce, danneggiando la crescita».

Governi e aziende investono abbastanza in cybersicurezza?

«La situazione è molto diseguale, anche in Italia. Le grandi aziende sono ben organizzate, tante medie e piccole non hanno accesso alle tecnologie e alle competenze più avanzate. Qui si può inserire l'azione dei governi. Oltre a investire sulla difesa delle infrastrutture critiche, devono educare i cittadini e le aziende. Singapore o il Regno Unito lo stanno facendo, anche con corsi nelle scuole. Noi cerchiamo di farlo con le imprese, spiegando loro che non puoi avere una difesa perfetta, ma mettere in campo dei processi per gestire l'emergenza. Che meno persone vanno dedicate a identificare la prossima minaccia e più alla risposta».


1


2

Greg Clark, ceo di Symantec (1) e **Evghenij Kaspersky**, a capo del gruppo omonimo (2): sono i due Big dell'antivirus; a destra **Dave Palmer**, fondatore di Darktrace, specializzata nella tecnologia di intelligenza artificiale per la cyberdefense