Sole 24 Ore Nòva 24

24-NOV-2022
da pag. 32 / foglio 1 / 2

Settimanale - Dir. Resp.: Fabio Tamburini
Tiratura: N.D. Diffusione: N.D. Lettori: 694000 (0003835)

Ransomware forti con crittografia intermittente e intelligenza artificiale

Cybersecurity. Contro attacchi sempre più numerosi, grazie a nuovi sistemi, non bastano in azienda le tecnologie, servono competenze multidisciplinari

L'Ia abilita la continua riscrittura del codice malevolo, la crittografia permette di bloccare velocemente i sistemi

Alessandro Longo

Gli attacchi cyber, a partire da quelli più pericolosi e diffusi del momento, i ransomware, diventano più intelligenti. Di conseguenza devono diventarlo anche le difese. È la corsa agli armamenti della cybersecurity, a forza di innovazioni contrapposte. Uno dei protagonisti, in entrambe le barricate, è ora l'intelligenza artificiale, come emerso ieri a Montreal al Forum organizzato dalla Italian Chamber of Commerce in Canada. «I cybercriminali si servono sempre più spesso dell'Ia», dice Domenico Raguseo, capo della cyber in Exprivia. Ora l'Ia è usata in tutte le fasi di azione del ransomware, almeno negli approcci più evoluti. Conferma Michele Colajanni, docente all'università di Bologna: «I criminali si servono dell'Ia per velocizzare la scrittura del codice malevolo e la sua continua modifica-ricompilazione, in modo da renderlo meno individuabile. Ma anche per velocizzare i messaggi di phishing con cui spingere la vittima, con testi personalizzati in modo automatico, a installare il malware». Ultimo tassello: «L'Ia è usata anche per velocizzare la scansione delle vulnerabilità dei sistemi dell'azienda target».

In modo analogo, l'Ia comincia a essere usata dalle organizzazioni più strutturate contro il rischio cyber. Ad esempio per stimarlo e per fare analisi delle vulnerabilità, per rilevare anomalie di comportamento dei sistemi, sintomo di una intrusione, come per velocizzare la risposta a un incidente. «L'automazione, con Ia, è necessaria per rispondere ad attacchi sempre più veloci e mutevoli», conferma Gianluca Mazzini, ceo di Lepida, in house della Regione Emilia Romagna: «Anche così si può vincere la battaglia di velocità che vede ora gli attaccanti avvantaggiati, soprattutto verso bersagli lenti e formali quali sono le pubbliche amministrazioni». Non sfugge agli esperti che questa corsa la stanno vincendo i criminali. «Sono specializzati in attacchi informatici, dopotutto; mentre le aziende che si devono difendere lo sono in altri campi e le nuove competenze le hanno dovuto costruire in seconda battuta», riassume Colajanni. Per altro, «dei nuovi strumenti per ora si stanno avvantaggiando soprattutto i criminali per diventare ancora più veloci», ribadisce.

Ed è una velocità crescente, quella di un attacco cyber che in pochissimo tempo può bloccare – con un ransomware – i sistemi di un'azienda. Come se non bastasse l'Ia, ci si mettono anche nuove modalità di crittografia usata dai ransomware, come si legge un recente articolo tecnico pubblicato dal ricercatore di sicurezza Aleksandar Milenkoski. Ha analizzato BlackCat, il ransomware scritto in Rust dall'omonima gang che ha causato danni, tra l'altro, a Moncler, Università di Pisa e al Gestore dei Servizi Energetici (Gse). La novità si chiama crittografia intermittente, che serve appunto a velocizzare il processo con cui il ransomware blocca tutto.

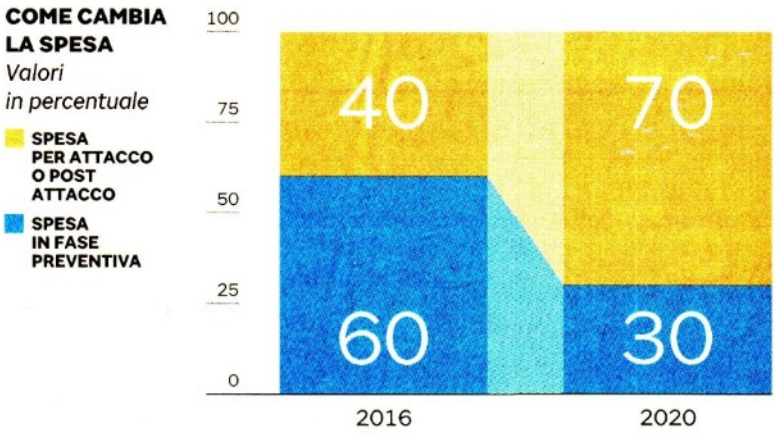
In sostanza la tecnica rende la criptazione più veloce a scapito della sua robustezza. L'obiettivo non è più renderla insuperabile anche in un tempo lunghissimo. A chi usa i ransomware basta che la crittografia sia tale da bloccare un sistema per un tempo sufficiente a causare grossi danni all'azienda. Tanto basta per costringerla a pagare il riscatto. La velocità maggiore serve di contro a bloccare più sistemi possibili prima che l'azienda possa intervenire.

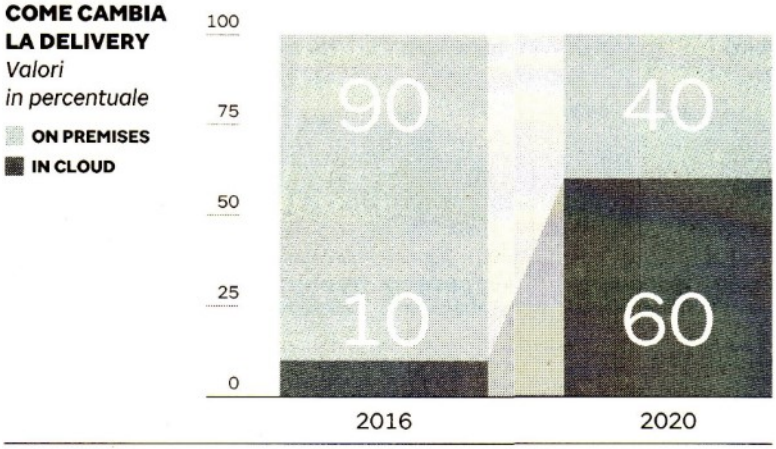
Se la sfida cyber fa un salto di qualità e i cattivi partono da posizione di vantaggio, alle aziende non basta investire in nuove tecnologie. «L'automazione delle difese non basta. Bisogna in primis governarle. Abbiamo imparato che non esiste sicurezza senza governance dei sistemi e viceversa», dice Mazzini. Vuol dire: «Azioni continue di controllo sui propri sistemi, policy rigorose di prevenzione e mitigazione dei danni, come stiamo provando a fare noi». Ma anche «costruzione di competenze multidisciplinari in azienda. Perché è una sfida che si può affrontare solo con un mix di professionalità, che devono dialogare e contaminarsi».

Superficie 31 %

Sole 24 Ore Nòva 24
Settimanale - Dir. Resp.: Fabio Tamburini
Tiratura: N.D. Diffusione: N.D. Lettori: 694000 (0003835)

Cyberdifese in evoluzione





Fonte: McKinsey