Affidarsi all’Intelligenza Artificiale? Si può (e si deve) fare

Lug 02, 2019 Marco Schiaffino Approfondimenti, Attacchi, In evidenza, Malware, RSS, Scenario, Tecnologia 0

Dalla ricerca SonicWall emerge uno scenario in cui gli attacchi alle aziende raggiungono volumi impressionanti come frequenza e intensità. Serve l’AI.

Un panorama in costante evoluzione in cui gli attacchi sono sempre più sofisticati e la pressione sulle infrastrutture informatiche di aziende e governi aumenta esponenzialmente. È questo ciò che emerge dal **Cyber Threat Report 2019** pubblicato da **SonicWall**.

Partiamo dalle buone notizie e in particolare dalla perdita di efficacia dei **ransomware**. Sfortunatamente l’arretramento di questa tipologia di malware non interessa tutto il mondo, ma alcune nazioni chiave come **Regno Unito e India**. A livello globale, invece, gli attacchi con ransomware segnano un +11% rispetto all’anno precedente.

La seconda buona notizia riguarda il numero di vulnerabilità individuate dai ricercatori nel 2018. Sono 18.097, in netto aumento rispetto al 2017, con 12.920 CVE pubblicate.

Perché è una buona notizia? Principalmente perché sembra che la diffusione dei programmi di bug bounty stiano sortendo i risultati che ci si aspettava. Più ricercatori al lavoro, più falle di sicurezza individuate prima che qualcuno riuscisse ad

approfittarne.

Le buone notizie finiscono qui. Secondo i rilevamenti di SonicWall, basati sui dati raccolti in tempo reale da circa **1,3 milioni di endpoint** in tutto il mondo, il volume complessivo di attacchi attraverso malware nel 2018 è infatti cresciuto notevolmente, arrivando a **10,5 miliardi** (erano 8,6 miliardi nel 2017) confermando una tendenza che ha avuto una flessione solo nel 2016.

Accanto alla crescita di attacchi malware, SonicWall segnala i rischi legati alle nuove tecniche di attacco side-channel come Spectre e Meltdown. “È solo una questione di tempo” ci spiega

Bob Vankirk, Chief Revenue Officer della società di sicurezza. “Tra qualche tempo ci troveremo a fronteggiare attacchi che sfruttano queste tecniche per fare leva sulle vulnerabilità hardware dei processori”.

Uno scenario che, secondo Vankirk, va di pari passo con l’evoluzione delle tecniche di attacco utilizzate dai governi nella cyber-warfare, come dimostrano i recenti attacchi portati dagli Stati Uniti nei confronti dell’Iran.

“Per fronteggiare minacce come queste è necessario usare strumenti alternativi rispetto ai tradizionali antivirus” prosegue Vankirk. “Quello che serve è un sistema di analisi in tempo reale che permetta di individuare e bloccare gli attacchi automaticamente”.

Un percorso, questo, che SonicWall ha intrapreso l’anno scorso attraverso una tecnologia battezzata con il nome di **Real-Time Deep Memory Inspection (RTDMI)**. “L’uso dell’Intelligenza Artificiale ci permette di individuare i malware direttamente a livello di memoria” spiega **Luis Fisas** di SonicWall. “Un sistema molto più efficiente delle classiche sandbox sia in termini di accuratezza, sia in termini di rapidità nel rilevamento e nel contrasto all’attacco”.

La logica, spiegano Fisas e Vankirk, è piuttosto semplice: **lo stesso aumento del numero di attacchi, che genera una maggiore mole di dati da dare in pasto ai sistemi di AI, permette di migliorare le prestazioni del motore di scansione**.

A dimostrarlo, proseguono, è il numero (oggettivamente impressionante) di nuove tecniche di attacco individuate attraverso RTDMI nel corso del 2018.

Dalle parti di SonicWall, però, ritengono che l'approccio automatizzato "in tempo reale" sul quale stanno lavorando abbia un altro importante vantaggio. **Il sistema, infatti, permetterebbe di reagire agli attacchi anche in contesti che non possono contare su strutture dedicate**.

"Le piccole e medie aziende sono quelle che rischiano di più in questo scenario" puntualizza Vankirk. "Non potendo contare su risorse dedicate al contrasto degli attacchi informatici, hanno infatti bisogno di sistemi che possano bloccarli automaticamente".

Condividi l'articolo

Raffica di vulnerabilità nell'infrastruttura server Lenovo

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/02/affidarsi-allintelligenza-artificiale-si-puo-e-si-deve-fare/