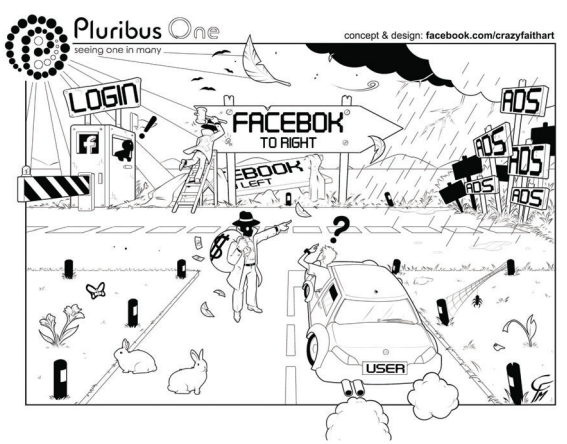
Chi difende l'Intelligenza Artificiale?

L'intelligenza artificiale protegge Internet. Pluribus One protegge l'IA

CISCO nel suo ultimo rapporto annuale ci fa sapere che il 34% delle aziende usa l'IA per la sicurezza informatica. Quello che usano è il "machine learning", algoritmi addestrati su enormi quantità di dati capaci di identificare anomalie nel comportamento dei calcolatori e dei loro utenti. Il machine learning può così riconoscere l'uso anomalo di un dispositivo da parte di un hacker che ha rubato la mia password. Sembra una panacea per la sicurezza informatica ma il diavolo come sempre sta nei dettagli. Gli algoritmi intelligenti imparano dai dati che gli vengono forniti: se non li proteggiamo potrebbero essere manipolati e falsificati per fare imparare all'algoritmo quello che vuole un hacker. È già accaduto al chatbot Tay di Microsoft, accade spesso con i filtri anti spam che usano l'IA.

Pluribus One, spin off dell'Università di Cagliari fondata nel 2015, con alle spalle più di vent'anni di ricerca universitaria in IA e cybersecurity, assegnataria di 5 finanziamenti europei per R&D, è la prima azienda al mondo che mette in sicurezza l'intelligenza artificiale. Pluribus One fornisce ai suoi clienti algoritmi di machine learning che sono davvero l'anello forte della catena della sicurezza informatica e non rischiano di diventare quello più debole perché "avvelenati" da dati falsificati. Bell'esempio



Phishing: frode informatica che ci spinge a visitare siti internet pericolosi rendendoli a prima vista simili ai siti che conosciamo bene e su cui spesso navighiamo

Pluribus One
seeing one in many

di quella che all'estero viene detta "imprenditoria accademica". Ricercatori di fama internazionale che creano un'azienda per dimostrare che la "next big thing" può nascere in Italia, nel Sud Italia.

E non ci sono dubbi che la sicurezza dell'intelligenza artificiale sarà la "next big thing". Le premesse ci sono tutte, i guru e i grandi player sono concordi. Uno degli ultimi rapporti ufficiali di Huawei, il colosso cinese da 100 miliardi di dollari, è dedicato alla sicurezza dell'IA: per Huawei è "una questione di vita o di morte". Lo scorso Dicembre la Commissione Europea ha presentato il suo piano strategico sull'IA: la stella polare della strategia europea è lo sviluppo di un'intelligenza artificiale sicura. È una congiuntura astrale. Se da una parte gli analisti prevedono che il mercato dell'IA per la cybersecurity varrà 34,81 miliardi di dollari nel 2025, e quindi tutte le aziende vogliono l'IA nei loro prodotti di sicurezza, dall'altra nessuno sa cosa accadrà quando le vulnerabilità dell'IA diventeranno di pubblico dominio. Il valore del mercato della sicurezza dell'IA potrebbe essere maggiore di quello dell'IA per la sicurezza.

L'obiettivo "luna" dell'IA sicura la giovane Pluribus One lo ha declinato in prodotti e soluzioni già sul mercato. L'offerta dell'azienda ruota intorno al tema della sicurezza del Web. Da un lato c'è il prodotto di punta Attack Prophecy che protegge i servizi erogati tramite applicazioni Web. Attack Prophecy protegge il business dei clienti con un algoritmo di machine learning che impara quale è il normale funzionamento dei servizi, riconosce eventuali anomalie e blocca tutti i tentativi di uso improprio, dagli attacchi noti della OWASP Top 10 a quelli "mai visti prima". Dall'altro lato ci sono le soluzioni per proteggere dal phishing, dal malware e dagli attacchi contro quello che sta diventando l'anello più debole per la sicurezza informatica: l'uomo.

La prossima sfida è lo sviluppo di una soluzione (xAV) per la protezione dei dispositivi mobili, anch'essa con a bordo IA sicura, che l'azienda sta realizzando grazie ad un finanziamento di Sardegna Ricerche (POR FESR RAS 2014-2020 - Az. 3.6.4).