Quando l’Intelligenza Artificiale diventa una minaccia

Nov 30, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Tecnologia 0

Non solo business e software di protezione: AI e Machine Learning possono essere sfruttati anche dai pirati informatici per i loro scopi.

Esistono tecnologie buone e tecnologie cattive? Più che una questione filosofica, quella a cui hanno cercato di rispondere **Trend Micro**, **Europol** e **United Nations Interregional Crime and Justice Research Institute (UNICRI)** è una domanda che molti ricercatori di sicurezza si stanno ponendo negli ultimi anni.

Il tema è quello dell’Intelligenza Artificiale e dei possibili utilizzi che possono esserne fatti nel settore della cyber security. **In altre parole, è il timore (condiviso dai più) che presto l’AI non venga utilizzata solo da software antivirus e strumenti di protezione, ma anche dai cyber criminali**.

Il corposo report stilato dai ricercatori (consultabile a questo indirizzo Web) prova a disegnare un quadro dei possibili utilizzi malevoli dell’AI che vadano oltre quelli visti finora, che si sono limitati alla produzione di deepfake più o meno accurati.

Lo scenario più inquietante, cioè quello dell’uso di tecnologie di intelligenza artificiale per **la creazione di malware di nuova generazione**, viene per fortuna archiviato in un prossimo (e si spera lontano) futuro.

Secondo gli autori del report, infatti, questo tipo di attività è per il momento limitata a qualche esperimento portato avanti da ricercatori di sicurezza per scopi accademici o comunque puramente teorici.

I pochi esperimenti portati avanti, come **DeepHack** e **DeepExploit**, hanno comunque suscitato un certo interesse nel mondo del cyber crimine, come testimoniano alcuni post intercettati da Trend Micro su forum frequentati da hacker.

Più probabile che l'utilizzo dell'AI possa essere indirizzato al potenziamento di tecniche di attacco già esistenti, come la creazione di messaggi di spam o di phishing che siano in grado di aggirare i filtri utilizzati dai software di protezione.

Anche l'applicazione dell'AI ai **sistemi di crittografia**, sia in chiave di sviluppo di nuovi algoritmi, sia in funzione dello sviluppo di strumenti per la sua violazione, è ancora a uno stato embrionale.

Gli studi in questo senso, però, hanno già dimostrato come i possibili sviluppi consentirebbero di creare sistemi di comunicazione pressoché impossibili da decifrare.

La sezione dedicata agli indizi individuati in rete da Trend Micro sull'utilizzo di sistemi di intelligenza artificiale nel

mondo del cyber crimine indicano però un progressivo sviluppo di queste tecnologie.

I riferimenti, per il momento, si limitano alla creazione di reti di bot per i social network (come Instagram) che siano in grado di simulare il comportamento umano e consentire così ai pirati informatici di aggirare i sistemi di controllo (come **CAPTCHA**) utilizzati per individuare i sistemi automatizzati.

Un possibile utilizzo dell'AI con scopi malevoli, secondo i ricercatori, potrebbe però trovare presto una sua applicazione nel mondo del gaming e, soprattutto, nell'ambito dei videogiochi in cui l'accumulo di denaro virtuale (ma convertibile in valuta reale) ha un ruolo preminente.

Un impiego simile potrebbe riguardare **la compravendita di criptovalute**, secondo uno schema che al momento è pura fantasia, ma che è già stato ipotizzato spesso in varie truffe online.

Insomma: lo stato delle cose, a quanto si legge nel report, è ancora uno scenario in cui ai tanti timori corrisponde solo un certo interesse dei pirati per il tema. Le cose, però, potrebbero cambiare molto, molto rapidamente.

Condividi l'articolo

IceRat: il trojan "virtuale" che sfugge agli antivirus Trova due falle zero-day in Windows 7 e 2008 Server… per caso

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/30/quando-lintelligenza-ar

tificiale-diventa-una-minaccia/?utm_source=rss&utm_medium=rss&utm_campaign=quando-lintelligenza-artificiale-diventa-una-minaccia