Co będzie z Captcha?

Niedawno opublikowane wyniki badań pokazują, że niektóre rodzaje zabezpieczeń captcha stały się przestarzałe. Powód: maszyny nauczyły się, jak je omijać.

Operatorom stron internetowych zależy na odwiedzinach prawdziwych użytkowników , lecz nie na rękę jest im przeciążenie strony doprowadzające do jej paraliżu. Captcha są zatem ważnym narzędziem, ułatwiającym weryfikację. Opierają się na niewielkich zagadkach obrazkowych, które człowiek z łatwością rozwiąże, podczas gdy dla maszyny będzie to nie lada wyzwanie.

Ciemna strona uczenia maszynowego

Ekipie badawczej udało się wykorzystać uczenie maszynowe do automatycznego rozwiązywania niektórych popularnych captcha tekstowych. Modelowy atak wymaga niewielkiego wysiłku, przez co captcha jako rozwiązanie zabezpieczające stają się przestarzałe. W przeciwieństwie do wcześniejszych modeli ten bieżący potrzebuje do skutecznej nauki niewielkiej ilości danych. Raport opracowany przez Science Daily pokazuje, że wystarczy 500 przykładów zagadek, by opracowany model nauczył się, jak je rozwiązywać.

- Jest to niepokojąca tendencja, ponieważ wiele stron wykorzystuje captcha do zapobiegania atakom opartym na przeciążeniu strony - tłumaczy Robert Dziemianko z G DATA. - Gdy atakujący zdobędzie dostęp do tej technologii, jest w stanie z łatwością obejść blokadę w postaci tekstowych captcha i doprowadzić do przeciążenia strony. Programowanie narzędzi rozwiązujących captcha było do tej pory bardzo czasochłonne. Wymagało wiele pracy przy wprowadzaniu setek tysięcy danych - dodaje przedstawiciel firmy G DATA.

Ponadto narzędzie tego typu można było zaprogramować jedynie dla danego specyficznego rodzaju captcha. Dlatego też przestępcy odwoływali się w przeszłości do najbardziej oczywistego rozwiązania: znajdowali inne osoby, które rozwiązywały captcha za nich. Z pomocą nisko opłacanych pracowników możliwe było rozwiązywanie nawet tysięcy captcha na godzinę. Szacunki przedstawione w innym raporcie z badań pokazują, że na rzecz przestępców rozwiązywano nawet 1000 różnych captcha za cenę około jednego dolara. Takie działanie otwiera drogę nie tylko atakom DDoS, ale również przesyłaniu wiadomości ze spamem.

Co to są Captcha?

Captcha to skrót od angielskiej frazy Completely Automated Public Turing test to tell Computers and Humans Apart (Całkowicie Zautomatyzowany Publiczny test Turinga do Odróżniania Komputerów od Ludzi). Pierwotnie test Turinga został zaprojektowany do informowania użytkowników o tym, czy mają do czynienia z komputerami, czy z ludźmi. Ściśle mówiąc, captcha stanowią odwrócony test Turinga: komputer daje użytkownikowi zadanie, które w swojej naturze jest niemożliwe do rozwiązania przez komputer. Jeden z najpopularniejszych przykładów takiego testu składa się z liter, których kształt został nieco zmieniony i które czasami umieszcza się na tle w innym kolorze. Zadaniem użytkownika jest wpisanie poprawnej sekwencji liter. Gdy mu się to uda, test zostaje zaliczony, ponieważ model zakłada, że jedynie człowiek jest w stanie poprawnie wykonać takie zadanie. Założenie to wykorzystywane jest do odróżnienia faktycznych użytkowników odwiedzających stronę od automatów tworzonych na przykład przez botnet. Inne captcha opierają się na obrazkach, a zadaniem użytkownika jest odnalezienie danych obrazków pomiędzy innymi elementami.

Jasny obraz sytuacji

W związku z powyższym nikogo nie powinno dziwić, że uczenie maszynowe to nie tylko nieocenione narzędzie do walki z cyberprzestępczością oraz wykrywaniem złośliwego oprogramowania, ale także technika, którą przestępcy mogą wykorzystać do niecnych celów. Jeden z badaczy odważył się już nawet stwierdzić w oparciu o przeprowadzone analizy, że operatorzy stron internetowych powinni zaprzestać korzystania z captcha i stosować rozwiązania alternatywne, takie jak analiza zachowań użytkowników czy lokalizacja urządzeń.

Na chwilę obecną atak jest skuteczny wyłącznie w odniesieniu do captcha zawierających tekst, a więc w przypadku captcha wykorzystujących obrazki (np. Wybierz wszystkie obrazki, na których widać samochód) atak nie ma (jak na razie) szans powodzenia.