Bitdefender

Podwójny wpływ sztucznej inteligencji na krajobraz cyberbezpieczeństwa

07.06.2023

Krajobraz cyberbezpieczeństwa stale ewoluuje, a wraz z postępem technologicznym zmieniają się narzędzia i taktyki stosowane zarówno przez cyberprzestępców, jak i specjalistów ds. bezpieczeństwa cybernetycznego. Jednym ze znaczących ostatnich osiągnięć, które przyciągnęło wiele uwagi, jest pojawienie się open-source'owych, generatywnych narzędzi sztucznej inteligencji (AI) i potężnych modeli językowych, takich jak ChatGPT i Bard. Technologie sztucznej inteligencji są jednak mieczem obosiecznym – choć mogą pomóc przepracowanym specjalistom ds. cyberbezpieczeństwa poprzez automatyzację i usprawnienie rutynowych zadań, mogą być również wykorzystywane przez cyberprzestępców do automatyzacji i skalowania ataków lub uczynienia ich bardziej przekonującymi.

Ciemna strona: narzędzie w rękach cyberprzestępców

Modele językowe, takie jak ChatGPT, ułatwiły cyberprzestępcom szybkie tworzenie wyrafinowanych, autentycznych wiadomości phishingowych i ataków socjotechnicznych. Ponieważ narzędzia te mogą natychmiast generować konwersacyjny tekst, hakerzy są w stanie w przekonujący sposób naśladować styl komunikacji zaufanych osób lub organizacji, zwiększając w ten sposób skuteczność swoich ataków. Wkrótce cyberprzestępcy prawdopodobnie wykorzystają te modele językowe w połączeniu z obrazami, dźwiękami i klipami wideo generowanymi przez sztuczną inteligencję, aby dalej oszukiwać niczego niepodejrzewających użytkowników sieci, aby udostępniali poufne informacje, zapewniali dostęp do systemów komputerowych lub podejmowali działania, których nie powinni.

Ponadto generatywne narzędzia sztucznej inteligencji, takie jak ChatGPT i inne, umożliwiają cyberprzestępcom skalowanie i automatyzację ataków w stopniu, który wcześniej nie był możliwy. Nawet początkujący cyberprzestępcy mogą korzystać z tych narzędzi, aby ułatwić sobie pisanie złośliwego kodu lub modyfikować istniejące złośliwe oprogramowanie. Chociaż ChatGPT ma pewne zabezpieczenia, aby uniemożliwić użytkownikom generowanie złośliwego oprogramowania lub innych treści w niecnych celach, badacze bezpieczeństwa firmy Bitdefender odkryli, że zabezpieczenia te można stosunkowo łatwo obejść za pomocą odpowiednich technik i wiedzy. Używając generatywnych narzędzi sztucznej inteligencji do usprawniania rozwoju złośliwego oprogramowania i automatyzacji dystrybucji swoich ataków, grupy cyberprzestępcze mogą zwiększyć ich częstotliwość i zarzucić szerszą sieć, aby atakować więcej potencjalnych ofiar.

Jasna strona: Pomoc dla przepracowanych zespołów bezpieczeństwa

Pomimo obaw i zagrożeń związanych z generatywną sztuczną inteligencją technologie te stanowią również okazję dla organizacji do wzmocnienia zabezpieczeń cybernetycznych i wsparcia ich często przepracowanych zespołów ds. cyberbezpieczeństwa. Przy stale rosnącej liczbie i złożoności cyberzagrożeń narzędzia oparte na sztucznej inteligencji mogą pomóc zespołom ds. cyberbezpieczeństwa.

„Sztuczna inteligencja może być również wykorzystywana do automatyzacji monitorowania i analizy zdarzeń i dzienników związanych z bezpieczeństwem, identyfikowania anomalii w zachowaniu oraz umożliwiania szybszego wykrywania i reagowania na potencjalne zagrożenia. Algorytmy uczenia maszynowego można wyszkolić w celu identyfikowania wzorców wskazujących na złośliwą aktywność, oszczędzając cenny czas specjalistów ds. cyberbezpieczeństwa na badanie i łagodzenie zagrożeń" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Bitdefender od dawna osadza w ten sposób sztuczną inteligencję i uczenie maszynowe (ML) w rozwiązaniach dbających o odpowiedni poziom cyberbezpieczeństwa użytkowników. Na przykład Bitdefender GravityZone eXtended Detection and Response (XDR) wykorzystuje technologie ML do korelowania i analizowania ogromnych ilości danych bezpieczeństwa z różnych czujników i źródeł w całej organizacji.

Ostatecznie organizacje muszą przyjąć proaktywne wielowarstwowe

podejście do bezpieczeństwa, aby wzmocnić swoją odporność cybernetyczną, ponieważ nowoczesne technologie sztucznej inteligencji stają się coraz bardziej popularne. Firmy powinny przyjąć najlepsze praktyki w zakresie szkoleń z zakresu bezpieczeństwa, aby pomóc pracownikom zrozumieć złożoność dzisiejszych zagrożeń i dowiedzieć się, jak nie stać się ich ofiarą. Przedsiębiorstwa mogą również rozważyć korzystanie z technologii bezpieczeństwa opartych na sztucznej inteligencji i uczeniu maszynowym, które mogą ulepszyć i pomóc ich zespołom ds. bezpieczeństwa w monitorowaniu, identyfikowaniu i reagowaniu na zagrożenia.

Biorąc pod uwagę dotychczasowy rozwój technologiczny, możemy postawić tezę głoszącą, że nie ma już powrotu do czasów sprzed wykorzystywania generatywnej sztucznej inteligencji. Narzędzia te są teraz łatwo dostępne dla wszystkich, ale dzięki odpowiednim strategiom i rozwiązaniom cyberbezpieczeństwa organizacje mogą je wykorzystać na swoją korzyść, aby być o krok przed przeciwnikami.

Źródło: https://bitdefender.pl/podwojny-wplyw-sztucznej-inteligencji-na-krajobraz-cyberbezpieczenstwa/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 07.06.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.