Hakerzy współpracują ze sztuczną inteligencją – ekspert ostrzega przed nowymi sposobami hakowania

Sztuczna inteligencja (AI) zmieniła zasady gry w wielu obszarach naszego codziennego życia, w tym w cyberbezpieczeństwie. Wraz z rosnącym wykorzystaniem nowych narzędzi opartych na AI, takich jak ChatGPT, liczba cyberataków podwoiła się, a same ataki stały się bardziej wyrafinowane. Eksperci ds. cyberbezpieczeństwa twierdzą, że narzędzia cyberbezpieczeństwa oparte na sztucznej inteligencji mogą pomóc chronić Twoją prywatność w nowej rzeczywistości, ale nie są one złotym środkiem.

> *„Sztuczna inteligencja nie pozbawi hakerów pracy, przynajmniej w najbliższym czasie. Cyberprzestępcy chętnie korzystają z narzędzi opartych na sztucznej inteligencji, ale chodzi o wprowadzanie ulepszeń, a nie zastąpienie działań. Hakerzy nauczyli się korzystać ze sztucznej inteligencji, aby zwiększyć wydajność swojej pracy oraz uczynić ją łatwiejszą, szybszą i bardziej efektywną. Wykorzystanie narzędzi sztucznej inteligencji ułatwiło automatyzację znacznej części ataków phishingowych i przewiduje się, że częstotliwość takich ataków będzie w przyszłości eskalować, stanowiąc poważne zagrożenie dla cyberbezpieczeństwa"*

– mówi Marijus Briedis, dyrektor ds. technologii w firmie NordVPN.

Istnieje kilka sposobów wykorzystania sztucznej inteligencji przez hakerów do zwiększenia skuteczności ataków cybernetycznych.

Dostosowywanie ataków typu spear-phishing

Najczęstszym sposobem, w jaki cyberprzestępcy wykorzystują sztuczną inteligencję, jest tworzenie spersonalizowanych i przekonujących ataków phishingowych. Ponieważ sztuczna inteligencja może analizować ogromne ilości publicznie dostępnych danych i lepiej rozumieć zachowania i preferencje ofiary, generowane przez sztuczną inteligencję spersonalizowane e-maile phishingowe mogą być bardzo skuteczne w oszukiwaniu osób. Co więcej, informacja publiczna to nie jedyna rzecz, jaką dysponują popularne narzędzia AI.

„W miarę rozpowszechniania się systemów sztucznej inteligencji wzrasta ryzyko niewłaściwego obchodzenia się z wrażliwymi danymi lub niewłaściwego ich wykorzystania. Na przykład, jeśli pracownik określonej firmy użyje narzędzia AI do napisania raportu na podstawie poufnych informacji, te same dane mogą później zostać wykorzystane do stworzenia tak zwanych ataków typu spear-phishing, które są w dużym stopniu dostosowane do indywidualnych celów, zwiększając prawdopodobieństwo powodzenia. Kiedy otrzymasz e-mail phishingowy zawierający informacje, które powinny być poufne, istnieje duże ryzyko, że dasz się nabrać"

– wyjaśnia Briedis.

Modyfikowanie złośliwego oprogramowania w czasie rzeczywistym

Narzędzia sztucznej inteligencji pomagają hakerom automatyzować zadania, takie jak rozpoznawanie i tworzenie niestandardowego złośliwego oprogramowania, dzięki czemu ich ataki są skuteczniejsze, trudniejsze do wykrycia i zakrojone na dużą skalę. Na przykład boty wykorzystujące sztuczną inteligencję mogą przeprowadzać zautomatyzowane ataki typu brute-force, co prowadzi do zwiększonej liczby ataków.

„Hakerzy wykorzystują sztuczną inteligencję również do wymuszania ataków złośliwego oprogramowania w celu ominięcia tradycyjnych zabezpieczeń cybernetycznych. Korzystając z algorytmów sztucznej inteligencji, napastnicy modyfikują złośliwe oprogramowanie na bieżąco, aby uniknąć wykrycia przez program antywirusowy i inne narzędzia bezpieczeństwa. Dzięki tego rodzaju automatyzacji hakerzy rzucają poważne wyzwanie tradycyjnym narzędziom cyberbezpieczeństwa i wykorzystują ich słabe punkty"

– mówi Briedis.

Jak minimalizować zagrożenia cyberbezpieczeństwa ze strony AI

Chociaż sztuczna inteligencja udowodniła swoją skuteczność w ulepszaniu cyberataków, można ją również wykorzystać do ochrony użytkowników, ale nie jest to złoty środek.

„Cyberbezpieczeństwo wymaga wielopoziomowego podejścia, obejmującego edukację użytkowników, regularne aktualizacje oprogramowania, silne hasła i najlepsze możliwe praktyki w zakresie bezpieczeństwa"

– dodaje Briedis.

Ekspert ds. cyberbezpieczeństwa Marijus Briedis radzi, jak ograniczyć zagrożenia cyberbezpieczeństwa stwarzane przez ataki oparte na AI:

- **Przed kliknięciem sprawdź docelowy adres URL**. Najczęstszym sposobem nakłaniania ofiar do pobrania złośliwego oprogramowania są phishingowe wiadomości e-mail, które zawierają fałszywe adresy URL i złośliwe pliki. Wygenerowane przez sztuczną inteligencję e-maile phishingowe mogą być trudne do rozróżnienia. Zamiast klikać link, najpierw najedź myszką na przycisk, aby zobaczyć docelowy adres URL. Sprawdź, czy wygląda znajomo i – co ważne – czy zawiera „https".
- **Dokładnie sprawdź autentyczność wiadomości e-mail**. Jeśli otrzymasz maila od kogoś, kogo znasz, zastanów się dwa razy, zanim klikniesz jakikolwiek link. Czy wysyłanie maili jest typowe dla tej osoby? Jeśli nie, skontaktuj się z nią przez telefon, media społecznościowe lub inne kanały, aby potwierdzić autentyczność.
- **Użyj niezawodnego programu antywirusowego**. Użytkownicy powinni wybrać program antywirusowy z zaawansowaną ochroną przed złośliwym oprogramowaniem, oprogramowaniem szpiegującym i wirusami. Program antywirusowy wykryje i zneutralizuje złośliwe zagrożenia, zanim wyrządzą one jakąkolwiek szkodę. Na przykład funkcja Threat Protection NordVPN neutralizuje cyberzagrożenia, takie jak pliki zawierające złośliwe oprogramowanie lub złośliwe strony internetowe, zanim zdążą uszkodzić Twoje urządzenie.
- **Włącz zaporę sieciową (firewall)**. Zapora sieciowa chroni system, monitorując ruch sieciowy
- i blokując podejrzane połączenia. Użytkownicy powinni mieć ustawienia zabezpieczeń i upewnić się, że wbudowana zapora sieciowa komputera działa.
- **Zachowaj bezpieczeństwo w publicznej sieci Wi-Fi, korzystając z VPN**. Publiczne sieci
- Wi-Fi są bardzo podatne na ataki hakerskie. Cyberprzestępcy często atakują użytkowników
- w bezpłatnych hotspotach i próbują zainfekować ich urządzenia złośliwym oprogramowaniem. Użytkownicy powinni zawsze korzystać z VPN, aby zabezpieczyć swoje połączenie Wi-Fi
- i chronić się przed niechcianymi szpiegami.

NordVPN to najbardziej zaawansowany na świecie dostawca VPN, z którego usług korzystają miliony użytkowników na całym świecie. NordVPN zapewnia podwójne szyfrowanie VPN i Onion Over VPN oraz gwarantuje brak śledzenia w sieci. Jedną z kluczowych funkcji produktu jest Threat Protection, która blokuje złośliwe oprogramowanie, niebezpieczne strony internetowe oraz skrypty śledzące i reklamy. NordVPN jest łatwy w obsłudze, oferuje jedne z najlepszych cen na rynku i ma ponad 5000 serwerów w 60 krajach na całym świecie.

Więcej informacji: http://nordvpn.com/pl.