AVRASYA İNCELEMELERİ MERKEZİ
CENTER FOR EURASIAN STUDIES

AVRASYA İNCELEMELERİ MERKEZİ
CENTER FOR EURASIAN STUDIES

MICROSOFT; KUZEY KORE, ÇİN, RUSYA VE İRAN MENŞEİLİ CASUSLUK GRUPLARININ YAPAY ZEKA UYGULAMASI CHATGPT'YE ERİŞİMİNİ ENGELLEDİ

-

15.02.2024

SonDakika (14 Şubat 2024)

Microsoft, siber saldırılarını planlamak için üretken yapay zeka kullandığını tespit ettiği Kuzey Kore, Çin, Rusya ve İran menşeili casusluk gruplarının yapay zeka uygulaması ChatGPT'ye erişimini engellediğini açıkladı. ChatGPT'yi kullanan bu gruplar, teknik operasyonlarını güçlendirmek, bilgi toplamak ve oltalama kampanyaları için yapay zekayı kullanıyorlardı. Microsoft, bu siber casusluk gruplarının ChatGPT'ye erişimini engelleyerek güvenlik önlemlerini artırmış oldu.

Microsoft'un internet sitesinde, şirketin iş ortağı OpenAI ile birlikte geliştirdiği ChatGPT'yi kullanan farklı uluslardan yapılan siber saldırılara ilişkin yapılan açıklamada, Çin'le ilişkilendirilen siber casusluk gruplarından "Sodium" ve "Chromium"un büyük dil modellerinin teknik operasyonlarını güçlendirme, Asya jeopolitiği, ABD içişleri ve diğer hassas konularda bilgi toplamak için yapay zekayı kullandığı bildirildi.

İran Devrim Muhafızları Ordusu bünyesinde çalıştığı belirtilen "Curium"un, yazılım hatalarını düzeltme, oltalama e-posta üretimi ve siber saldırılarda fark edilmemek için ChatGPT üzerinden ipuçları aradığı aktarıldı.

Devamı için tıklayınız.

Kaynak/Source: