AIG AIG損保

2023/7/11 版 vol.383

サービスデリバリー部

Success Story

ChatGPT の悪用事例が報告されております。

ChatGPT は、大量の言語を学習して自然な文章が生成できる人工知能（AI）チャットボットです。
最近、より高度な言語理解能力を備え、複雑なタスクにも対応できる「GPT4.0」が発表されて話題となっておりますが、すでに犯罪者によって巧妙な手口で不正利用（フィッシングメールやマルウェアの作成等）されていることが確認されております。

■ChatGPT を悪用した不正手口

【事例①】 マルウェア（悪意のあるプログラム）の作成

通常、マルウェアの作成には高度なプログラミングの知識や経験が必要ですが、さまざまなプログラミングのソースコードを迅速に作ることができるため、プログラミングスキルが低いサイバー犯罪者でもChatGPTを利用して「すぐにマルウェアが作成できる」ことが明らかになりました。

【事例②】 暗号化（データを暗号化して個人情報や機密情報などを保護するための）ツールの作成

プログラミングスキルの低いサイバー攻撃者が、ChatGPT を利用して暗号化ツールを作成したことが判明しました。悪意を持って使うことで、本人の操作なしで他人のマシンを完全に暗号化し、システムに入り込んで不正を働く「ランサムウェア」へと変化します。

【事例③】 闇取引のプラットフォームの作成

ダークウェブを作成するプログラムの披露によって、犯罪者たちの間で不正に入手したアカウント情報やカード情報などの取引が行われます。

【事例④】 公式サイトになりすましてカード情報を窃盗

複数のフィッシングサイトが公式の ChatGPT になりすまし、クレジットカード情報を盗み出していることが判明しました。また、サイバー攻撃者が ChatGPT の人気を利用してマルウェアの配布やサイバー攻撃を実行した事例も確認されています。

■ChatGPT を使った不正利用で考えられる被害

ChatGPT の需要が急速に伸びていることと比例して、不正を働こうと企む悪用者が人工知能を使ってコンピュータのプログラムを作成したり、ハイレベルな文章を作らせたりする行為が増え、セキュリティ面でのリスクも大きくなることが予想されます。

【被害①】 不正に作成したマルウェアや暗号化ツールによる攻撃

マルウェアや暗号化ツールのプログラムを素人でも容易に作成できる可能性が広がり、攻撃リスクがいっそう高まることが懸念されます。

【被害②】 本物そっくりな偽サイトやメールによるフィッシング攻撃

少ない労力で大量の不正アタックが可能となる上、日本語翻訳機能の精度が上がることで、海外の攻撃者が今までよりも自然な日本語でフィッシングメールを作成することができるようになります。

■対策：従来からご案内している情報セキュリティ対策の強化

今後、ChatGPT を使って作成した偽メールの文面やサイトの見た目などが、ますます正規サイトそっくりになっていくことが予想されます。

対応策

①発信元のメールアドレス、URL を確認するクセをつけましょう。
②OS、アプリケーション等のソフトウェアは最新の状態に保ちましょう。

出典：ChatGPT を使った不正利用とは？4 つの事例や被害を防ぐ対策を紹介
https://frauddetection.cacco.co.jp/media/fraud-access/9951/