サイバーセキュリティ最前線

AIを悪用したサイバー攻撃が多発!!
セキュリティ対策のアップデートが急務!!

2024年はChatGPTなどに代表される生成AIの普及にともない、AIの利用が急速にすすんだ年でもあった。が、その利便性の裏ではサイバー攻撃者によるAIの悪用がすすんでおり、セキュリティ分野の専門家たちも警鐘を鳴らしている。

AIが生み出すあらたな脅威

現時点ですでに確認されている手法として、生成AIを用いた高度なフィッシング（詐欺メール）やソーシャルエンジニアリング攻撃（ミスをしやすい点など人間の弱点を悪用する手口）がある。これらの攻撃では、標的の行動パターンや関心に応じてAIでメッセージを自動生成するなどの巧妙化がすすんでいる。また、詐欺メールなどが日常茶飯事となり、迷惑メールなどを判別できるスパムフィルタリング技術をすり抜けるケースが目立ってきている。そして、AIによるマルウェアの自動生成も進化しつづけており、「小規模なハッカー集団であっても大規模かつ高度な攻撃を行えるようになってきた」と指摘する声も。

さらに、専門家たちは近い将来、AIがサイバー攻撃をより進化させるのではないかと指摘している。たとえば「リアルタイムで学習し適応する自律型マルウェアが登場しはじめるのではないか」と。マルウェアがみずからネットワーク内の情報を収集・学習し、攻撃のタイミングや対象を判断するようになると、従来の防御策が通用しにくくなるだろう。また「自然言語処理技術を駆使したリアルタイムのなりすましチャットが登場する可能性もある」とも。これが実現すると、AIが偽のカスタマーサポート担当者になりすまして、ターゲットから個人情報や機密情報を引き出すといった事態が発生するかもしれない。

技術と時代にあわせたアップデートが必要

こうした状況にあって、長年にわたってITセキュリティに取り組む㈱ブロード（東京都千代田区）は、セキュリティ対策として「RidgeBot」の導入を提案している。このツールがあれば簡単にペネトレーションテスト（侵入検査）ができるという。専門職の手を借りずにAIを利用して実際の攻撃手法を模倣して脆弱性を洗い出すというものだ。「開発元の米Ridge Security社は新種の攻撃パターンもいちはやくAIに学習させる。このスピード感はバツグンで、攻撃側のAI利用にも十分に対抗することができるはずだ」とブロードは太鼓判を押す。

また、進化をつづけるマルウェアには「HPSCE」が有効だという。「『仮想のパソコン』でメールやインターネット由来のすべてのファイルを開いて使用できるツールなので、マルウェアの種類を問わずに確実に隔離することが可能になる」そうだ。

さらに、一層巧妙化するソーシャルエンジニアリング攻撃やなりすましチャットのような手口については「ユーザー一人ひとりが適切なアクセス権を持つように管理することが被害の抑制につながる」と警告する。そして、それには特権管理分野のリーディングカンパニーである米BeyondTrust社のソリューションが有効だという。

そのほか、AIとは少々異なるが、量子コンピュータの発展・普及によって暗号解読リスクが高まるといった指摘もあり、NIST（アメリカ国立標準技術研究所）の調査によると、調査対象とした69種の暗号化アルゴリズムの候補のうち、量子コンピュータに耐えられるものは4種のみだったとか。サイバーセキュリティについても、技術と時代にあわせたアップデートが急務となっている。