報道関係者各位

AI はついにサイバー攻撃の夢を見るようになるのか？

～ AI によるサイバー攻撃に対抗するためには新たなセキュリティ技術革新が必要、ウィズセキュアがレポート ～

2022 年 12 月 20 日
ウィズセキュア株式会社

現在のサイバー攻撃における人工知能 (AI) の利用は未だ限定的ではありますが、先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は同社が発行した新しいレポートで、これが近い将来に変化する可能性があると警鐘を鳴らしています。

ウィズセキュアがフィンランド国家緊急供給庁 (NESA) と共同で作成したこのレポートは、AI とサイバー攻撃の両者が重なる領域における現在の動向と今後の展開を分析したものです。AI を利用したサイバー攻撃は、現在のところはまだ稀であるものの、ソーシャルエンジニアリングの応用 (なりすましなど) や、バックエンドシステムのデータ解析などのリサーチャーやアナリストが直接観測できない方法で利用されているとしています。

しかし、レポートではそれと同時に、量と質の両方における AI の進歩によって、より高度なサイバー攻撃が近いうちに起こりうるであろうことが強調されています。標的型攻撃、ソーシャルエンジニアリング、なりすましは AI を利用した脅威のうち、現在最も差し迫ったものであり、今後 2 年以内に攻撃の件数と巧妙さがともに進化すると予想されています。攻撃者たちは今後 5 年以内に、脆弱性の発見、攻撃作戦の計画と実行、防御を回避するステルス機能の使用、侵害されたシステムやオープンソースのインテリジェンスからの情報収集・マイニングを自律的に実行できる AI を開発するものと思われます。

ウィズセキュアのインテリジェンスリサーチャーである Andy Patel (アンディ・パテル) は、こうした状況について次のように述べています。
「AI が生成したコンテンツはソーシャルエンジニアリングのために使用されていますが、攻撃キャンペーンの指揮、攻撃手順の実行、マルウェアのロジックの制御を目的とした AI 技術は、まだ実際には観測はされていません。こうした技術は、まず国家レベルの攻撃グループなど、十分な資金と高度な技術を持つサイバーアクターによって開発され、それらの技術の一部はそれより低いスキルを持つ攻撃者の手に渡り (トリクルダウン)、サイバー攻撃の世界でより広く使用される可能性があります。」

攻撃者による AI の利用がもたらすセキュリティ課題の一部は現在の防御で対応可能ですが、その他の課題については防御側が適応／進化することが必要であると、レポートは述べています。合成されたコンテンツを利用する AI ベースのフィッシング、生体認証システムのなりすまし、その他の攻撃への対策として新しい技術が必要となります。また、AI による攻撃の脅威を管理する上で、情報共有、セキュリティ人材の確保、セキュリティ意識向上のトレーニングなど、テクノロジーに依らないソリューションの重要性についても触れています。

ウィズセキュアでシニアデータサイエンティストを務める Samuel Marchal (サミュエル・マルシャル) は、今後取るべきアプローチについて、こう締めくくっています。
「セキュリティは、他の多くの AI アプリケーションと同じほどのレベルの投資や進歩が見られないため、最終的には攻撃者が優位に立つ可能性があります。正当な企業／組織、開発者、リサーチャーはプライバシー規制や法律に従っていますが、攻撃者はそうではないことを忘れてはいけません。政策の立案者が、安全で信頼性の高い倫理的な AI ベースのテクノロジーの開発を期待するのであれば、AI を利用したサイバー脅威との関係で自分たちのビジョンを確立する方法を検討する必要があるでしょう。」

本レポートの全文 (英語) は以下のページよりダウンロードいただけます。
https://www.traficom.fi/en/publications/security-threat-ai-enabled-cyberattacks

WithSecure Web サイト:
https://www.withsecure.com/jp-ja/
WithSecure プレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure について

WithSecure™は、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。
1988 年に設立された WithSecure は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の配信をおこなっています。