報道関係者各位

ウィズセキュア、2023 年のサイバー脅威に関する予測を発表

～ AI を使ったサイバー攻撃やクラウド環境への攻撃が増加すると予測 ～

2022 年 12 月 15 日
ウィズセキュア株式会社

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、同社のセキュリティエキスパートによる、2023 年におけるサイバー脅威を取り巻く環境に関する予測コメントを発表しました。

1. 自然言語生成モデルがサイバー攻撃者に利用される

Andy Patel (アンディ・パテル)
セキュリティコンサルタント

子供たちはすでに自然言語生成モデルを使って、宿題をごまかしています。サイバー攻撃者はこの技術を利用して、説得力のある偽のコンテンツを作成し始めるでしょう。こうしたモデルは、文法的に正しく、比較的よく書かれたテキストを作り出し、わずかな編集を加えるだけで完全な説得力と信憑性を持つに至ります。このような方法により、偽物の NGO／シンクタンク／政策関連サイト、そして標的型の高度なソーシャルエンジニアリングキャンペーンで使用されるフェイク企業の Web サイト、LinkedIn で標的型フィッシングに使用されるような偽のソーシャルメディアプロフィールの作成に使用される可能性があります。

2. セキュリティ侵害を通じて、機械学習モデルを盗み出そうという試みが増える

Andy Patel (アンディ・パテル)

2022 年末、AI アートをサービスとして提供する NovelAI 社が侵害を受け、同社の持つ AI モデルがインターネット上に流出しました。このようなサービスが増えれば増えるほど、AI モデルの流出や盗難が増えることが予想される。特に、これらのサービスプロバイダーのほとんどは、ユーザーにアクセス料を課しているためです。AI による音声模倣技術が容易に利用できるようになり、ソーシャルエンジニアリング攻撃でより広く使用されるようになると予想されます。

3. クラウドに特化した攻撃が主流に

Leszek Tasiemski (レシェック・タシエムスキー)
プロダクト部門長

サイバー攻撃者は、クラウドに特化した攻撃手法をマスターしつつあります。これまでクラウドで観測される攻撃の多くは、従来の攻撃を「移植」したものです。クラウドインフラにおけるセキュリティ／監視／制御が難しいという点を突いて、攻撃がおこなわれており、今後はクラウドインフラの弱点／設定ミス／脆弱性などを狙ったクラウドに特化した攻撃が増加していくでしょう。クラウド IAM の考え方は複雑かつ多様であるため、特に保護が難化します。

4. データ処理に必要な電力は、サステナビリティの枠において象のような存在となる

Leszek Tasiemski (レシェック・タシエムスキー)

私たちは、データ通信やクラッキングに多くのエネルギーが必要であることを忘れてしまいがちです。2021 年には暗号通貨関連を除いても約 600TWh (テラワット時) の電力が消費されました。企業や個人は、消費電力を削減する方法を模索することになるでしょう。多くのデータセンターでは、すでに再生可能エネルギーへの転換がかなり進んでいます。また、今後予想されるのは、コードを実行するインフラだけでなく、ソフトウェア (コード) のエネルギー効率もより重視されるようになることです。エネルギーやクラウドの価格が高騰しているため、より効率的なソフトウェアが求められ、その効率性が競争におけるアドバンテージになる可能性が高いのです。最もエネルギーを消費する仕事の 1 つは、機械学習モデルのトレーニングです。AI 技術アプリケーションのエネルギーフットプリントを最適化する革新的なアイデアが期待されます。サイバーセキュリティにおいては、マイニングマルウェア／ソフトウェアの検出と除去がより一層求められるようになるでしょう。

5. 2038 年問題は思っているより早くやって来るため、今から準備が必要

Tom Van de Wiele (トム・ヴァンドゥウィール)
プリンシパルスレット&テクノロジーリサーチャー

2038 年問題には、テクノロジーが関連する、予見できる問題／予見できない問題の両方が徐々に露見し始めてきています。例えば、契約の終了日の計算、大きな買い物をした場合や産業界における保証の有効期限など、2038 年が既に問題となるであろうものなどです。現在、そして今後数年間において起こるであろう最初の問題は、計画／タスク／PKI／その他未来の日付を使用しなければならないシステムに関係するものでしょう。メディアはこれを大げさに報道する可能性がありますが、それは必ずしも悪いことではありません。Y2K の場合、コンピュータが現在ほど多くの人々の生活に密接に関連しておらず、影響も限定的だったため、いい啓蒙活動になったと言えます。しかし現在私たちが抱える問題は、2000 年に COBOL が使用されていた範囲と比較して、現在は基本的に主要なオペレーティングシステム／ライブラリ／ソフトウェアエコシステムは C/C++で動いているものが遥かに多い、いうことです。
これは、静観していれば通り過ぎていってくれるものではありません。企業は、自社の中核的なビジネスプロセスの一部として使用されている全てのソフトウェアについて、その場しのぎでない見直しを行い、ベンダーやメーカーが何をしているかを調べ、潜在的な問題を予測するための対話を開始しなければならないでしょう。また、サポートサービスやサードパーティが使用する技術を見直すためのプロセスが整備されていることを確認する必要があります。事業継続性とディザスタリカバリの計画は、ほとんどの企業において脅威マップで上位に位置付けられます。サポートを受けるのに手間がかかったり高価だったり、または不可能だったりする、小規模または特注のソフトウェアに依存してきた企業にとっては、代替手段を探して移行する必要があります。

6. マルウェアによる攻撃キャンペーンは、人間のスピードから機械のスピードへと移行する

Mikko Hypponen (ミッコ・ヒッポネン)
主席研究員

マルウェアによる攻撃キャンペーンは、人間のスピードから機械のスピードへと移行していくでしょう。最も高い能力を持つサイバー攻撃者グループは、単純な機械学習技術を使用して、私たちの防衛手段に対する自動的なリアクションを含め、マルウェアキャンペーンの展開と運用を自動化する能力を獲得するでしょう。マルウェアの自動化には、不正な電子メールの書き換え、不正な Web サイトの登録と作成、検知を回避するためのマルウェアコードの書き換えやコンパイルなどの技術が含まれるようになると考えられます。

上段: 左から Andy Patel, Leszek Tasiemski　　下段: 左から Tom Van de Wiele, Mikko Hypponen

本リリースの内容をもとにした「Cyber Security サウナ Japan」ポッドキャストは、以下のページにてご覧いただけます:
https://www.withsecure.com/jp-ja/whats-new/podcasts/japan-podcast-03

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。