報道関係者各位

ウィズセキュア、2024 年のサイバーセキュリティ動向予測を発表

～ サイバー犯罪の専門化、クラウドサービスや AI を悪用した攻撃について注意喚起 ～

2023 年 12 月 20 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、2024 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. サイバー犯罪の専門化

近年、APT (高度で持続的な脅威) グループ、ランサムウェア攻撃グループ、イニシャルアクセスブローカーなどにより、企業内の貴重なデータに到達するためのネットワークへの侵入経路として、インターネット境界に面したサービスの大規模な悪用が急増しています。ランサムウェアグループ『Clop』がファイル転送ソフトウェア『MOVEit』に仕掛けた攻撃の手法とその成功により、同様の流れでエッジデータ転送サーバーをターゲットとした、より大規模な攻撃キャンペーンが実行されるのではないかと考えます。MOVEit は大量の重要なファイルを組織間で確実に転送するために使用されていますが、Clop は MOVEit のサーバーを悪用してこれらのファイルにアクセスし、流出させました。ランサムウェアグループにとって、大量の重要データへのアクセスは最終目標であり、脆弱性を持つ MOVEit サーバーよりもネットワークのさらに先へのアクセスではなく、悪用されたサーバー自体に価値があるような模倣的な攻撃が増えることが想定されます。
このタイプの攻撃は手順が少ないため攻撃者にとっては単純なものであり、同時に防御側にとっては検知が非常に困難となります。攻撃はすべて 1 台のサーバーに向けられるため、ラテラルムーブメント (水平移動) を検知することはできません。ターゲットとなるサーバーはインターネットに面しているため、例えば高度に統制されたドメインコントローラーで構成されるコアサーバーネットワークよりもノイズの多い環境となります。こうしたサーバーがリモートの宛先に大量のファイル転送を行うことは通常の動作だといえるため、異常なアクティビティとして認識されなかったり、セキュリティチームによって誤検知として処理されたりする可能性は高いであろうと考えられます。

2. クラウドサービスの普及とリモートワークの継続による攻撃対象の拡大

サプライチェーンの一部が侵害を受けると、複数の組織に悪影響を及ぼす可能性があります。多くのユーザー数を持つ VoIP ソフトウェアのプロバイダーを侵害し、そのユーザーを感染させた 3CX の攻撃は、そのような例の 1 つです。攻撃者は 3CX の Web サーバーの脆弱性を悪用し、ソフトウェアのアップデートに悪意のあるコードを混入しました。3CX のサプライチェーン攻撃は、1 つのソフトウェアサプライチェーン攻撃が別のソフトウェアサプライチェーン攻撃につながったものです。サプライチェーンシステムだけでなく、サードパーティベンダーのシステムも保護することの重要性を示しており、今後もサプライチェーン攻撃は多くの課題をもたらすことになると考えられます。
生産性の向上と競争力維持のために、クラウドサービスの活用を含む DX (デジタルトランスフォーメーション) が進む中、セキュリティが十分に確保されていない新しいテクノロジーやプロセスの導入も増加が予想されます。新しいインターフェース、API、通信チャネルを備えたクラウドサービスは攻撃者にとって新たな標的となり、潜在的な攻撃対象領域が拡大することになります。
クラウドインフラとリソースの設定と管理におけるエラーや見落としが原因で発生するクラウドサービスの設定ミスは、セキュリティの脆弱性、データの漏洩、運用上の問題につながります。こうした設定ミスを軽減するには、定期的なセキュリティ監査を実施し、クラウドサービスプロバイダが提供するベストプラクティスに従い、潜在的な問題の継続的な監視を怠らないことが必要となります。

3. オープンソースは安全な AGI (汎用人工知能) 作りに貢献できるのか？

オープンソースの AI は今後も改善され、広く使用されることでしょう。これらのモデルは AI の民主化をもたらすものであり、権力を少数の企業から人々の手へと移すものです。2024 年には、この分野でさらに多くの研究とイノベーションが起こり、また、オープンソース支持者の数は増えるでしょう。
2024 年のアメリカ大統領選挙に向けて、AI はフェイクニュースや影響力を持つ戦略のために使われるでしょう。サイバー犯罪のエコシステムはアクセスブローカー、マルウェア作成、スパムキャンペーンサービスなど、細分化が進んでおり、フェイクニュースの分野では PR やマーケティングを装いながら、フェイクニュースや影響力の行使をサービスとして提供する企業も数多く存在します。サイバー犯罪者は効率化のために AI を活用し、生成モデルを用いてフィッシングコンテンツ、ソーシャルメディアコンテンツ、ディープフェイク、合成画像／動画を作成するでしょう。こうしたコンテンツの作成にはプロンプトエンジニアリングの専門知識が必要であり、それさえもサービス化されていくかもしれません。画像や動画を生成する AI サービスが制御しやすくなるにつれて、アクセシビリティにおいてテキスト生成に追いつき始めると考えられます。そして AI サービス統合や大手による独占が始まると予想されます。AI が生成する膨大な数の画像がインターネット上に氾濫し歴史的な画像も含めほぼすべての画像がその真贋を疑われるようになるでしょう。
今後登場するサービスや製品では AI 機能の搭載の有無が購入／導入決定の要素の 1 つになりますが、初期の IoT デバイス同様、セキュリティを軽視した製品も市場に出てくることが予想されるため、ユーザーはこうした点も十分考慮する必要があります。

4. サプライチェーンへの攻撃

デジタル世界において私たちは、サプライチェーンのセキュリティを完全に把握することができない製品やサービスを利用しています。私たちのデータはいたるところに存在し、さまざまなプロバイダーが提供するサービスによって処理されていますが、そのプロバイダーも自身のサプライチェーンにおけるセキュリティの全容を把握できているとは限りません。
セキュリティ／プライバシー保護のために多くの規制がサービスプロバイダーに対して導入されつつありますが、これらの規制は現在の世界の考え方に基づいて運用されています。テクノロジーの進化に合わせて規制は変化し、そしてサプライチェーンは絶えず新たな課題を持つこととなります。
実世界では、井戸に毒を盛ればその地域のコミュニティーに影響を与えることができます。デジタル世界では、たった 1 人で海をも汚染することができます。攻撃者は大手のサービスプロバイダーそのものを標的にする必要はなく、オープンソースのコードや AI モデルを標的にすることもできます。汚染されたオープンソースコードには汚染されたコードを特定するツールがあるのとは対照的に、汚染された AI モデルが提供する変更にユーザーが気づかない可能性があり、深刻な事態をもたらすことになります。このような状況では、もはやゼロトラストは機能せず、AI が信頼できるものかどうか、人々には知る由もないでしょう。

5. サイバーセキュリティにおけるグリーンコーディング

様々なアプリケーションにおいてデータ量が増加するなか、温室効果ガスの排出量の削減をおこなう上で、ICT 業界がクラウドサービスと各種デバイスの両方において果たす役割は大きなものとなります。今後 12～18 ヶ月の間に、コードの全体的なエネルギー効率を優先させるべきというユーザー側からの要請に後押しされるかたちで、ICT 業界における共通規格が登場すると予想されます。コードを最適化するには、デバイスから実際の使用データを収集し、ラボでのテストにとどまらず、高い効果を持つ分野を特定する必要があります。AI テクノロジーはコンテンツ作成と分析に優れていますが、その進歩はエネルギー集約的なものであり、コンピューティングの運用に影響を与えています。生成 AI エンジンの構築と運用には従来のアルゴリズムとは対照的に計算コストがかかります。持続可能で効率的な利用のために、これらのテクノロジーを実世界のシナリオに適用する際には、こうしたさまざまな要素を考慮することが極めて重要となります。

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

ウィズセキュアは、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検出し、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 年に設立されたウィズセキュア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、X (旧 Twitter) アカウント @WithSecure_JP でも情報の発信をおこなっています。

※　以下、メディア関係者限定の特記情報です。個人の SNS 等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】
ウィズセキュア株式会社
広報部　　秦　和哉
TEL：03-4578-7745 (直通)　／　080-6842-8222 (モバイル)
press-jp@withsecure.com